



FFIEC Information Technology Examination Handbook

Architecture, Infrastructure, and Operations

JUNE 2021

Contents

INTRODUCTION.....	1
I.....ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS	2
II.....ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS	
GOVERNANCE	3
II.A Board and Senior Management Responsibilities.....	4
II.A.1 Strategic Planning.....	6
II.A.2 Enterprise Risk Management.....	7
II.B Other Roles and Responsibilities.....	7
II.B.1 IT Management Responsibilities	8
II.B.1(a) Chief Architect.....	8
II.B.1(b) Chief Data Officer	9
II.B.1(c) IT Operations Management	10
II.B.2 IT Operations Personnel Responsibilities	10
II.C Policies, Standards, and Procedures.....	11
II.D Internal Audit, Independent Reviews, and Certification Processes	12
II.E Communication.....	13
II.F Board and Senior Management Reporting	13
III.....COMMON AIO RISK MANAGEMENT TOPICS.....	15
III.A Data Governance and Data Management	15
III.A.1 Data Identification and Classification	16
III.A.2 Database Management.....	17
III.A.2(a) Database Security.....	18
III.A.3 Non-Production Environments	19
III.A.4 Data Analytics	20
III.B IT Asset Management.....	22
III.B.1 Technology Asset Inventory.....	23
III.B.1(a) Hardware Inventory.....	24
III.B.1(b) Software Inventory	25
III.B.2 IT Asset End-of-Life	26
III.B.3 Shadow IT.....	27
III.C IT and Business Environment Representations	28
III.C.1 Network Diagrams	30
III.C.2 Data Flow Diagrams	31

III.C.3	Business Process Diagrams and Narratives.....	33
III.D	Managing Change in AIO	34
III.D.1	Change Management	35
III.D.2	Transitioning From Strategic Change Management to Day-to-Day Operations	37
III.E	Oversight of Third-Party Service Providers	37
III.F	Resilience	38
III.G	Remote Access	39
III.H	Personally Owned Devices	41
III.I	File Exchange.....	41
IV	ARCHITECTURE.....	43
IV.A	Architecture Plan	44
IV.B	Design Objectives.....	44
IV.C	IT Architecture Design	46
IV.D	Enterprise Architecture	47
V	INFRASTRUCTURE	49
V.A	Hardware	50
V.B	Network and Telecommunications	50
V.B.1	Network.....	51
V.B.2	Telecommunications	52
V.B.2(a)	Voice Communications	53
V.B.2(b)	Data Communications.....	54
V.C	Software.....	55
V.C.1	Internally and Externally Developed Software	55
V.C.2	Software Types.....	56
V.C.2(a)	Open Source Software.....	59
V.C.2(b)	Mainframe Security Software	59
V.C.2(c)	Application Programming Interfaces	60
V.C.3	Software Hosting	62
V.D	Environmental Controls	63
V.D.1	Heating, Ventilation, and Air Conditioning.....	64
V.D.2	Smoke and Fire.....	64
V.D.3	Water	65
V.D.4	Power.....	65
V.E	Physical Access Controls	66

VI	OPERATIONS	67
VI.A	Operational Controls	67
VI.A.1	Operating Centers	68
VI.A.2	Authorization Boundary	69
VI.A.3	Identity and Access Management	69
VI.A.4	Personnel Controls	70
VI.B	IT Operational Processes	71
VI.B.1	Maintenance	71
VI.B.2	Configuration Management	72
VI.B.3	Vulnerability and Patch Management	73
VI.B.3(a)	Vulnerability Management	73
VI.B.3(b)	Patch Management	74
VI.B.4	Backup and Replication Processes	75
VI.B.5	Scheduling	76
VI.B.6	Capacity Management	76
VI.B.7	Log Management	77
VI.B.8	Disposal of Data and Media	78
VI.C	Service and Support Processes	79
VI.C.1	Service Management	79
VI.C.2	Operational Support	80
VI.C.3	IT Support	80
VI.C.4	Event, Incident, and Problem Management	82
VI.D	Ongoing Monitoring and Evaluation Processes	83
VI.D.1	Monitoring and Reporting	84
VI.D.2	IT and Operations Key Performance Indicators	84
VI.D.3	Control Self-Assessments	85
VI.D.4	Continuous Improvement	85
VII	EVOLVING TECHNOLOGIES	87
VII.A	Cloud Computing	87
VII.A.1	Essential Characteristics	87
VII.A.2	Cloud Service Models	88
VII.A.3	Cloud Deployment Models	89
VII.A.4	Shared Responsibilities	90
VII.A.5	Risk Considerations for Cloud Computing	91
VII.A.5(a)	Access Control Considerations	92
VII.B	Zero Trust Architecture	93

VII.C	Microservices	94
VII.D	Artificial Intelligence and Machine Learning	96
VII.E	Internet of Things.....	97
APPENDIX A: EXAMINATION PROCEDURES.....		99
APPENDIX B: GLOSSARY		132
APPENDIX C: ABBREVIATIONS		151
APPENDIX D: REFERENCES		153

INTRODUCTION

The “Architecture, Infrastructure, and Operations” booklet is one in a series of booklets that compose the *Federal Financial Institutions Examination Council (FFIEC)*¹ *Information Technology Examination Handbook (IT Handbook)*. The *IT Handbook* is prepared for use by examiners.² With the publication of this booklet, the FFIEC member agencies replace the “Operations” booklet issued in July 2004. The title change reflects the overall importance of an entity’s architecture, infrastructure, and operations (AIO). For *IT Handbook* purposes, the term “entities” includes depository financial institutions,³ nonbank financial institutions,⁴ bank holding companies,⁵ and third-party service providers.⁶

This booklet discusses enterprise-wide, process-oriented approaches that relate to the design of technology within the overall business structure, implementation of IT infrastructure components, and delivery of services and value for customers. It discusses the following:

- Principles and practices for IT and operations as they relate to safety and soundness, consumer financial protection, and compliance with applicable laws and regulations.
- Processes for addressing risk related to the design and implementation of IT systems.
- Principles to help examiners evaluate the delivery of financial products and services.
- Management oversight of AIO and its related components, including governance; common risk management topics; specific activities of AIO; and evolving technologies that examiners may encounter during their reviews.

This booklet does not impose requirements on entities. Instead, this booklet describes principles and practices that examiners review to assess an entity’s AIO functions. Appendix A of this booklet provides objectives-based examination procedures. The application of the principles and related examination procedures may vary according to an entity’s complexity and risk profile.

¹ The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. 95-630. The FFIEC members are the Board of Governors of the Federal Reserve System (FRB), the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the State Liaison Committee (SLC).

² Each FFIEC member agency uses the principles outlined in this booklet, consistent with the member agency’s supervisory authority.

³ The term “depository financial institution” includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions.

⁴ The term “nonbank financial institution” includes non-depository financial institutions under the jurisdiction of either state banking departments or the CFPB.

⁵ The term “bank holding company” includes any company that has control over any bank or over any company that is or becomes a bank holding company as defined by the Bank Holding Company Act.

⁶ The term “third-party service providers” means third parties that provide services, the provision of which is subject to examination under the Bank Service Company Act, the Home Owners’ Loan Act, the Dodd–Frank Wall Street Reform and Consumer Protection Act, or other relevant law.

I ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS

This booklet provides a foundation for understanding the principles and practices within the functions of AIO. Architecture, infrastructure, and operations are separate but related functions that, together, management should oversee to appropriately manage an entity's activities related to designing, building, and managing the entity's technology. For the purposes of this booklet, the functions are referred to as AIO. The functions of AIO comprise a variety of activities, such as network and application design within architecture; selection and placement of physical and virtual technologies within infrastructure; and configuration, deployment, and maintenance of the infrastructure that supports the business within operations. The following definitions and descriptions provide an overview of the IT environment.⁷

Architecture refers to the manner in which the strategic design of the hardware and software infrastructure components (e.g., devices, systems, and networks) are organized and integrated to achieve and support the entity's business objectives. Planning and designing an effective IT architecture facilitate management's ability to implement infrastructure that aligns with the entity's strategic goals and business objectives.

Infrastructure refers to the physical elements, products, and services necessary to provide and maintain ongoing operations to support business activity and includes the maintenance of physical facilities. The focus of this booklet is on IT infrastructure, which is a subset of infrastructure and includes hardware, network and telecommunications, software, IT environmental controls (e.g., power, heating, ventilation, and air conditioning [HVAC]), and physical access. Once built and implemented, IT infrastructure can be managed internally or by a third-party service provider as part of the operations function.

Operations are the performance of activities comprising methods, principles, processes, procedures, and services that support business functions. Operations transform resource or data inputs into desired products, services, or results, and help in the creation and delivery of business value to internal and external customers. Operations include the ongoing maintenance, monitoring, and support for business systems, products, and services. This booklet addresses IT operations in the context of tactical management and daily delivery of services to support the overall business processes of the entity.

The principles and practices of the AIO functions outlined in this booklet are important for an effective IT environment. They support an entity's business lines and delivery of products and services to meet strategic business objectives. Inadequate coordination and oversight of these principles and practices may result in various risks (e.g., credit, liquidity, operational, and compliance).

⁷ The IT environment is the environment in which the entity directly operates, including direct interactions with the entity's third-party service providers.

II ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS GOVERNANCE

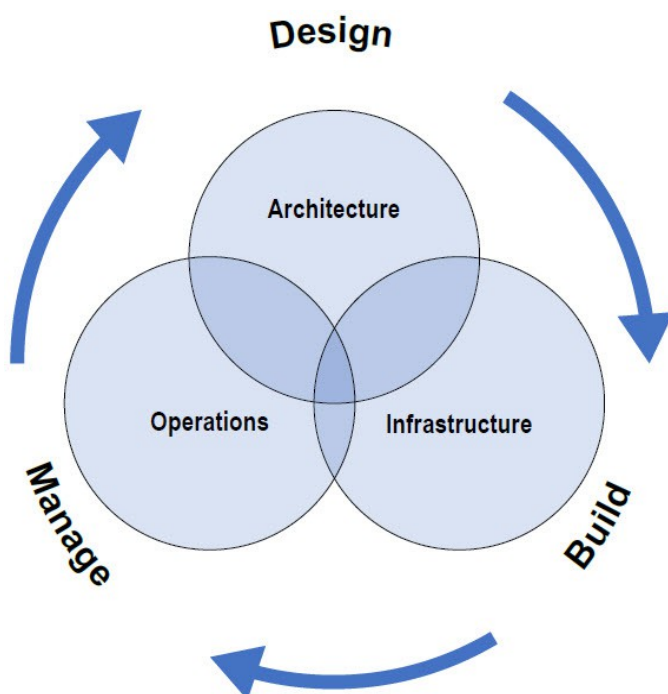
This section provides information about the governance of the AIO functions, including board and senior management responsibilities. General information about governance and risk management is contained in the *IT Handbook's* "[Management](#)" booklet and other member agency guidance.

Management should implement a process, such as a life cycle approach, to continuously manage technology to support operational needs and mitigate AIO-related risks. Figure 1 identifies the actions associated with this process for changing the architecture design to address evolving strategic and technology needs, building infrastructure that accommodates architecture changes, and managing technology in day-to-day operations.

To address risks, management should employ effective governance that includes the following:

- Delineation of board and senior management responsibilities.
- Strategic planning.
- Enterprise risk management (ERM).
- Delineation of other roles and responsibilities.
- Policies, standards, and procedures.
- Internal audit, independent reviews, and certifications.
- Communications.
- Board and senior management reporting.

Figure 1. Example of Life Cycle Approach for Governing AIO Risk



II.A Board and Senior Management Responsibilities

Action Summary

The board is responsible for overseeing, and senior management is responsible for implementing and maintaining, a safe and sound operating environment that supports the entity's goals and objectives and complies with applicable laws and regulations. Management should establish responsibility and accountability for the administration of the day-to-day functions of the IT environment.

Examiners should review for the following:

- Board regularly receives reports on AIO functions and activities from management.
- Discussions regarding AIO with the board are captured in meeting minutes.
- Tracking mechanisms and processes are in place to monitor issues related to AIO to their resolution.

The board,⁸ or its designated committee, and senior management should consider the entity's business objectives when governing the functions of AIO, including functions performed by affiliates and third-party service providers. Management should identify and evaluate risks associated with AIO, set short- and long-term objectives, and create policies and procedures to mitigate those risks. Furthermore, management should consider security and resilience in the design of new products and services.

Board oversight practices should include the following:

- Aligning AIO principles and practices with the board's strategic plans and risk appetite.
- Budgeting appropriate resources to support AIO activities.
- Ensuring board members have appropriate knowledge of risks to provide a credible challenge⁹ to management responsible for AIO functions.
- Enabling appropriate management training on AIO to carry out its responsibilities and manage risk.
- Reviewing AIO operating results and performance through audit reports, testing results, and management assessments and reports.

⁸ Most financial institutions have boards of directors; not all third-party service providers do. When an entity does not have a board, the senior leaders may have the responsibilities of the board described in this booklet.

Management oversight should include the following:

- Validating through audits and other independent assessments that the following are comprehensive, meet enterprise-wide business and strategic plan objectives, and can assist in the identification of AIO risks:
 - Architectural designs and integration across the entity (e.g., business units and other departments).
 - Infrastructure testing (e.g., network performance, penetration testing, and vulnerability assessments).
 - Operational testing (e.g., functional testing and operational resiliency).
- Addressing risks self-identified by management, from AIO-related audits, and from other independent assessments, including the following risks:
 - Architectural risks, such as a lack of stakeholder communication, inadequate requirements planning, lack of documented architecture review, and insufficient planning for aging architecture.
 - Infrastructure-related risks, such as under- or over-provisioning because of poor capacity planning, hardware or software incompatibility, and migration problems.
 - Operational risks, such as deficient IT asset management (ITAM), inadequate access management processes, equipment failures, inadequate processes for system updates, computer attacks, insider threats, disasters, and lack of qualified operations personnel.
- Assessing and updating management's AIO strategies and plans to reflect the current business conditions and operating environment for continuous improvement.
- Promoting alignment and integration between functions of AIO.

⁹ A credible challenge involves being actively engaged, asking thoughtful questions, and exercising independent judgment.

II.A.1 Strategic Planning

The board and senior management should evaluate whether the IT strategic plans align with the enterprise-wide business and strategic plan, as well as established priorities. Management should address the following key factors of strategic planning:

- **Participation of senior management:** Senior management should understand and support AIO activities and confirm the inclusion of those activities in the IT strategic plan. Senior management should continuously review the strategic planning process and incorporate changes, as appropriate.
- **Responsibilities within the AIO functions:** Management should define the responsibilities in AIO and determine whether the IT strategic planning process enables personnel to work toward achieving enterprise-wide business and strategic plan objectives.
- **Evaluation of architecture:** Management should evaluate the entity's current architecture and determine whether it meets enterprise-wide business and strategic plan objectives. If necessary, management should adjust its architecture to meet those plan objectives.
- **Impact of IT infrastructure:** Management should understand the relationship between IT infrastructure and the enterprise-wide business and strategic plan objectives. IT infrastructure should directly support IT operations activities to meet IT strategic needs.
- **Post-implementation evaluation:** Management should perform a post-implementation evaluation of the performance and results of IT projects and initiatives to determine whether each project achieved the anticipated benefits and stayed on budget or provided justification for cost variances. The evaluation should be based on management-defined metrics.

When considering whether AIO elements meet strategic plans, and to align with IT and enterprise-wide strategies, management should do the following:

- Evaluate whether past and current IT performance can support the planned IT strategy or future IT activities.
- Take steps to ensure and validate that the IT department is delivering services on time, within budget, and to business specifications.
- Balance resource investments between systems that support current operations and systems that transform operations and enable business units to grow and compete in new areas.

At a larger or more complex entity that provides IT services internally (e.g., help desk or in-house development teams) or externally as a third-party service provider (e.g., core processing providers or cloud service providers), management may consider the following in the IT strategic planning process:

- **IT services strategy management:** Service strategy defines the perspective, position, plans, and patterns that can be used to meet business outcomes. An IT service strategy helps management meet the needs of the entity (e.g., performance increase or constraint removal) while also providing for availability, capacity, continuity, and security.
- **Financial management for IT services:** Financial management for IT services is a method of allocating the cost of providing those services through contractual agreements or service-

level agreements (SLAs). The scope of financial management for IT services could include budgeting to control income and expenses, accounting for expenditures, and customer billing.

- **Service portfolio management (SPM):** SPM enables the entity to balance the investment in AIO with the ability to meet business outcomes. SPM provides for the following:
 - Decisions regarding services offered (e.g., cost benefit analysis).
 - Service catalog, including services that support IT functions.
 - Customer evaluations of services provided.
 - Control of services provided.
 - Planning and periodic assessment for a service's end-of-life (EOL).
- **Demand management:** Demand management includes consideration of customer demand for services and the entity's capacity to meet that demand.

II.A.2 Enterprise Risk Management

Management should implement an ERM structure that incorporates the functions of AIO. ERM should include a consistent and current review of the entity's products, processes, applications, infrastructure, interconnectivity, and other related risks to business operations. Depending on the entity's size and complexity, AIO may be incorporated into ERM in a less formal manner. For more information on ERM, refer to the *IT Handbook's* "[Management](#)" booklet.

Management should establish and maintain an effective risk management process for initiating and overseeing all AIO-related activities, including those that are outsourced. Management should consider doing the following when developing its risk management process for coverage of AIO risks:

- Perform an initial assessment of the entity's AIO-related risk.
- Design architecture to meet the entity's business goals or objectives, including enterprise and IT alignment, integration and interoperability, change management, and IT performance.
- Use infrastructure and appropriate implementation processes to support the entity's strategic objectives.
- Identify infrastructure assets (e.g., hardware and software) and associated interconnectivity critical to business and IT operations.
- Perform ongoing monitoring to identify and evaluate changes in risk from the initial assessment and periodically update the assessment.
- Identify and document roles, responsibilities, procedures, and reporting mechanisms for risk management in AIO activities.
- Define risk tolerances and risk and performance metrics for AIO activities.

II.B Other Roles and Responsibilities

Board oversight of IT, and subsequently the IT environment, is discussed in the *IT Handbook's* "[Management](#)" booklet. There are, however, specific governance topics related to operational oversight discussed in this booklet. Entities may use different titles than those illustrated within this booklet; the responsibilities described, however, should be appropriately assigned. Common

responsibilities and those responsibilities specific to architecture, infrastructure, and operations are described within the relevant sections.

II.B.1 IT Management Responsibilities

IT management is composed of individuals with responsibility for overseeing the management, maintenance, and use of IT resources. While the titles of these individuals may vary, common titles include chief information officer (CIO) or chief technology officer (CTO). For more information about CIO and CTO roles, refer to the *IT Handbook's* "[Management](#)" booklet. The CIO or CTO may also be responsible for overseeing the architecture function, implementing and maintaining the entity's infrastructure, and managing IT operations in an integrated IT environment. A specific individual (e.g., IT manager or chief architect) or a team (e.g., enterprise architecture [EA]) can carry out the architecture function's responsibilities. Generally, management should assign responsibilities based on the complexity of the entity's architecture needs. Responsibilities for architecture and data management may fall to a chief architect or a data officer; however, in smaller or less complex entities, these responsibilities may be rolled into one or more other roles. In such cases, management should maintain appropriate separation of duties. Regardless of how they are assigned, common responsibilities are described in the following sections.

II.B.1(a) *Chief Architect*

A chief architect or enterprise architect is an individual responsible for the IT architecture process that reviews how IT functions can be centralized, allowing departments across the entity to work together seamlessly. This individual should understand interrelationships between IT and the entity's business functions. The chief architect may be a C-level executive and, depending on the entity's complexity, may oversee and coordinate the efforts of other technology-specific architects, (e.g., chief security architect, chief data architect, and chief cloud architect). Architecture responsibilities typically include the following:

- Developing and maintaining the enterprise model and repository and establishing a common understanding, vocabulary, and blueprint for all stakeholders. In smaller or less complex entities, a formal chief architect may not be named, but the responsibilities should be addressed according to the entity's size and complexity.
- Maintaining responsibility for designing the entity's IT architecture to achieve the enterprise-wide business and strategic plan objectives.
- Designing the architecture to accommodate IT changes in a way that maximizes value and minimizes issues associated with changes.
- Communicating to the board and senior management any challenges (e.g., changing industry trends or resource constraints) in meeting those goals.
- Maintaining representations (e.g., blueprints, network diagrams, and topologies) of the entity's IT environment to help ensure that geographically diverse business units and divisions operate in an integrated manner.
- Reviewing existing infrastructure and operations and working with other members of management to determine the capabilities needed by IT systems to deliver new products and services.

- Working with other members of management to evaluate the implication of strategic planning (e.g., significant changes to architecture) on the entity's technology landscape.¹⁰
- Maintaining process and technical knowledge about security, storage, data management, and network service delivery.
- Utilizing appropriate knowledge of IT architecture, structural design (e.g., layout and capacity to meet business needs), business operations, and current technologies.

The chief architect typically reports directly to the CIO or other senior management and often works with the CIO to do the following:

- Develop IT architecture policy and terminology.
- Oversee IT architecture product development, use, and refinement.
- Serve as owner of the IT architecture repository.

II.B.1(b) *Chief Data Officer*

Typical responsibilities of a chief data officer (CDO) include enterprise-wide governance and use of information or data as an asset and assisting in protecting that data and deriving maximum value from it. Other responsibilities may include development of data-related policies, data life cycle management, data asset management (e.g., standardizing data formats and sharing data assets), oversight of compliance with applicable laws and regulations, and conformance with data management industry practices. The CDO provides input to the chief architect in the design of IT systems to promote alignment with enterprise-wide business and strategic plan objectives. This individual may be a C-level or senior executive who also reports to and works with other C-level personnel to manage risk. In smaller or less complex entities, this role may not be separate. Regardless, the responsibilities should be addressed. The CDO also performs the following:

- Oversees data management and data analysis and manages data-related projects (e.g., migrating data to the cloud or implementing a data analytics program).
- Analyzes whether the entity's products and services meet enterprise-wide business and strategic plan objectives from a data perspective.
- Makes data and reporting tools accessible to the entity's stakeholders, maintains data quality, and enables trust in data integrity.
- Owns the entity's strategic use of data and helps the entity perform more efficiently, improve productivity and revenue, and create business opportunities and innovation.
- Communicates information about the entity's data and analytics to appropriate stakeholders.
- Defines a data strategy to enable information sharing and meet compliance objectives and the entity's security requirements.
- Evaluates data and its usage across the enterprise rather than serving a specific business unit. When developing products, considers planning the data and analytics platform first, then defining the release plan and road map.

¹⁰ An entity's technology landscape includes the entity's IT environment in which they directly operate, any direct interactions with the entity's third-party service providers, and other technology considerations outside of the entity (e.g., global security issues, competitor IT initiatives, and new technologies).

- Develops the metrics for monitoring data activities to meet customer needs, not just performance related to projects or programs.

II.B.1(c) *IT Operations Management*

IT operations management is responsible for overseeing the IT environment, including performing and administering the day-to-day technology operations, security, and resilience. It is responsible for managing the capacity, performance (e.g., speed and flow of data), and availability of the components used in an entity's infrastructure, including hardware, networks and telecommunications, software, and storage. Whether centralized or decentralized, IT operations management should support line-of-business and functional operations by facilitating enterprise information systems reporting, product and service development, service delivery, and transaction processing.

II.B.2 IT Operations Personnel Responsibilities

IT operations personnel are responsible for the day-to-day operating and maintenance of the infrastructure components to support the entity's business operations. The following are some examples of their responsibilities and functions:

- Network infrastructure management
 - Network and connectivity for internal and external communication.
 - Remote access.
 - Internal and external telecommunications management.
 - Port management.
 - Network monitoring and issue resolution.
- Server and device management
 - Servers (on premises and off premises).
 - Storage solutions.
 - Entity-supported devices (e.g., desktops, laptops, and mobile devices) and personally owned devices (e.g., mobile devices and personal assistants) where used.
- IT environment management
 - Facility management, including data centers and connectivity to third-party service providers.
 - Help desk management.
 - Identity and access management (IAM).
 - Backup and replication management.
 - Configuration management.
 - IT environment resilience.
 - Cyber and information security.
 - IT project management.

The following are examples of common titles, roles, and responsibilities within IT operations:

- **Database administrator (DBA):** An individual or department responsible for the maintenance of security and information classification of the data stored on a database

system(s). This responsibility includes the design, build, maintenance, and performance tuning of the database. DBAs use specialized software tools to store and organize data to support the entity's business needs.

- **Systems analyst:** An IT professional who coordinates with stakeholders to promote the effective and efficient functioning of infrastructure. Systems analysts research problems, develop solutions, and recommend appropriate courses of action. Systems analysts serve as translators between business and IT personnel by communicating each stakeholder's requirements and constraints. Systems analysts use their knowledge of the entity's computer systems, procedures, and technology needs to help IT personnel design systems that support the enterprise-wide business and strategic plan objectives. They may manage projects or assist with activities related to third-party service providers.
- **Client support specialist:** An individual who assists employees, clients or customers, and third parties. Client support specialists use computer software and equipment to facilitate business needs and troubleshoot software and hardware issues. Client support specialists may also be referred to as user support specialists or "help desk" depending on the type of users they assist. In entities with a service management function, the role of the client support specialist may be carried out by service request or problem management personnel.
- **Systems administrator:** An individual or group responsible for overseeing the day-to-day operability of a computer system or network. Systems administrators install and maintain information systems, support effective system utilization, and implement policies, procedures, and security controls.
- **Network administrator:** Manages a network within an organization. Responsibilities include network security, software installation, distribution of software upgrades, daily activity monitoring, enforcement of licensing agreements, development of a storage management program, and performance of routine backups. Network administrators may design and analyze network infrastructures and make decisions regarding hardware and software upgrades.

II.C Policies, Standards, and Procedures

Management should document and maintain policies, standards, and procedures related to AIO. Smaller or less complex entities may have one policy and related procedures that encompass AIO, while larger or more complex entities may have multiple policies, standards, and procedures covering various aspects of AIO or various divisions or departments. Regardless of the entity's size and complexity, management should implement policies, standards, and procedures that address scope, responsibilities, accountability, authority, and guidance to develop and maintain effective processes related to AIO. With respect to AIO, documentation should include the following:

- Policies¹¹ that provide the guiding principles by which an organization designs, builds, and operates its information and technology assets and set the foundation for meeting the entity's objectives. For example, an entity may have policies outlining the types of hardware or software it will or will not use (e.g., "We will not use any unapproved software.").

¹¹ The [National Institute of Standards and Technology's \(NIST\) Glossary](#) defines policies as statements, rules, or assertions that specify the correct or expected behavior of an entity.

- Standards¹² that build on the policies and provide more granular information for AIO activities. For example, standards may explain the types of data that are allowed to reside in the cloud or the types of controls to be implemented to mitigate the risks of data residing in the cloud.
- Procedures¹³ that describe the specific ways for personnel to perform AIO activities. For example, AIO-related procedures may cover topics including how to harden new systems or perform architecture reviews with the necessary steps for personnel to follow.

II.D Internal Audit, Independent Reviews, and Certification Processes

Action Summary

The board and senior management should engage internal audit or other independent personnel or third parties to review AIO functions and activities and validate effectiveness of controls. Effective AIO auditing assists the board and senior management with oversight, helps verify compliance with applicable laws and regulations, and helps ensure adherence to contractual agreements and entity policies, standards, and procedures to mitigate risks.

Examiners should review for the following:

- Independence of AIO-related audits or other reviews.
- Appropriate scope and detail of AIO-related audits or other reviews.
- Applicable reporting of the AIO-related audit results to the board.
- Evaluation of third-party service providers' AIO-related audit or review reports.
- Qualifications of auditors reviewing AIO functions and activities.

The board and senior management should engage audit or use other independent reviews to assess the AIO design, implementation, and operational effectiveness, including the adequacy of policies and procedures and the effectiveness of controls. In many cases, the review of AIO functions and activities will be included within other audits. Audit should review the entity's AIO functions and activities and management's ability to oversee and control risks related to those functions and activities. Auditors should be qualified and knowledgeable to review AIO functions and activities. For example, if an entity uses cloud environments, the auditor should have training and experience reviewing cloud infrastructures. Auditors should be independent of the AIO functions and activities being reviewed. Audit scope and frequency depend on the complexity of the AIO functions and activities; the entity's risk profile; and design,

¹² The [NIST Glossary](#) defines standards as rules, conditions, or requirements that describe the following information for products, systems, services, or practices: (1) classification of components, (2) specification of materials, performance, or operations, or (3) delineation of procedures.

¹³ The [ISACA Glossary](#) defines a procedure as a document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.

implementation, and operational changes that the entity may experience. Larger or more complex entities may have multiple audits covering various departments or aspects of AIO functions and activities. Smaller or less complex entities may include a review of AIO within an IT general controls audit.

Audit or independent review reports to the board and senior management should provide an independent assessment of management's ability to oversee the entity's AIO functions and activities. For example, as part of their assessment, auditors or reviewers should perform the following:

- Evaluate supporting documents demonstrating that management has based AIO decisions on the entity's business strategy, security, and resilience needs.
- Leverage system and organization controls (SOC)¹⁴ reports and other external audit reports for the entity's third-party service providers to evaluate potential risks to the entity, such as interconnectivity and supply chain risks.
- Identify and report AIO issues to senior management and the board.

Some entities may choose to achieve an external certification (e.g., International Organization for Standardization [ISO] or Payment Card Industry Data Security Standard [PCI DSS]) to demonstrate the effectiveness of controls. These certifications can be reviewed along with audit reports or other independent reviews. Certifications are often a point-in-time assessment, however, and do not replace audit reports.

II.E Communication

Effective communication helps ensure that key issues are understood across the entity, objectives are received and acknowledged by management and staff, and everyone understands his or her role. Effective communication of AIO concepts is critical to bridge discussions and decision-making between technical staff and management. The significance of IT, in terms of investment and potential impact on the entity's business operations, highlights the importance of communicating the risks associated with IT and progress of IT strategic initiatives. Management is responsible for communicating relevant AIO information (e.g., disruptions, initiatives progress, or issue status) to the entity's staff, applicable customers, and third parties.

II.F Board and Senior Management Reporting

Management should report to the board periodically on the status of AIO-related initiatives, progress, issues, and metrics. The board should regularly monitor strategy, security, and resilience activities to verify that they are implemented as envisioned and reviewed (periodically

¹⁴ "In 2017, the [American Institute of Certified Public Accountants (AICPA)]...introduced the term system and organization controls (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization and system or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the AICPA enables the introduction of new internal control examinations that may be performed (a) for other types of organizations, in addition to service organizations, and (b) on either system-level or entity-level controls of such organizations." (AICPA, [SOC 2 Examinations and SOC for Cybersecurity Examinations: Understanding the Key Distinctions.](#))

and as changes occur). Board minutes should reflect significant AIO-related discussions, including credible challenges and approvals.

A fundamental element for reporting includes setting baseline metrics against which management can measure performance and risks. Developing, implementing, and monitoring metrics for AIO functions and activities are key for evaluating progress toward achieving strategic goals and business objectives. Common metrics reported to senior management and the board help to identify the following:

- Performance of IT and AIO activities.
- Return on investment for IT.
- Anomalies.
- Areas for improvement (e.g., cost, system, process, or service) providing opportunities for AIO.

III COMMON AIO RISK MANAGEMENT TOPICS

IT systems are designed, built, and implemented to achieve strategic goals and business objectives. While there are risks specific to each of the AIO functions, certain risks are common to all three. Common AIO risk management topics are discussed in the following sections:

- Data governance and data management.
- ITAM.
- Business and IT environment representation.
- Managing change in AIO and change management.
- Oversight of third-party service providers.
- Resilience.
- Remote access.
- Personally owned devices.
- File exchange.

III.B Data Governance and Data Management

Action Summary

Management should promote a culture that takes a data-centric approach for AIO functions and define responsibility and controls as part of data governance and data management processes.

Examiners should review for the following:

- Data identification and classification processes.
- Data management controls for safeguarding data in physical and digital form.
- Effectiveness of processes for monitoring new and existing databases, noncompliant or misconfigured databases, and changes to the databases.
- Effectiveness of processes for securing databases, analytics tools, and reports.
- Processes for controlling non-masked data in non-production environments.
- Processes for patching databases and monitoring whether the patch level of the production database is up to date.

The AIO functions are critical to planning for and implementing IT activities to meet business needs for one of the entity's most critical and valuable assets—data. Management should, therefore, govern and manage data based on the entity-assigned data classification described in the [“Data Identification and Classification”](#) section of this booklet.

Data governance and data management are fundamental to maintaining the confidentiality, integrity, and availability of information. Data governance is a set of processes for formally managing data assets throughout the entity. It establishes authority, management, and decision-making parameters related to the data that the entity produces or manages. Additionally, data governance involves the process for setting and enforcing the business and IT priorities for managing data.¹⁵ The data management process involves the development and execution of policies, standards, and procedures to acquire, validate, store, protect, and process data. Effective data management ensures that the required data are accessible, reliable, and timely to meet user needs. When data are no longer used, management should have a process for the data's removal or destruction and validate the effectiveness of that process.

In larger or more complex entities, data governance and data management are formally managed with defined responsibilities and functions. In smaller or less complex entities, these functions may be included in the responsibilities of a business line manager. Regardless of the entity's size or complexity, business line management, which generally is the most knowledgeable about the entity's data usage, should be consulted to assist in data classification, the development of recovery standards, and control validation by personnel responsible for these activities. Management should define responsibilities and processes for governing data, including the identification, management, and oversight of any metadata. Someone may be able to infer sensitive information from the metadata that could lead to misuse of the information. For example, third-party service providers could sell the metadata, providing an unauthorized individual with information about the entity's customers or business strategies. This could increase legal risks because the metadata could be used to compromise (e.g., through social engineering) the entity or its customers.

Effective data management continuously evolves as the entity grows or transforms to meet business objectives. Management should promote a culture that takes a data-centric approach, including for AIO functions.

III.B.1 Data Identification and Classification

Data identification and data classification are important components of data management. To effectively manage data, it is important to identify what data the entity has, particularly to identify sensitive customer and entity information. The data identification process includes structured data, managed by a system of record, as well as unstructured data (e.g., physical loan files, emails, documents, images, presentations, or free-form text comment fields in applications) created or processed by end users. There are inventory tools available to assist management with the data identification process. Once the data is accurately identified, it should be appropriately classified.

¹⁵ Refer to the U.S. Department of the Treasury's [Data Governance Board Charter](#).

Data classification is the process of categorizing data based on the expected damage to operations following loss or compromise of the identified information. Classification is based on its level of confidentiality (i.e., sensitivity), integrity, and availability, as well as the value and criticality to the entity. Management should identify and understand the nature of the entity's data to classify it effectively, including the following:

- Sensitivity, criticality, and importance of the data for the entity, its business units, or its customers on a day-to-day basis.
- Frequency, recurrence, and use of data by the entity and its business lines.
- Format in which data are maintained (e.g., database, online files, or paper copies).

Management should use the results of the data classification process for implementing controls to safeguard data, whether in physical (e.g., paper and storage media) or digital form. Management should understand where data reside and maintain the effectiveness of controls over those data, including controls over databases. Management should regularly update the information and technology asset inventory (described in the [“IT Asset Management”](#) section of this booklet) for new assets (e.g., data, hardware, systems and software, and databases) regardless of whether the asset and its data are maintained in-house or by a third-party service provider. For more information, refer to the *IT Handbook's* [“Information Security”](#) booklet.

III.B.2 Database Management

When evaluating AIO, it is important to evaluate database management. Databases are used to store data so that they can be organized, easily accessed, effectively managed, and readily updated. Often, an entity's data are stored in databases and accessed or used by software. Databases can exist on mainframes, within internal networks, in a cloud environment, and on standalone computers.

Databases typically contain critical and sensitive data, including customer account data. Therefore, databases pose unique risks (e.g., data corruption, data misuse, data errors, or unauthorized changes). For that reason, securely designing, building, and operating databases are important to protecting the data itself. Management should implement a process to adequately secure and oversee the entity's databases to minimize the potential for unintentional or unauthorized modification, destruction, or disclosure of sensitive customer or entity information.

As part of understanding where data reside, management should ascertain the effectiveness of database controls, and assign appropriate staff to update the data and technology inventories. Management should determine whether databases are appropriately located and structured, have sufficient capacity, and are resilient. Management should regularly monitor for new databases or significant changes (including data loss) to existing database(s) and report on misconfigured databases or those that are out of compliance with the entity's configuration standards.

Databases are also an important building block used to construct information for use by business lines, customers, third-party service providers, and partners (e.g., joint ventures). It is important to understand how databases interconnect throughout the entity when developing an architectural design and selecting appropriate infrastructure.

In addition to databases, there are other methods (e.g., data warehouse, database server, tape, and paper) and formats (e.g., structured data and unstructured data) for storing data when considering database management control implementation. Regardless of how the data are stored, the focus should be on identifying, managing, and securing the data as well as identifying business uses for the data and providing access to authorized lines of business.

Responsibilities for database management controls typically are managed by a DBA; however, in smaller or less complex entities, these responsibilities may be assigned to other personnel. A DBA is typically responsible for database configuration, including security configuration, access controls, and maintenance, as well as training employees on databases. Additionally, this individual monitors the databases and maintains awareness of normal operations. A DBA should work with the information security officer to strengthen database security.

A DBA should monitor for anomalous database activities, which could indicate errors or fraud. For example, delays in response time for user queries may indicate the presence of malware or corrupted data. In preparation for such a scenario, the DBA should be familiar with procedures to protect sensitive information, restore normal operations, and notify the information security officer. As DBAs have highly privileged access to databases, use of accounts belonging to DBAs should be limited and independently monitored.

III.A.2(a) *Database Security*

Databases often store sensitive information; therefore, they are frequent targets of malicious activity by internal and external sources. As part of database management activities, management should implement effective database security controls. Examples of database security controls include the following:

- Change passwords for default user accounts and, subsequently, disable or delete those accounts when possible.
- Track and monitor activity for default accounts that cannot be disabled or deleted.¹⁶
- Restrict account access (e.g., to view or modify data, to modify the database or data structure, and to change access rights) and limit privileges and permissions to only those necessary to carry out job responsibilities and automated functions.
- Implement password management tools or activities (e.g., password changes after a determined time frame, vaulting of system-level passwords, and use of password complexity rules).
- Employ an appropriate level of encryption on data in transit and data at rest based on the type and criticality of the information according to the entity's data classification policy.
- Configure and review audit logs (e.g., configuration settings, access control, and log review processes).

¹⁶ Default accounts often come with the hardware, software, databases, or operating systems. While it is a good practice to disable or delete these accounts, at times system-level default accounts cannot be deleted without affecting the system functionality. In such cases, default passwords on the account should be changed and any activity performed by those accounts monitored.

- Regularly monitor database activity logs to track account access and activity, including activity that modifies sensitive information and alters the database security parameters or structure (e.g., modifying or deleting database tables or connections).
- Independently monitor DBA and privileged account activities (e.g., use of or changes to system privileges).
- Classify data maintained within the database.
- Restrict and monitor data extraction (e.g., limiting and monitoring data queries, user abilities, and the use of standardized business intelligence tools¹⁷ to query databases to provide standardized reporting).
- Implement and adhere to patch management processes to maintain a current and secure database and underlying operating system (OS).
- Implement OS controls (e.g., configuration settings and access control).
- Monitor OS-level privileged account activities.
- Manage application-level access (e.g., access by and through applications).

The DBA may use automated tools to help implement controls and monitor the database environment. These tools include database discovery, security scanning, configuration lockdown, automated remediation, and security reporting. For more information, refer to the *IT Handbook's* "[Information Security](#)" booklet.

III.B.3 Non-Production Environments

Entities often have environments beyond the production environment. This allows management to make changes and perform testing in a way that does not impact the entity's production environment. For example, entities that develop their own software often have multiple environments to support their development processes. These non-production environments, commonly used for development, testing (either for testing changes or exploring the feasibility of potential new technologies, products, and services), or quality assurance, provide alternate information processing environments; allowing an entity to develop and test system changes without impacting production. While production environments pose significant risks to the entity and its customer information, non-production environments are not without risks. These risks include:

- **Privacy and misuse of data.** Entities sometimes copy production data into non-production environments, potentially allowing individuals to access information beyond what is needed for their job description.
- **Security tradeoffs.** To facilitate rapid changes or for development and testing of functionality, management may disable or omit security.
- **Data corruption.** Stale or incorrect data may inadvertently corrupt production data if non-production data are not appropriately segregated from production data.
- **Transition to production.** Failure to enable production levels of security may introduce vulnerabilities into the production environment.

¹⁷ Business intelligence tools can be used to help management gather and analyze its data (e.g., transactions that match fraudulent activity patterns) and can expand the entity's attack surface because of their access to an entity's databases.

- **Secondary use.** At times, non-production environments or data may be used for other than their intended purposes (e.g., training), which could expose sensitive data unnecessarily. Additionally, data used may not be appropriately secured.
- **Data breach.** If non-production environments are not properly secured, malicious actors may gain access and use that access as a conduit into production environments. Additionally, malicious actors may be able to access sensitive data contained within non-production environments.

Management should consider design, placement, and effective security controls for non-production environments. Non-production environments should be independent of production environments to maintain data integrity and resilience. Management should use simulated synthetic data in non-production environments when possible. When production data must be used for testing, it should be masked, or sanitized whenever feasible. In cases where masking data is not feasible, management should require approval by the appropriate level and implement controls similar to those used in production environments. Controls could include IAM, password controls, and logging and monitoring of activity within non-production environments. For more information, refer to the *IT Handbook's* "[Information Security](#)" booklet.

III.B.4 Data Analytics

Data analytics is the process of evaluating and organizing data sets to draw conclusions, make predictions, and reveal trends. The results of data analytics may be used to improve decision-making, optimize processes, and increase efficiency. Data analytics can help management discover hidden patterns, correlations, security threats, trends, customer preferences, and other useful business information. Management should consider the uses and risks of data analytics. While management may use data analytics to make business decisions (e.g., introducing a new product or analyzing security logs), data analytics reports could expose sensitive data. Therefore, management should limit access to analytics tools and related outputs and incorporate confidentiality, integrity, and availability when designing or selecting analytics tools. Management also should inventory the data sources, assess the information type according to the entity's data classification policy, and appropriately secure those sources according to the data's risk classification.

Management should develop design requirements and parameters for analytics. Data analytics results can be produced as dashboards and reports, which may be available on demand. Management and personnel using data analytics should have sufficient knowledge to interpret dashboards and reports. Insufficient dashboards or reports, or incomplete data, can lead to a misunderstanding or misuse of the data in decision-making processes. Management should consider the following when implementing and using data analytics:

- Document the types of data maintained, data owners and users, and purpose for reports.
- Determine usage needs by stakeholders (e.g., internal personnel and customers) and the ability of analytics reports to meet them.
- Determine whether there are opt-in considerations based on the information type in the analytics reports.
- Determine disclosure requirements (e.g., to regulatory agencies, internal stakeholders, and customers) in the event of a security incident.

- Implement access controls and activity monitoring over analytics tools and reports.
- Define processes to remove or destroy data when no longer used in the data analytics tools.
- Identify data that are subject to applicable laws and regulations (e.g., “Interagency Guidelines Establishing Information Security Standards” [Information Security Standards],¹⁸ the Fair Credit Reporting Act, and the Equal Credit Opportunity Act) or other relevant industry standards (e.g., PCI DSS).
- Identify data analytics processes used by the entity to comply with applicable laws and regulations (e.g., Bank Secrecy Act/anti-money laundering, the Office of Foreign Assets Control, or the Sarbanes–Oxley Act [SOX]).

According to the National Institute of Standards and Technology (NIST), the growth of data is outpacing the abilities of current data analytics systems to process the data.¹⁹ This exponential growth of data has produced larger and more varied pools of data, often referred to as big data,²⁰ which need to be analyzed more rapidly.

Big data can be mined for information and is notable for the volume of data (including large amounts of sensitive customer information), the speed at which the data is processed, the variation in data types, or the variability (e.g., the change to a data set’s data flow rate, format, or volume). Specialized tools and software have enabled complex and high-volume data analytics, especially for big data. Risks associated with big data include unintended uses of information or patterns (specifically with sensitive customer and entity information); concerns with the maintenance, use, and protection of sensitive customer and entity information; third-party access to data; and compliance risks. As part of its mitigation strategy, management should implement appropriate security policies, standards, and procedures, along with data access and security controls in accordance with the entity’s data classification policy. Refer to the *IT Handbook’s* “[Information Security](#)” booklet for more information.

¹⁸ Refer to 12 CFR 30, appendix B (OCC); 12 CFR 208, appendix D-2 and 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA) (collectively referenced in this booklet as the Information Security Standards).

¹⁹ [NIST Big Data Interoperability Framework: Volume 1, Definitions.](#)

²⁰ [Ibid.](#)

III.C IT Asset Management

Action Summary

Management should have appropriate ITAM processes to track, manage, and report on the entity's information and technology assets.

Examiners should review for the following:

- Policies, standards, and procedures.
- Technology asset inventories.
 - Hardware inventory, including telecommunications.
 - Software inventory.
- Processes to address IT asset EOL.
- Processes to prevent and detect unknown or unapproved technology (called shadow IT).

ITAM is the process to track, manage, and report on information and technology assets²¹ throughout their entire life cycle. ITAM plays a significant role in the AIO functions, demonstrated by the following examples. In architecture, if management is aware of the entity's current inventories, it can determine the necessary design changes to meet strategic goals and objectives. For infrastructure, ITAM allows management to acquire hardware or software components that are interoperable with the entity's existing infrastructure. With respect to operations, the ITAM inventories help management know what systems need to be patched and the patch time frames, what hardware or software is nearing its EOL, where the entity's vulnerability management focus should be, or when any additional security measures are necessary.

Management should have a comprehensive inventory of its electronic (or digital) and physical information assets to adequately safeguard them against reasonably foreseeable threats. An inventory will assist management as it develops and maintains the entity's information security program as described in the Information Security Standards.²² As part of the entity's information and technology asset inventory, management should specifically identify the entity's information assets, determine the assets' appropriate classification, and protect the assets according to the

²¹ Information and technology assets can include hardware, software, mobile devices, virtual and cloud assets, physical assets (e.g., cabinets, locks, and hard copy information assets), digital information assets (e.g., data), and third-party managed assets.

²² Refer to 12 CFR 30, appendix B (OCC); 12 CFR 208, appendix D-2 and 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA). Section III.C of the Information Security Standards requires each financial institution to have a comprehensive written information security program designed to manage and control risk where each institution shall design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities. Each institution must consider whether the security measures set forth in III.C.1 are appropriate for the institution.

entity's data classification process. Refer to the *IT Handbook's* "[Information Security](#)" booklet for more information on methods for safeguarding sensitive customer information.

Management should implement policies, standards, and procedures to govern all aspects of ITAM, including information and technology assets. The ITAM process includes identifying the technology assets that the entity possesses and manages, determining each asset's status (e.g., active or inactive), and identifying the life cycle phase of those assets. Management should regularly review and validate the accuracy of the inventories. The ITAM process also includes identifying personally owned technology assets that are allowed to connect to the entity's network, with considerations such as the design, implementation, and controls over the assets' use. Management may use ITAM to help make informed, business-driven decisions for entity-owned and personally owned IT assets.

The inventories help management identify or understand the following aspects of ITAM:

- License utilization.
- Support costs related to maintenance, utilization, and obsolescence.
- Existence of unauthorized devices operating on the entity's networks.
- Potential vulnerabilities, such as hardware and software that are in need of upgrade or are reaching EOL.
- Compliance with internal configuration and security standards, as well as contractual requirements.
- Critical interdependencies (e.g., third-party service providers, software, hardware, and business units).

As part of ITAM, management should use appropriate inventory mechanisms to track and validate the entity's information and technology assets. Smaller or less complex entities may use informal methods (e.g., spreadsheets) to track IT assets. Larger or more complex entities may use more sophisticated methods or automated tools to assist with ITAM. Automated tools can provide a variety of functionality, such as logging and vital asset statistics. Some automated tools alert management when a new or unapproved device is connected to the entity's network. Because automated inventory methods or tools may not identify all IT assets that connect to the network, management may need to manually inventory those types of devices (e.g., internet of things [IoT] devices).

III.C.2 Technology Asset Inventory

Building technology asset inventories is a foundational process that management uses to identify entity-owned IT assets. The inventories should include information regarding the entity's hardware, software, and telecommunications. Management also should consider IT assets that do not fall into traditional hardware or software inventories, such as internet assets (e.g., website addresses owned, certificates employed, domains used, or rights to audio or video files). Smaller or less complex entities may have one comprehensive inventory that contains all of its technology assets. Larger or more complex entities may have multiple inventories to track their technology assets. Management can leverage the technology asset inventories for the following purposes:

- Supporting the entity's risk assessments (e.g., information security, SOX, continuity and resilience, or business unit).
- Evaluating the design of the infrastructure and IT environment supporting business processes.
- Identifying potential security weaknesses (e.g., assets reaching EOL or operating on outdated versions of software).
- Managing vulnerabilities by identifying necessary versions and patch levels for continuity of operations.
- Aligning with strategic planning (e.g., acquiring specific technology for current and future business needs).
- Assisting in audit risk assessments and building the audit universe and scope.

There are tools that may help management identify and manage hardware (including telecommunications) and software in the entity's IT environment. For example, automated asset management tools can scan an entity's IT environment for unauthorized hardware, software, and devices (sometimes called shadow IT). Smaller or less complex entities may use manual asset inventory processes; these processes, however, should allow management to effectively document, track, and oversee the entity's technology assets.

ITAM policies, standards, and procedures should outline a process to update the technology inventories after changes to IT infrastructure or operations. All inventories should be periodically reviewed to verify that they accurately capture the entity's technology assets.

III.B.1(a) *Hardware Inventory*

Management should maintain a hardware²³ inventory that identifies the entity's hardware assets. The hardware inventory should identify equipment owned and managed by third parties on the entity's behalf that may be located within the entity's environment (e.g., wire transfer routers, core processing hardware, and third-party security monitoring devices). The hardware inventory should include entity-owned and entity-managed virtual infrastructures (e.g., virtual servers on the entity's premises or virtual servers in a cloud environment). To the extent possible, hardware items should be assigned a unique identifier (e.g., labels or bar codes) to allow management to identify, account for, and monitor for changes to hardware assets.

The entity's hardware inventory should contain information about the entity's network and telecommunications equipment. The information includes the type, use, and configuration of the equipment and related software that provides internal and external network connections.

The following are examples of information to include in the hardware inventory:

- Vendor and model.
- OS version or release level.
- Function or use.

²³ For the purposes of this booklet, hardware includes devices, mainframes, servers, storage equipment, desktops, and printers.

- Status (e.g., active, nearing EOL, or decommissioned).
- Memory and storage size.
- Processor speed.
- Owner or contact information.
- Network connectivity.
- Physical location.
- Identifiers (e.g., internet protocol [IP] address and media access control [MAC] address).
- Criticality classification.
- Upstream and downstream connections.
- Environment (e.g., production, test, or development).
- Firmware version.
- Most recent maintenance date.
- EOL date, if applicable.
- Network and telecommunications equipment, including:
 - Routers.
 - Firewalls.
 - Intrusion detection and prevention systems (IDS/IPS).
 - Virtual private networks (VPN).
 - Telecommunication lines.
 - Provider.

In addition to hardware, additional information should be considered when evaluating the network (e.g., network segments and associated attributes, such as IP addresses, domains, network protocols, and third-party network contractual arrangements) and these can also tie to the entity's software inventory.

III.B.1(b) *Software Inventory*

Similar to a hardware inventory, management should maintain an accurate software inventory. The software inventory provides detailed information on software used within the entity's IT environment. The following are examples of information to include in the software inventory:

- Application or database name and type (e.g., general ledger or payroll).
- Developer (e.g., developer name or internally developed).
- Vendor name, if not the developer.
- Install date.
- License renewal date.
- EOL (e.g., end-of-support) date and expected software life, if applicable.
- Serial number.
- Version.
- Patch level.
- Last patch date.
- Number of copies, licenses, and users allowed, if applicable.
- Environment where software runs (e.g., production, test, or development).
- Owner or contact information.

- Internally run or hosted at a third-party service provider and where, if applicable.
- Criticality based on the software assessment (e.g., line of business use, interconnectivity, and recovery priority).
- Data classification based on data type (e.g., sensitive customer or entity information).
- Physical or virtual location.

III.C.3 IT Asset End-of-Life

With respect to technology, EOL is a time frame usually defined by a technology vendor to describe when an asset has reached the end of its useful life cycle or when the vendor will no longer support the asset or continue to sell or license it. All technology, including hardware, software, and assets in the cloud, has an asset life cycle. NIST states that an asset's typical life cycle²⁴ includes enrollment, operation, and EOL phases. Each IT asset should be captured in the entity's ITAM inventory, tracked throughout its operational life to monitor for changes (e.g., vendor announcements regarding support or changes in functionality, reliability, or processing speed) in the asset or the changing needs of the entity, and prepared for physical removal at the end of its useful life. Management should implement policies, standards, and procedures to identify assets and their EOL time frames, to track assets' EOLs, and to replace, or upgrade, the asset. Failure to maintain effective identification, tracking, and replacement processes could have operational or security implications (e.g., unavailable or unapplied security updates [patches] that make technology vulnerable to disruption).

EOL for hardware (e.g., servers, routers, and cables) refers to the end of its useful life when the hardware is no longer capable of supporting the entity's strategic objectives. Hardware EOL may be due to issues such as wear and tear, capacity or speed issues, or obsolescence of hardware components. Alternatively, software EOL refers to the time frame when a software development company no longer provides automatic fixes, updates, or software support for the product (e.g., OS or application software). Management should address EOL in contract provisions with its third-party service providers. For more information on contract provisions, refer to the *IT Handbook's* "[Outsourcing Technology Services](#)" booklet.

With respect to existing technology, effective EOL management should include the following:

- Adding assets to the information and technology inventories and tracking changes made to assets.
- Conducting risk assessments to help determine the EOLs of existing assets.
- Reviewing EOL time frames for existing assets to determine accuracy and relevance.
- Developing replacement plans for assets nearing obsolescence.
- Establishing procedures for the secure destruction or data wiping of hardware (e.g., hard drives; copy machines; servers, desktops, and laptops; or mobile devices) and software (e.g., databases) to prevent the inadvertent disclosure of sensitive information.

For new technology assets, effective EOL management should include the following:

²⁴ Refer to NIST Special Publication (SP) 1800-5, [IT Asset Management](#).

- Incorporating EOL considerations in strategic planning.
- Planning for obsolescence during initial project stages (e.g., during requests for proposals or proofs of concept).
- Registering and tracking assets in the information and technology asset inventories, including available EOL information.
- Developing plans for maintaining operational viability and security of IT assets beyond EOL, if necessary.

III.C.4 Shadow IT

Shadow IT refers to IT devices, software, or services operating within the entity's environment without the knowledge, approval, or control of IT management. Shadow IT can also be identified within a third-party service provider's environment. Unapproved devices, software, or services should not be running at the entity, but they could be placed there by the following:

- Business units to support their specific needs in contravention to the enterprise's needs.
- Third-party service providers to support services provided to the entity or to collect data for the service providers.
- Individuals (internal or external) for convenience to allow them to use entity resources (e.g., wireless network) or for malicious purposes (e.g., to steal data or processing power).
- Incomplete decommissioning process for legacy systems (e.g., business unit systems that were never decommissioned because of software compatibility limitations).

Failure to address the risks of shadow IT may lead to an unknown attack vector due to management's lack of awareness of unapproved devices, software, or services. Therefore, management should understand and communicate the following risks of shadow IT to the entity's personnel:

- Security weaknesses, data breaches, or data loss from using unapproved devices, software, or services.
- Inability to maintain or update (e.g., apply patches to) unknown devices or software resulting in vulnerable devices or software.
- Costs related to identifying, diagnosing, and mitigating security issues.
- Inability to back up and recover unknown devices or software.
- Unintentionally performing automatic backups of unapproved and possibly infected devices or software leading to the spread of malware.
- Penalties for using software or services without a license.
- Legal risks related to data use or data ownership (e.g., data residing on devices outside of the ownership or control of the entity).
- Potential nullification of cyber insurance.

Management should establish IT governance practices and security controls along with consistent policies, standards, and procedures to mitigate risks of shadow IT. Security awareness training should include the risks of shadow IT and the rationale for preventing its use. Such

training may deter deployment of shadow IT, encourage personnel to notify management of its use, and inform personnel of notification procedures (e.g., how and when to notify).

Identification of shadow IT on an entity's network or systems often occurs through regular review of the network's assets, comparing the results of the review to approved assets on the inventories and diagrams. Using IT detection tools may allow management to monitor for and identify shadow IT (e.g., unauthorized IoT devices or rogue Wi-Fi connections). When connected to the cloud, software or hardware tools (e.g., cloud access security brokers) can be used to discover unknown applications. In addition, management should employ appropriate data protection and data loss prevention tools to minimize the potential for exfiltration or misuse of sensitive customer and entity information.

The identification of shadow IT does not eliminate it. Shadow IT remains until management appropriately addresses it. While shadow IT should be addressed in a timely manner, there is a risk that removing shadow IT could negatively affect a department process. The entity's product and service delivery and revenue stream could be affected if shadow IT is removed without an appropriate plan. Management should perform the following when determining appropriate methods to address shadow IT:

- Identify security risks associated with shadow IT in use and determine whether there is malicious intent.
- Identify the reason for use (e.g., compatibility issues or preference for specific device type).
- Determine the clients or processes shadow IT may be supporting.
- Verify interconnectivity with third-party service providers and integration with other entity software.
- Determine the appropriate disposition of shadow IT (e.g., remove or transition to entity-managed infrastructure and add to the ITAM process).
- Review policies, processes, and tools to understand any gaps that may allow shadow IT to occur.

Without appropriate identification of shadow IT, independent reviews (e.g., penetration tests, vulnerability assessments, or audits) may not be comprehensive. While audit processes typically do not identify shadow IT, internal audit should evaluate management's processes to monitor, identify, and remove unapproved devices, software, or services.

III.D IT and Business Environment Representations

Common types of documentation maintained to represent the entity's IT and business environments are network diagrams, data flow diagrams, business process flow diagrams, and business process narratives. Management should document and maintain accurate representations of the current IT and business environments and should employ processes to update representations after the implementation of significant changes. Representations may assist management by identifying the following:

- Physical and virtual technology assets (e.g., hardware and software), including locations, version and model numbers, and whether the assets are still supported.

- Information (digital and physical, as appropriate) assets (e.g., location and flow of sensitive customer information and data storage locations), including interdependencies of assets, data classification, owner designation, and environment details (e.g., production, test, or development).
- Hardware and connections for network maintenance, troubleshooting, and recovery from disruptions.
- Interconnectivity and process flows between and among the following:
 - Lines of business.
 - Entity and external parties (e.g., third-party service providers and customers).
 - Network access points (e.g., VPN connections).
 - Other devices.
- Points of internal or external connectivity that may need protection or additional controls that may be appropriate.
- Locations of sensitive data at rest and security points for data in transit.
- Potential for expansion (e.g., new technologies), reconfiguration, or removal of technology assets.
- Opportunities for business process improvements (e.g., incompatible business line process flows).

While various representations may be used for different purposes, management should coordinate the development of representations among stakeholders. This coordination allows management to obtain a holistic view of the entity's IT environment and understand how it supports business processes. The diagrams and narratives should be aligned with each other and across lines of business. For example, if the business flow diagram refers to a particular function, or application, other diagrams and narratives should use similar naming conventions to refer to that function for reference purposes.

Management should periodically review documented diagrams and narratives to verify the accuracy of the representations of the IT and business environments. Inaccurate information could result in incorrect decisions, which could lead to security vulnerabilities, maintenance issues, or recovery delays. Management should provide for the resilience of this documentation by maintaining current and accurate backups.

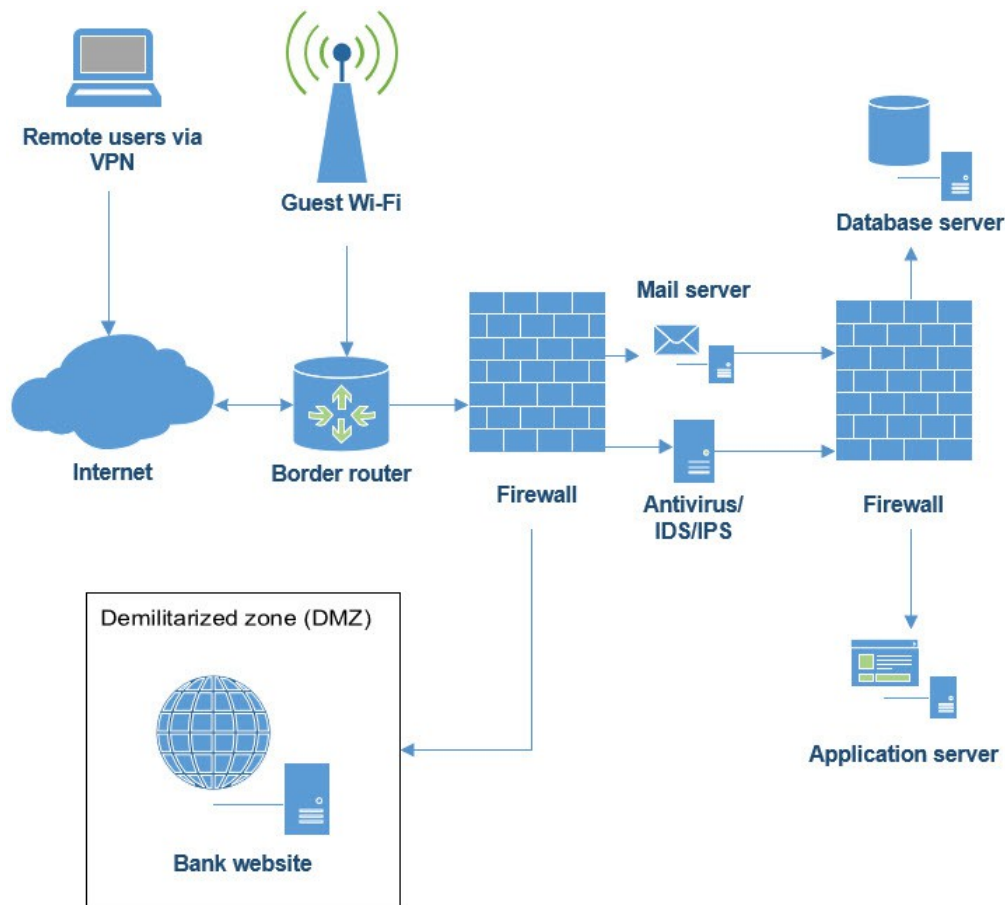
Management should appropriately restrict access and editing privileges to the representations due to the confidential or sensitive information they contain (e.g., IP addresses, location, or interconnectivity of network elements). Management should consider developing versions of the diagrams or narratives with only the information needed for entity and third-party service provider personnel to perform their duties.

For larger or more complex entities, manual documentation and monitoring processes may not be effective at identifying all pertinent information. Therefore, automated tools may be used to document and assist in the management of the IT and business environment.

III.D.2 Network Diagrams

A network diagram (also called a network map or network topology) is a visual representation of nodes and connections in a computer network. Figure 2 is an example of a network diagram. An entity's network diagram may include the following:

- Hardware (e.g., critical systems, routers and switches, and storage devices) and virtual components (e.g., virtual servers and cloud infrastructure).
- Internal and external connections (e.g., internet access, cloud access, remote access, and third-party access).
- Network segments and associated trust level (e.g., trusted, semi-trusted, untrusted, or restricted), including boundary protections.
- Bandwidth of connectivity within and between network segments.
- Infrastructure used to support specific business units.
- Geographical locations of infrastructure.
- Connectivity (e.g., fiber optic, multiprotocol label switching (also known as MPLS), VPN, dial-up, and wireless).
- Security elements (e.g., firewalls and IDS/IPS).
- IP addresses of specific infrastructure elements.
- Connection points for third-party service providers and customers.
- Encrypted or other secure communication channels.

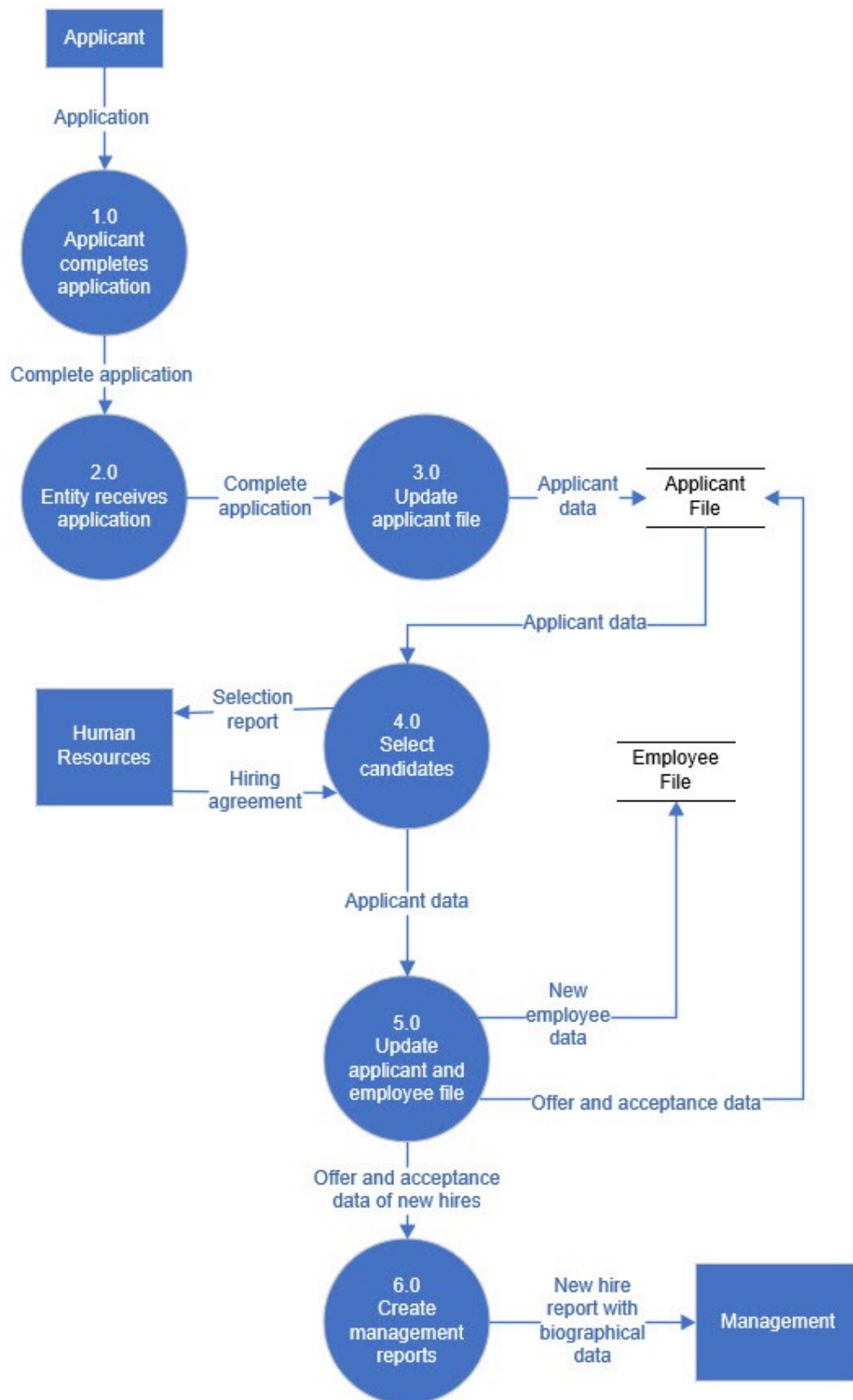
Figure 2. Example of a Network Diagram

Note: Figure 2 is for illustrative purposes only and shows components a network diagram may contain.

III.D.3 Data Flow Diagrams

A data flow diagram is a graphical representation of the flow of data internally through the entity's network(s), business units, products, and software, and to third parties, as applicable. (Refer to figure 3.) Data flow diagrams and network diagrams may include similar information (e.g., critical hardware) but have different purposes. Data flow diagrams show how the entity's data flows between critical hardware on the network, not just where a piece of hardware resides.

Figure 3. Example of a Data Flow Diagram



Note: Figure 3 is for illustrative purposes and does not show every step in the process.

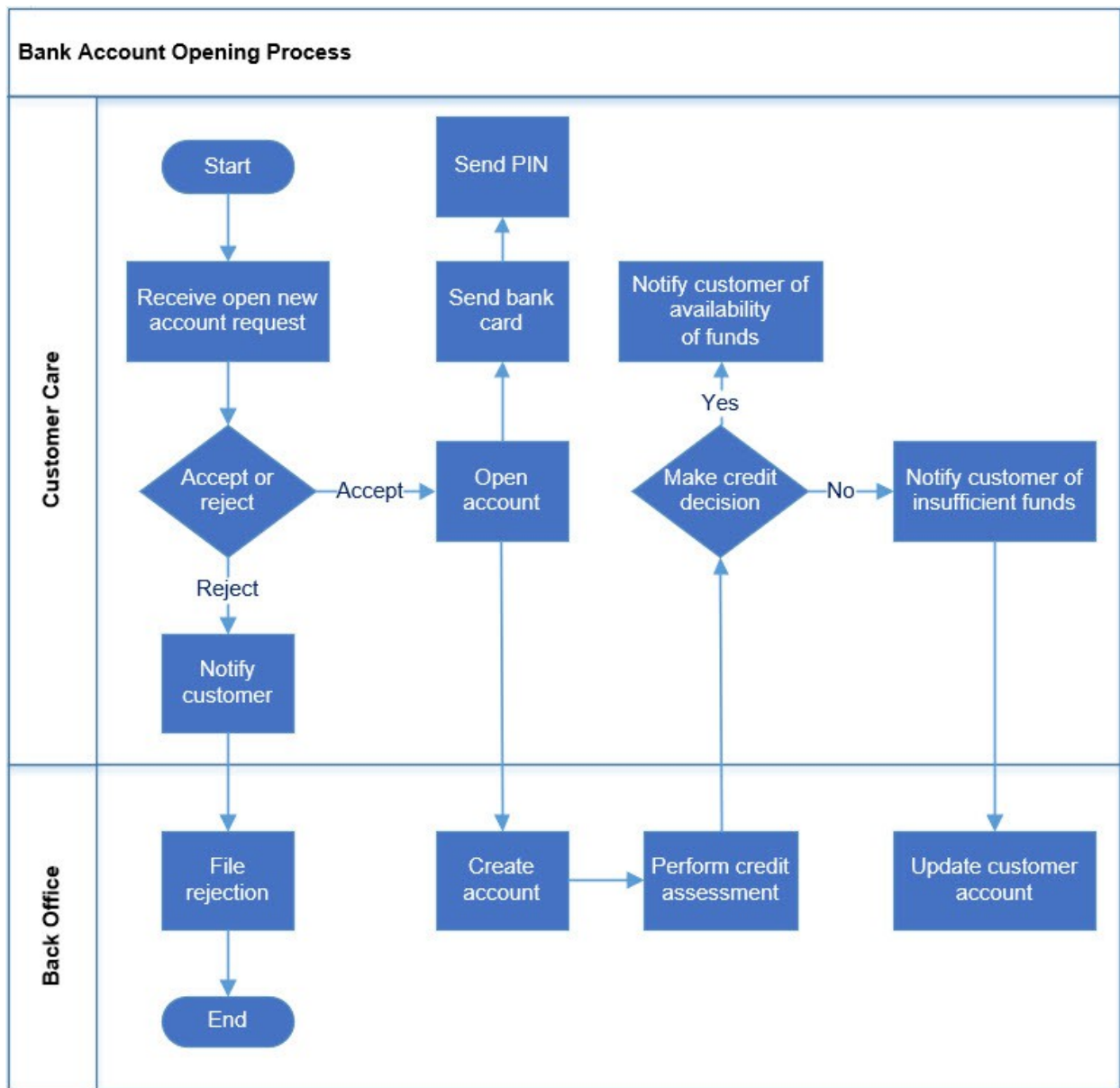
In smaller or less complex IT environments, data flow diagrams and network diagrams may be combined. In larger or more complex IT environments, the entity generally has multiple data flow diagrams and network diagrams broken out in a variety of ways (e.g., lines of business, geographic locations, network segments, and business functions). Data flow diagrams may include the following:

- Storage locations of data (i.e., data at rest), especially sensitive data, and where data flow between equipment and systems (i.e., data in transit).
- Data sharing between applications.
- References to network diagrams for details of internal and external connectivity.
- Specific operational or business processes and any single points of failure.
- Data flow within the entity (e.g., operational or business process interaction and interdependencies) and between the entity and its third-party service providers.

III.D.4 Business Process Diagrams and Narratives

Business process diagrams depict the relationships between an entity's business processes and control points, including interactions and interdependencies. The diagrams illustrate processes, functions, and decision points for a business activity, such as those depicted in figure 4. The diagrams often depict the handoff between departments that have a role in carrying out different parts of the business activity.

Figure 4. Example of Process Flow Diagram



Business process narratives, on the other hand, describe the entity’s business processes and related control points, often to support control reporting, such as for SOX or SOC reports. Business process narratives often align with and help provide additional information about business process diagrams and control objectives and may be useful for understanding how an entity’s business units function.

III.E Managing Change in AIO

An entity’s IT environment and its products and services, whether internally or externally provided, should be adaptable to change. Management generally makes changes to meet strategic goals and objectives (e.g., adding new products or services, growing the entity’s business,

providing integration and centralization of functionality, expanding to new geographic areas, or expanding operational capabilities) or to deliver financial, performance, or security improvements. Changes may be accomplished by implementing new technology (e.g., systems or software) to support new or changing products and services. Once management initiates changes, it relies on involvement from architecture for design, infrastructure to build, and operations to deploy the changes needed to meet the strategic goals. Depending on the type, complexity, and impact of the change, stakeholders across the entity should have input into the change process.

For complex changes (e.g., core conversions, migrations to cloud-based environments, or implementing a system to support a new product), formal planning and management oversight processes are warranted. For routine changes (e.g., implementation of patches), management may follow a less extensive process. Regardless of the type, management should ensure that changes to any IT system or service are supported by an orderly, adaptable, documented, and measurable process. Such a process can minimize risk, maintain the integrity and security of the entity's IT infrastructure, maintain or enhance the value to the business, and maintain uninterrupted delivery of the service. For more information on implementing technology changes, refer to the *IT Handbook's* "[Development and Acquisition](#)" booklet.

III.E.1 Change Management

Change management is the continuous process of maintaining the integrity of hardware, software, firmware, and documentation, and controlling and approving changes (e.g., addition, modification, or elimination) to information or technology assets or related infrastructure. Change management is an operational process that involves the implementation and management of changes to meet the strategic goals of the entity. Some changes to the IT environment may occur within the entity's infrastructure (e.g., hardware, software, and telecommunications), while others may involve third-party service providers (e.g., cloud or managed security service providers). While some change management activities may involve longer-term strategic planning and IT architecture, other changes, such as remediating vulnerabilities or responding to malicious events, may require more rapid action.

The entity's policies, standards, and procedures should address change management, including each step of the change process. Policies, standards, and procedures should categorize changes by severity, specify corresponding approval processes, and identify responsible staff, applicable stakeholder working groups, or entity committees. Management should identify metrics (e.g., implementation time, success rates, and the number of planned versus unplanned changes) to track the efficiency and success of the change management process.

An entity's change management process should ensure that changes are implemented with the goal of preserving the IT environment's confidentiality, integrity, and availability. Management should incorporate appropriate segregation of duties and monitoring throughout the change management process as outlined in the *IT Handbook's* "[Information Security](#)" and "[Development and Acquisition](#)" booklets. Ideally, the change management process consists of the following:

- **Request:** A documented request should outline the reasons for change (e.g., business justification) and include details of the change (e.g., system to be changed, impact analysis to identify risks and affected systems, change time frame, and back-out plan).
- **Review:** Management should review requests to determine viability and business practicality.²⁵ Requests may be prioritized during this stage or may be returned to the request originator for more information.
- **Approve:** There should be a documented hierarchy for approving change requests. Appropriate approval mechanisms²⁶ should be commensurate with the scope, cost, urgency, and overall risk to the entity and its IT environment.
- **Design and build:** Management should follow formal processes to preserve integrity throughout the development life cycle and ensure adequate controls (e.g., restrictions for moving code from staging to production).
- **Test:** Management should document that the change performs as intended, identify any flaws (e.g., integrity issues), and verify that the change integrates with other systems.
- **Implement:** Management should follow a formal process to deploy the change during off-peak hours or planned system outages.
- **Verify and close:** After deployment, management should perform a post-implementation review to verify that the change was implemented successfully and achieved performance objectives. After verification, management should follow processes to document the change's closure.

Changes can pose risks to the confidentiality, integrity, and availability of the entity's IT environment. Therefore, management should preserve systems' security throughout the change management process. Improperly tested changes or changes implemented without approvals or documentation may cause systems to crash, return unanticipated results, allow the insertion of malicious code, or make it difficult for management to troubleshoot future problems. To minimize these risks, management should have processes to implement changes based on the change type. Entities often have the following types of changes:²⁷

- **Planned changes:** These changes follow the entity's complete process, often using most of the steps outlined in the preceding bullets, thereby addressing risks (e.g., potential for errors, unintended impacts to interrelated systems, or business process issues related to the unavailability of critical systems).
- **Routine changes:** These changes (e.g., installation of patches) are generally performed frequently or regularly and follow standard procedures. They may be pre-approved.
- **Emergency changes:** For this type of change (e.g., to restore a failed hardware component, respond to an ongoing cyber event, or address a service interruption), certain components of the change management process may be truncated or omitted out of necessity. Changes that

²⁵The review may be performed by IT management, stakeholders (e.g., service owner, technical staff, or financial personnel), or a formal committee (e.g., IT steering or operations) depending on the proposed change's scope, costs, risks, impact, and implementation time frame.

²⁶ Refer to the [NIST Glossary](#). Approval mechanisms may include a change advisory (or control) board, IT steering committee, management committee, or other personnel, depending on the entity's size and complexity.

²⁷ Entities often use different words to refer to these types of changes (sometimes even using the same words to refer to different types of changes). During examinations, examiners should use the entity's terminology.

are implemented because of an urgent need may carry substantial risk, given the lack of advance planning and testing. Therefore, all emergency changes should be reviewed and approved after implementation.

For more information, refer to the *IT Handbook's* "[Development and Acquisition](#)" booklet.

III.E.2 Transitioning From Strategic Change Management to Day-to-Day Operations

Management should implement a process to transition system changes from a strategic change management process to day-to-day operations. The transition of responsibilities and knowledge should be part of the overall system development life cycle process as discussed in the *IT Handbook's* "[Development and Acquisition](#)" booklet. Knowledge about IT processes gained through the change management process should be effectively transferred in a useful format to personnel responsible for operating the systems and processes. The efficient aggregation and organization of information allows management to reduce repeat service request inquiries, increase instances of self-driven problem solving, and encourage the level of overall knowledge within the entity.

III.F Oversight of Third-Party Service Providers

Many entities outsource the AIO activities to one or more third-party service providers, often depending on the entity's size and complexity and the level of expertise available in-house. Management should identify the internal and external roles and responsibilities for AIO activities and implement processes to oversee the activities performed by third-party service providers on the entity's behalf. The responsibility and oversight, if properly assigned and defined, should interact as seamlessly as possible to ensure that management identifies and addresses all risks according to contracts and other agreements (e.g., SLAs). Management should be aware of the data destruction processes maintained by the entity's third-party services providers, including cloud service providers.²⁸ The SLA should outline that the third-party service providers take adequate measures to ensure data destruction occurs in a manner that would prevent unauthorized disclosure of information.

Management should review independent audit or other assurance reports demonstrating the third-party service provider's ability to meet the entity's AIO needs and provide services in a safe and sound manner. Management should report to the board on the effectiveness of any AIO activities performed by third-party service providers and any issues uncovered through the entity's third-party risk management processes.

²⁸ See the [FFIEC Joint Statement: "Security in a Cloud Computing Environment."](#)

III.G Resilience

A secure and resilient IT environment,²⁹ including AIO functions, is essential to the delivery of an entity's critical services. An entity's AIO functions should be integrated into the entity's business continuity management (BCM) program to help management mitigate threats, respond to and recover from disruptions, and incorporate lessons learned to strengthen the entity's resilience.

Resilience of an entity's AIO functions extends beyond recovery capabilities. Resilience is achieved by taking proactive measures to maintain confidentiality, integrity, and availability and mitigating the risk of a disruptive event through system design (including backup systems), infrastructure selection, and IT deployment. The threats related to disruptive events may pose risks from multiple attack types (e.g., cyber and physical), duration (e.g., advanced persistent threat³⁰ [APT]), and delivery via deception (e.g., simultaneous distributed denial of service [DDoS] and business email compromise attacks). Management should design, implement, and operate its IT systems and processes to provide resilience for critical business activities. As part of its consideration for resilience of AIO functions, management should determine its reliance on people, processes, and technology, including third-party service providers, to assist in its assessment of risk.

Management should design systems and software with resilience (e.g., redundancy, additional layers of defense, and resilient backup systems) and information and cybersecurity (e.g., inspect and detect vulnerabilities and attacks) at the beginning of the architecture process. Management may include activities related to ITAM (e.g., inventory, audit, and testing) to demonstrate resilience effectiveness. Management may have differing design risks and oversight responsibilities in a cloud environment (i.e., because a cloud service provider often has different types of clients co-located, an entity may be affected by attacks aimed at other industry segments).

The entity's infrastructure should support varying levels of resilience depending on the criticality of the systems and software to ongoing business operations. For instance, management may use redundant servers, have alternate data centers, or employ backup as a service to provide the appropriate level of resilience. For both architecture design and infrastructure implementation, it is important to follow the entity's project management processes to appropriately integrate resilience throughout the enterprise. Following formal processes to integrate resilience may help inform strategic decision-making and effectively address resilience needs for the entity's core business lines. To maintain resilience, infrastructure should be implemented in a way that allows for secure remote administration and maintenance, for situations when personnel are unable to perform operations on-site.

²⁹ For larger or more complex entities, refer to the interagency paper *Sound Practices to Strengthen Operational Resilience* released by [FDIC](#), [FRB](#), and [OCC](#).

³⁰ Refer to [NIST SP 800-160 Volume 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach](#).

Management should address resilience in operations to prevent data loss, protect sensitive customer information from unauthorized disclosure or manipulation, minimize disruption to service delivery, and prevent the loss of situational awareness of the entity's operations. This involves having adaptable and comprehensive operational controls, operational processes (e.g., vulnerability and patch management), service delivery and support processes (e.g., resilience in supply chain), and ongoing monitoring and evaluation capabilities (e.g., monitoring for indicators of an APT).

When operating in, or planning a migration to, a cloud environment, management should not assume that systems are resilient. During migration to cloud services, management should identify the assets, applications, and services located in the cloud. Management should verify that resilience is covered in contracts with cloud service providers. Additional risk mitigation options may be available in a cloud environment, such as tools to enable backups or the ability to store backups in multiple locations. For more information, refer to the *IT Handbook's* "[Business Continuity Management](#)" booklet.

III.H Remote Access

NIST defines remote access as access by users (or information systems) communicating external to an information system security perimeter. Examples of remote access include remote administration, access to the entity's network by third-party service providers, teleworker access, and customer access. Management should consider the implications of remote access in AIO.

When designing the entity's IT architecture for remote access capabilities, management should plan for the methods and access points that will be used across the enterprise to maintain security and control access to entity resources. Architectural design considerations include tunneling, web portals, direct application access, and remote desktop access.

- Tunneling involves establishing a secure communications tunnel, via encryption, between a telework client device and remote access servers within an entity, typically a virtual private network (VPN) gateway. When determining whether to use tunneling³¹ as a remote access method, management should consider the communications tunnel via encryption and the endpoints to which it is connected, as well as its capability to authenticate users and restrict access to IT systems.
- A portal³² is a server that offers access to one or more applications through a single centralized interface. A remote user accesses a portal client (e.g., a web browser) on a client device to access the portal. When determining whether to use a portal, management should consider whether it adequately protects communications between the client devices and the portal, and also whether it can authenticate users and restrict access to the entity's internal

³¹ Refer to NIST ITL Bulletin, [Security for Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Solutions](#).

³² Examples of portals include web-based portal, terminal access server, or virtual desktop infrastructure. Refer to NIST ITL Bulletin, [Security for Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Solutions](#).

resources. There is an important difference between tunnels and portals—the location of the application client software and associated data (i.e., in a tunnel, the software and data are on the client device; in a portal, they are on the portal server).³³

- Direct application access (e.g., webmail) occurs by accessing an individual application directly from most types of client devices without using remote access software. When determining whether to use this form of remote access, management should consider the security provided by the application, such as communications encryption and user authentication.
- Remote desktop access provides the ability to remotely control a particular desktop computer at the entity—most often, the user’s own computer at the organization’s office—from a telework client device. When determining whether to implement remote desktop access, management should consider limiting this method for exceptional use cases and implementing appropriate security controls (e.g., IAM and activity monitoring).

There are a number of risks associated with remote access, including unauthorized access, unrestricted privileged access, modification of information, inadequate monitoring, unencrypted communications, unpatched remote devices, and uncontrolled personally owned devices. Management should protect remote access technologies because they generally have a higher exposure to external threats compared with technologies accessed from inside the organization.³⁴ As more people work remotely, the scale of risk from remote access may increase. To mitigate risks associated with remote access, management should do the following:

- Develop and enforce a remote access policy that includes tiered levels of remote access and risk-based security controls over different types of remote access (e.g., remote administration and telework).
- Implement IAM based on job type and access and use appropriate authentication techniques (e.g., multi-factor authentication) for privileged access and activities, such as remote administration tasks.
- Use validated encryption technologies to protect communications between the entity and the remote user and encryption of sensitive data stored on the devices used for remote access.
- Securely configure remote access servers, including application of timely patch updates.
- Secure entity-owned telework client devices—including desktop and laptop computers, smartphones, and tablets—against common threats.
- Implement mitigating controls on the use of personally owned devices used to remotely access entity resources.

For more information on mitigating risks associated with entity-owned and personally owned devices, refer to the *IT Handbook*’s “[Information Security](#)” booklet.

³³ [Ibid.](#)

³⁴ [Ibid.](#)

III.I Personally Owned Devices

Personally owned and controlled user devices used for the entity's business purposes are known as bring your own device (also referred to as BYOD) resources. Personally owned devices may be used for remote access. They generally are not managed by the entity, creating the potential for an unsecured device to pose risks to the information that the user accesses and the entity's other connected systems and networks.³⁵ For example, a device compromised by a malicious user could be used to remotely access to the entity's network.

Before allowing the use of personally owned devices, management should perform due diligence on the types of devices that can be used. Management should consider the architecture of the entity's IT systems, to determine where and how personally owned devices will access the entity's network, in order to maintain appropriate security, segmentation, and access. Additional infrastructure (e.g., hardware and software) may be necessary to support the secure use of personally owned devices to access services. Management should determine the controls needed to adequately safeguard the network. Technical policy enforcement may ensure devices utilize anti-virus software and current operating systems, and that devices are not jailbroken.³⁶ For more information, refer to the *IT Handbook's* "[Information Security](#)" booklet.

III.J File Exchange

File exchange (also known as file sharing) is a method of sending and receiving files inside the entity and with other parties through email attachments, file sharing services, and other means. Risk considerations in file exchange include the following:³⁷

- Security deficiencies in file exchange methods (e.g., lack of encryption or use of weak encryption).
- File storage on untrusted servers controlled by third-party service providers leading to unauthorized access of the stored files and unapproved copies of the files.
- Files traversing untrusted networks, leading to unauthorized access (e.g., man-in-the-middle attacks or eavesdropping).
- Alteration (e.g., modification with incorrect information or injection of malicious code) of any file, even files without sensitive information.
- Solutions that are often difficult for users to set up and use (e.g., if the sender and recipient need to install software to exchange cryptographic keys).
- Use of unapproved, insecure, or ad hoc file exchange methods (e.g., shadow IT),
- Access to shared file repositories resulting in version control or unauthorized access issues.
- Identification of root causes of data exposure and measures to reduce the likelihood of its occurrence.

³⁵ [Ibid.](#)

³⁶ Refer to *FFIEC IT Handbook's* "Architecture, Infrastructure, and Operations" booklet [Glossary](#) for a definition of the term jailbreaking.

³⁷ NIST ITL Bulletin, "[Security Considerations for Exchanging Files Over the Internet.](#)"

Management should implement the following basic actions to improve the security of the entity's file exchange³⁸ activities:

- Identify user needs for exchanging files, both internally and externally. Identifying needs should include the senders and recipients, frequency of exchange, and nature of data being exchanged (e.g., public information, personally identifiable information, or proprietary).
- Design the client server architecture to provide for confidentiality, integrity, availability, and resilience. Examples of design considerations include the following:
 - File size and data complexity (e.g., XML or JSON (Java)).
 - Frequency of file updates.
 - File and data flows.
 - File usage by the various systems and by end users, including business unit usage.
 - Maintenance of security for files in transit and at rest.³⁹
- Identify the infrastructure, including the appropriate systems and software, necessary to support file exchange activities. File exchange solutions include email, file sharing services, managed file transfer, and custom applications (e.g., web and mobile). Often, entities may use more than one solution to meet their file exchange needs, in order to balance security and usability. Additionally, management should have appropriate infrastructure to support monitoring of the entity's file exchange activities. Some risk considerations in choosing a monitoring system include the following:
 - Monitoring for all methods of transferring files to third parties, including e-mail, copying information to external media, or use of shadow IT, which may not be visible to network security controls.
 - Capturing file exchanges between servers and between client devices and servers.
 - Monitoring beyond email to include monitoring of file exchanges happening through other means.
- Provide the appropriate operational controls, such as the following:
 - Conduct monitoring to ensure approved solutions are being used when needed to protect file exchanges, to avoid shadow IT solutions.
 - Include detection controls (e.g., IDS/IPS and firewalls) for inappropriate file sharing.
 - If using a third-party service provider file exchange solution, use only a trusted provider that employs appropriate controls for file exchange and storage solutions.
 - Consider solutions (e.g., cloud access security brokers (CASBs) for monitoring cloud-based file exchange and sharing capabilities) for providing visibility into cloud applications and their associated risks.
 - Define appropriate policies, standards, and procedures for file exchange activities.
 - Provide training to employees on approved solutions.

³⁸ [Ibid.](#)

³⁹ Refer to the *IT Handbook's* "[Information Security](#)" booklet for more information.

IV ARCHITECTURE

Action Summary

Management should design, apply, and align its IT architecture to meet the strategic and business objectives of the enterprise. The architecture plan should meet the entity's needs for confidentiality, integrity, and availability to minimize operational risks resulting from poorly designed systems.

Examiners should review for the following:

- Identification of the entity's information and technology assets.
- Assessment of future enterprise IT needs.
- Documentation of the architecture plan, including policies, standards, and procedures.
- Development of appropriate design objectives, including changes, EOL, and identification of shadow IT.
- Design of IT architecture (e.g., in-house, virtualization and cloud, or hybrid).
- Documentation of EA elements.

Architecture refers to the manner in which the strategic design of the hardware and software infrastructure components (e.g., devices, systems, and networks) are organized and integrated to achieve and support the entity's business objectives. Planning and designing an effective IT architecture facilitate management's ability to implement infrastructure that aligns with the entity's strategic goals and business objectives.

Management should implement architecture principles that can be applied enterprise wide. When designing an entity's architecture, management should balance the mitigation of risks to various stakeholders, considering both the enterprise's needs as well as the needs of individual business units. Regardless of how management designs the entity's architecture, it should align the architecture with IT and business objectives, for example, providing maximum benefits with lowest risks and acceptable costs. The architecture's design should meet the entity's needs for confidentiality, integrity, and availability and adhere to the entity's policies, standards, and procedures. In addition, management should consider the entity's architecture requirements for its existing technology and any planned changes.

Management should clearly define its mission and any strategic initiatives for architecture. Business units should understand their portion of the design, which should align with management's mission and strategic initiatives. In determining its future architecture, management should first identify the entity's IT assets and external constraints, as well as industry IT architecture trends. Once management understands the entity's current state of architecture, management should perform a gap analysis to determine the requirements to reach its future state.

Management should have policies, standards, and procedures to govern the entity's architecture design process. The design process should address the following:

- Definition of responsibilities and decision-making.
- Identification of functional requirements.
- Assessment of alignment with the entity's IT and strategic plans.
- Evaluation of the inventory of current IT assets and the purpose of those assets.
- Performance of a cost-benefit analysis of the architecture plan or project.
- Acquisition of approvals for the initiative.
- Implementation and maintenance of the architecture.
- Resolution of disputes or architectural issues.

Poorly designed architecture can lead to issues with confidentiality, integrity, and availability in both infrastructure and operations.

IV.A Architecture Plan

Management should have a documented and approved architecture plan that identifies the entity's current state. The architecture plan should align with the entity's strategic plan to support the business and strategic objectives of the entity. Management should have policies, standards, and procedures that govern architecture initiatives and changes to the architecture plan. There should be processes including obtaining approvals for initiatives, making changes to the plan, and reporting to management or the board as appropriate.

Smaller or less complex entities may have a less structured architecture plan and generally have fewer initiatives or changes to the plan. Larger or more complex entities often have complex architecture plans, architecture review processes, and architecture boards or planning groups to ensure that initiatives are carried out according to architectural principles.

When the entity is planning larger or more complex architecture changes, implementation of those changes should maintain and follow a project management process that includes the following phases:

- Plan (e.g., identify requirements and functional specifications and design technical architecture).
- Execute (e.g., build and implement solution and monitor and control risks).
- Closeout (e.g., update documentation and incorporate lessons learned into the architecture plan).

IV.B Design Objectives

An architecture process creates a systematic approach to streamline the design process and provides management with a plan to organize and integrate new hardware and software with existing infrastructure. When designed properly, the process can help maintain agility and flexibility in meeting changing business needs. Hardware and software selection and

implementation rely on the collaboration between IT and business line management. A fundamental step is to define terminology to provide a common set of terms used by IT and business unit personnel to design the entity's architectural process.

Management should evaluate its needs and consider the following:

- Collaboration between IT and business units.
- Prioritization of investments.
- Comparison of existing architecture with long-term goals and anticipated future needs and changes.
- Establishment of processes to evaluate and procure technology.
- Storage (e.g., network-attached storage and storage area network [SAN]), backup, and capacity needs to accommodate the entity's strategic plans.
- Whether the architecture will support internet-facing applications, internal network applications, or both.

Management should include the following aspects in its architecture design:

- Performance and reliability (e.g., system processing at normal and peak loads, response time, load balancing, and uptime required by end users).
- Integrity (e.g., validation checks to promote accuracy).
- Availability and resilience (e.g., meeting recovery time objective [RTO] and recovery point objective [RPO] requirements, providing redundancy, and avoiding single points of failure).
- Scalability (e.g., the ability of systems and software to accommodate growth).
- Flexibility (e.g., the ability of systems and software to accommodate changes without requiring new hardware or code changes).
- Security and privacy throughout the entity's network (e.g., IAM controls and data loss prevention).
- Interoperability⁴⁰ and integration (e.g., among OSs, databases, networks, and user interfaces, and loose coupling).
- Ability to integrate and align with one or more third-party service providers.⁴¹
- Testing (e.g., integration and business continuity testing) internally and with third-party service providers as appropriate.
- Auditability (e.g., audit trails and logs).
- Advancements in technology.

The design objectives should include considerations for avoiding the potential for shadow IT. Management should design its systems to provide the capability to monitor and alert for the use of shadow IT because shadow IT uses entity resources and could provide unknown avenues for exploitation. Management should consider how evolving technologies (e.g., cloud, IoT, and artificial intelligence [AI] and machine learning [ML]) can affect its systems' design.

⁴⁰ For supervisory purposes, interoperability refers to the ability of data, systems, or software to work with or on multiple systems or software.

⁴¹ Situations where the entity's IT architectural design does not align with the third-party service provider's systems, resulting in difficulty managing integration (e.g., costs of making manual changes, security issues, and errors and omissions) between the entity and its third-party service provider.

Management should plan for obsolescence, EOL, and decommissioning of systems to understand the resource requirements throughout any system's expected life cycle. Planning for obsolescence and EOL allows management to consider how it will protect the confidentiality, integrity, and availability of the information on a system. The architectural process should include planning for system decommission, including the migration from the old system and disposal of all critical components, services, and information when systems need to be replaced. If management does not plan for system obsolescence, EOL, and decommissioning, sensitive information may be retained on discarded components. Unnecessary and potentially unprotected system components may unknowingly remain connected to the network, using resources and providing a potential avenue for compromise, similar to what happens with shadow IT.

IV.C IT Architecture Design

IT architecture design includes determining the appropriate deployment environments. Design environments may be managed in-house or by a third-party service provider, including a cloud service provider. Whether in-house or outsourced, management may use a combination of physical and virtual design environments and should consider the risks and benefits of both. For example, if management is considering moving some operations to the cloud, management should determine how the entity will benefit from virtualization or a cloud-based solution and the design implications, personnel responsibilities, and security provisions of that decision. Physical and virtual design environments may not differ substantially; the differences will be apparent in the design's implementation.

Designing the architecture of an entity's IT systems may include "the placement of the virtualization solution and the selection of virtualization software."⁴² Entities may incorporate virtualization into their architecture design to reduce costs and risks of maintaining and managing multiple pieces of physical hardware. Virtualization allows virtual elements to be transferrable between different pieces of hardware within physical or third-party-hosted environments, including cloud environments. In designing the entity's virtual environment, management should consider the design risks associated with the following elements:

- **Virtual machines (VM).** To address the lack of visibility and control over the entity's virtual environment, management should design secure virtual infrastructures, including the ability to oversee the interconnectivity and segmentation of VMs.
- **Hypervisors.** To ensure visibility and control of the environment and address the susceptibility to unauthorized access, malware, and mismanaged traffic, management should design where the hypervisors sit and the connectivity between hypervisors and VMs.
- **Containers.** To manage container vulnerabilities, unintentional interactions (e.g., between containers and applications or containers and host OSs), and container failures (e.g., security misconfiguration, application programming interface [API] disconnection, and lack of portability), management should have vulnerability management processes, employ segmentation, and provide the ability to monitor containers. Additionally, to avoid having to re-create data when updating and replacing containers, management should design for storing data outside of the container.

⁴² Refer to NIST SP 800-125, [Guide to Security for Full Virtualization Technologies](#).

- **Microservices.** To address the risks to application compatibility and functionality, management should have a design process that allows for the use of microservices as an integrated component of overall IT operations. Additionally, management should address the risks to security (e.g., having multiple microservices can increase the financial institution's attack surface), reliability (e.g., ability to re-use and API alignment with business processes), and latency (e.g., fault tolerance and scalability) in the entity's development process. For more information, refer to the *IT Handbook's* "[Development and Acquisition](#)" booklet.

Other considerations include the placement and selection of storage, design of network topology, availability of bandwidth, and need for management reporting systems. Management also should consider designing its systems to allow for the implementation of monitoring tools (e.g., identifying node and system failures in the cloud).

IV.D Enterprise Architecture

EA is the description of an entity's entire set of information systems:

- How they are configured.
- How they are integrated.
- How they interface to the external environment at the enterprise's boundary.
- How they are operated to support the enterprise mission.
- How they contribute to the enterprise's overall security posture.

EA includes an entity's current state (also called baseline architecture), a future state (also called target architecture), and a plan to achieve the future state to meet the business objectives. EA provides a logical structure allowing management to classify, organize, and document elements of the entity's systems, functions, and information.

Smaller or less complex entities may not have EA, but those entities still should manage their existing architecture needs and planned changes. As an entity becomes larger or more complex and different systems are needed to support that growth, management should consider the implementation of EA to align its architecture with the entity's strategic plans and business functions. Regardless of entity size or complexity, management should evaluate the best approach to implement security and resilience and build these characteristics throughout its architecture. When legacy systems exist, management should analyze the functionality, including security and resilience, of current systems and identify gaps. This helps management determine whether the legacy system should be maintained, replaced, or retired and what effect that will have on EA.

Management may designate internal staff to design and manage EA, employ a third-party service provider, or use a combination of internal staff and third-party resources. For a larger or more complex entity, the chief architect's role typically includes EA responsibilities. The architect may help management analyze the current architecture using an industry framework to better align the architecture with the entity's strategic objectives. In a larger or more complex entity, a formal group (e.g., architecture review board) may assist in oversight of EA. Management may

use aspects of industry frameworks⁴³ as appropriate for the entity's business needs. A framework may have different characteristics (e.g., informal, formal, prescriptive, principles-based, or a hybrid).

⁴³ Some examples of industry architecture frameworks include The Open Group Architecture Framework (also known as TOGAF) and Federal Enterprise Architecture.

V INFRASTRUCTURE

Action Summary

Management should implement an IT infrastructure that achieves and promotes the objectives of confidentiality, integrity, and availability, and meets the entity's business objectives. Management should develop, document, and implement infrastructure control policies, standards, and procedures to safeguard facilities, technology, data, and personnel. IT infrastructure implementation practices should include redundancy and resilience for physical infrastructure elements and related products, services, and telecommunications.

Examiners should review for the following:

- Processes to identify, track, and monitor infrastructure components.
- Contractual arrangements addressing infrastructure, if applicable.
- Sufficient resources with infrastructure knowledge, skills, and expertise.
- Network configuration management and change control processes.
- Security and monitoring processes to analyze data traffic and detect anomalous activity.
- Software planning to address:
 - Scalability, interoperability, and portability.
 - Adequate software controls.
 - Use of and controls over open source software.
- Mainframe controls, if applicable, to address unique risks associated with mainframes.
- Security controls for the use of application programming interfaces (API).
- Environmental and physical access controls.

As previously stated, infrastructure refers to the physical elements, products, and services necessary to provide and maintain ongoing operations to support business activity and includes the maintenance of physical facilities. IT infrastructure includes hardware, network and telecommunications, software, IT environmental controls (e.g., power and HVAC), and physical access that allow for an enterprise IT environment's operation and management. IT infrastructure implementation should include considerations for server and data redundancy and resilience of telecommunications lines. Planning and designing an effective IT architecture facilitates management's ability to implement an IT infrastructure that achieves and promotes the objectives of confidentiality, integrity, and availability and supports the entity's business operations. IT infrastructure may be managed internally or externally by a third-party service provider, including a cloud service provider.

V.A Hardware

NIST defines hardware as “the physical components of an information system.”⁴⁴ Hardware devices can be an ideal target for malicious actors. Therefore, management should track and monitor all hardware assets (whether or not they are connected to the network) to maintain an accurate and current record of the technology assets in its environment. This is often done with an accurate hardware inventory. Without an accurate inventory, management may encounter challenges in protecting hardware assets, managing cyber risks, and recovering from and responding to incidents. For more information, refer to the “[IT Asset Management](#)” section of this booklet.

Management should identify unauthorized technology assets and determine their disposition (e.g., remove, isolate (quarantine), or add them to the inventory). If an asset is determined to be unauthorized, management should evaluate how the device gained access and what, if any, compromise may have occurred. Management should determine whether the policy or procedures should be updated or whether additional training is necessary. Automated tools can assist management in maintaining the accuracy and availability of hardware components. Network discovery tools identify assets connected to the network and compare them to an inventory of authorized hardware assets. Advanced asset discovery tools (e.g., using dynamic host configuration protocol [DHCP] on servers or asset management tools using IP addresses) may be used to provide oversight of the entity’s technology asset inventory.

V.B Network and Telecommunications

Networks are systems implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. Management should document and maintain a current inventory of network and telecommunications hardware and software and the network configuration. For more information, refer to the “[IT Asset Management](#)” section of this booklet.

NIST defines telecommunications as “the preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.” Given the critical nature of telecommunications, management should ensure appropriate redundancy capabilities in the entity’s telecommunications infrastructure and should understand the limitations of the entity’s third-party telecommunications providers’ infrastructure. Network and telecommunications infrastructure form the backbone for the entity’s data and voice communication, including information sharing and data transfer, and facilitate the integration of technology systems.

⁴⁴ Refer to the [NIST Glossary](#).

V.B.1 Network

Network infrastructure consists of components (e.g., hardware and software) that transport data, support software functions, deliver services, and provide communications. Entity and customer traffic pass through these components, which include the following:

- Hubs and switches.
- Load balancers.
- Routers.
- Domain name system.
- Servers.
- Firewalls.
- IDS/IPS.
- SANs.

Once management has an accurate inventory that contains network components and information, management should document the network's baseline configuration, including processes to review and approve changes. Management should regularly assess and document compliance with the entity's baseline configuration⁴⁵ to validate that settings are in place and commensurate with the board's risk appetite. Intentional or unintentional misconfigurations can lead to system issues or exploitation of vulnerable services and settings by malicious actors. To reduce exposure to potential vulnerabilities and failures arising from unused services, management should implement appropriate network configuration management and change control processes. Configuration rules allowing traffic to pass through the network should be documented with the necessary detail to justify the business need. Management should periodically review the configurations of network devices. Tools are available to verify that network devices are using approved configurations and notify management when unauthorized changes are detected.

Network devices are often delivered with enabled services, open ports, and commonly known default passwords. Management should appropriately control networked devices by managing ports (e.g., close unnecessary ports), protocols (e.g., deactivate unsecure protocols), and services (e.g., disable unnecessary services) to minimize exposure to vulnerabilities or errors. For more information on these and other system "hardening" activities, refer to the *IT Handbook's* "[Information Security](#)" booklet. Ports, services, and protocols should be mapped to the technology asset inventory. Automated tools are available to perform port scans to validate that only approved ports, protocols, and services are in use. The latest version of security-related updates should be installed on network devices, when appropriate. For more information, refer to the "[Patch Management](#)" section of this booklet.

A server is a computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries). A server's standard, or baseline, image is the approved set of server configurations, applications,

⁴⁵ Guidance for implementing best practices for server configurations can be found at the [NIST National Checklist Program](#) and through other industry sources (e.g., [Center for Internet Security](#)).

and systems, which can be used to deploy servers consistently and rebuild them more easily and quickly, when necessary. Management should maintain standard images (or templates) of the entity's servers. Standard images of servers should be stored securely, and if a server needs to be rebuilt (e.g., upon discovery of an infected system), management should use clean, trusted images to restore the server. Deviations from the standard image should be documented, reviewed, and approved.

Management should implement security and monitoring throughout the entity's network to monitor system components, analyze incoming and outgoing data traffic, and alert authorized personnel if anomalous activity is detected. To accomplish this, security and monitoring mitigation strategies include the following:

- Use of software tools to protect against and monitor for malicious actors scanning for internet-accessible services or open ports.
- Implementation of firewalls and packet filtering to limit internet traffic to exclude services and ports (e.g., whitelist and blacklist).
- Deployment of IDS/IPS that use signature-based detection, anomaly-based detection, and stateful protocol analysis to detect and prevent attacks against the network or attacks against services, systems, applications, or data. IDS/IPS alert personnel to potential attacks, while IPS can be configured to take an action predefined by management, such as blocking various types of activities.
- Use of internal tools (e.g., data loss prevention, email content filtering, and internal IDS/IPS) to detect, identify, and prevent misuse by entity personnel.

When possible, management should perform administrative activities from dedicated workstations (used exclusively by administrators to manage the network's technology devices) located on an isolated portion of the network not used for regular business activity. Management should use multifactor authentication over encrypted network connections for administrators accessing and managing network devices.

V.B.2 Telecommunications

Telecommunications infrastructure should be appropriate for current and anticipated internal traffic needs and have sufficient connectivity to facilitate external communications.

Telecommunications infrastructure includes both voice and data transmissions that are broken up into multiple packets to facilitate transmission of those packets over shared paths.

Telecommunications packets typically incorporate message content and completion validation messages. Between telecommunications endpoints, packets can be lost, encounter interference, or arrive out of order. Capacity, latency, and connectivity issues can affect the arrival of packets or completion of messages. Therefore, management should monitor telecommunications traffic. In addition, administrators should periodically review network devices to identify any that are operating in promiscuous mode or acting as packet "sniffers" for network traffic.

Management should physically secure telecommunications equipment⁴⁶ and restrict and monitor access (e.g., through access devices, logs, and cameras). Changes to telecommunications equipment and configurations should follow enterprise change control standards, including approval, testing, and migration to production. Identification, authorization, and authentication to access (including remote access) telecommunications systems should follow entity policies, standards, and procedures, including approval and documentation of exceptions. Documented wiring strategies (e.g., schematics and color coding) and organized cables facilitate easy troubleshooting, repair, and upgrade.

An entity's telecommunications infrastructure components should be designed and built for resilience. Loss of telecommunications can have a material impact on the ability of an entity to function, exposing it to legal and financial risks. Management has little direct control over the telecommunications services beyond the entity's network. The telecommunications lines are subject to environmental risks (e.g., weather or natural disasters) and other risks (e.g., terrorism, sabotage, or accidents), which can damage communications cables and equipment at the entity, the telecommunications service provider, or in between. Where available, the entity's selection of infrastructure components and telecommunications providers should ensure access to a diversity of suppliers and connectivity to avoid a single point of failure. Management should implement route diversity, where available, to ensure data can travel along an alternate route if its primary path is blocked. For more information, refer to the *IT Handbook's* "[Business Continuity Management](#)" booklet.

The telecommunications services sector is designated as a critical infrastructure sector for national security and emergency preparedness. The telecommunications services sector provides support for the clearing, payment, and settlement processes, which are considered critical activities in another critical infrastructure sector, the financial services sector. For more information, refer to the *IT Handbook's* "[Business Continuity Management](#)" booklet.

V.B.2(a) *Voice Communications*

Voice communications are critical to meeting business needs by facilitating understanding and interactions among personnel, internal and external entity customers, and third-party service providers. Regardless of the type of voice communication solution (e.g., voice over internet protocol [VoIP], dial-up, or mobile), risks include quality of service degradation (e.g., echo or dropouts), resilience (e.g., loss of voice communication), and security (e.g., eavesdropping), which can lead to a failure to address time-sensitive issues and loss of business. Therefore, management should address these risks through their development and acquisition processes and in their written policies, procedures and practices.

Entities often use VoIP for internal and external voice communications.⁴⁷ VoIP refers to the transmission of voice communications over the internet rather than through the public switched telephone network (PSTN). When a telephone call is made using VoIP, the caller's voice is

⁴⁶ Typically, telecommunications equipment is located in a separate telecommunications closet or room.

⁴⁷ For the purposes of this booklet, voice communications refers to the transmission of speech over communication (e.g., telephone) lines.

translated into a stream of data packets. The data packets are transmitted over the internet and converted to a voice signal on the other end of the communication. In addition to an IP-enabled telephone, VoIP systems include call managers, gateways, routers, firewalls, and protocols. The call manager performs the functions of a traditional phone network and is the core of the VoIP system. A VoIP gateway provides conversion of calls between the data network and the PSTN. Routing and switching infrastructure provides the basic network connectivity and transport.

As with telecommunications in general, the risks associated with VoIP include service quality (e.g., packet delays resulting in garbled communication), failure of communication (e.g., loss of voice communication), and security issues. Security issues include configuration weaknesses in VoIP devices and underlying OSs that enable denial of service (DOS) attacks, eavesdropping, voice alteration (hijacking), and toll fraud (theft of service). VoIP is susceptible to the same risks as data networks that use the internet, such as exposure to viruses, worms, trojans, and man-in-the-middle attacks. Each of these can result in the loss of confidentiality, integrity, and availability.

Management should perform a comprehensive risk assessment to ensure the confidentiality, integrity, and availability of voice communications using VoIP technology. When considering VoIP in the design of its network architecture, management should implement physical and logical controls in the VoIP environment and evaluate options for backup systems (e.g., hard-wired communication lines) that will provide redundancy in communication during power outages.⁴⁸ Traditional security controls may not provide appropriate security for VoIP systems, therefore, management should consider control solutions specific to VoIP, such as VoIP-ready firewalls.

V.B.2(b) *Data Communications*

Data communications is the transfer of data over networks⁴⁹ using a combination of telecommunications services and network devices. Networks connect devices within a single geographic site or can connect multiple geographically dispersed entity and third-party service provider sites. They connect servers, end user devices (e.g., workstations, laptops, and mobile devices), wireless routers, and network security devices, such as firewalls and IDS/IPS.

Entities contract with telecommunications service providers for the physical connection supporting data communications among network sites. Given the network's importance to the entity's infrastructure, management should monitor incoming and internal data communications traffic for problems such as outages, connectivity degradation, throughput issues, capacity concerns, and other anomalies. Inadequate maintenance or an inadequate response to problems may lead to degraded data communications service levels. Management should implement redundant telecommunications services (e.g., alternate telecommunications providers or lines)

⁴⁸ Widely accepted practices are available in [NIST SP 800-58, Security Considerations for Voice Over IP Systems](#).

⁴⁹ Networks can be composed of local area networks, wide area networks (WAN), and metropolitan area networks (MAN). WANs or MANs extend a data network to geographically dispersed offices, operations centers, service providers, and partners.

where appropriate and establish work-around procedures for situations where redundant telecommunications are not feasible.

V.C Software

NIST defines software as computer programs (which are stored in and executed by computer hardware) and associated data (which also are stored in the hardware) that may be dynamically written or modified during execution. As part of infrastructure planning, management should determine the types of software needed to implement the entity's strategic objectives. Software implementation planning is fundamental to the confidentiality, integrity, and availability of the entity's data that interact with software. Management should consider the software's scalability, interoperability, and portability. As with its other infrastructure elements, management should perform the following:

- Track and monitor the entity's software assets whether they rely on network connectivity or are strictly isolated to individual workstations.
- Maintain an accurate and current record of the software assets in its environment, often through the use of software inventories.
- Periodically review existing software to meet changes in the entity's strategic objectives and operational goals.

The following sections describe the various developed or acquired software types and associated risks with the use of each.

V.C.1 Internally and Externally Developed Software

Understanding the types of software needed to meet the entity's infrastructure and operational requirements is key to successful software implementation. In addition to choosing software, management should consider whether it develops the software internally or obtains the software from a third party. Options include the following:

- **Internally developed software:** An entity's internal development team can develop software or management can engage third-party development teams to develop software on the entity's behalf. Management is responsible for maintaining the software; therefore, entity personnel should have the resources and expertise to stay abreast of vulnerabilities and develop software updates and patches to promote the security and resilience to meet business needs. Refer to the *IT Handbook's* "[Development and Acquisition](#)" booklet for more information on internally developed software.
- **Externally developed software:** Externally developed software is available in multiple forms. These include the following:
 - **Commercial off-the-shelf (COTS) software:** COTS is a software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public. COTS is also referred to as off-the-shelf. COTS software is built with default functionality and configurations to accommodate a variety of uses. It offers

several advantages, such as lower cost and easier installation, and generally includes software support. COTS software may not, however, meet the entity's needs or security requirements. For example, COTS software may not integrate easily with existing software and may require further configuration to meet the entity's needs.

- **Custom software:** Custom software (e.g., core processing software) is developed for entities to provide custom functionality. Custom functionality can be developed by the entity or a third party (e.g., vendor or third-party service provider) by changing existing software through modules or functionality extended by add-ons (e.g., software extensions) to meet the entity's needs. Regardless of how custom software is developed, it should be designed to integrate with the existing enterprise software, hardware, and data. Risks associated with custom software may include higher support costs for modifying outdated software. Regular updates and maintenance of custom software may be more difficult because of the customization or lack of expertise.

Management should approve the software's use and ensure that the software meets the entity's infrastructure requirements (e.g., hardware requirements) and strategic objectives. Management should allocate resources to support the software (e.g., costs to maintain the software or support personnel), and personnel should have the expertise needed to maintain and patch the software. Refer to the *IT Handbook's* "[Development and Acquisition](#)" booklet for more information on software development and acquisition risk management.

V.C.2 Software Types

Entities use a variety of software to support day-to-day operations. These are common software types that support the infrastructure needs and business objectives. Regardless of the software used, management should be aware of and implement risk mitigations for general risks associated with software in the entity's infrastructure environment. To mitigate software vulnerabilities, management should keep the software current and appropriately patched. To mitigate unauthorized access to sensitive information, management should implement appropriate IAM controls, including activity monitoring. Risks associated with development, information security, and third-party service providers are discussed in the *IT Handbook's* "[Development and Acquisition](#)," "[Information Security](#)," and "[Outsourcing Technology Services](#)" booklets.

Software types found in server-based or cloud-based infrastructure environments typically include OS, core processing, productivity, enterprise, security, and system auditing software. The software types described in the following bulleted list can be proprietary (i.e., development is performed by designated employees or vendors) or open source, which is described in a sub-section after the bulleted list. There are also software types to address risks and controls specific to mainframe security and APIs described in the following sub-sections.

The following are general types of software found in both server-based and cloud-based infrastructure environments:

- OS software:** An OS is a program that runs on a computer and provides a software platform on which other programs (e.g., application software and utility software⁵⁰) can run. An OS manages computer hardware resources and provides common services (e.g., access and security controls, file system maintenance, and communications management). There are numerous server, desktop, and laptop OSs, as well as mobile (e.g., tablet and smartphone) OSs. Regardless of the type used, if the OS is not maintained, other software may not function adequately or at all, which affects the entity's ability to conduct business. Therefore, management should oversee and maintain the OS, including testing and installing patches when appropriate. Because having access to the OS, including utility software, provides access to applications running on the OS platform, management should restrict and monitor administrator access to the OS and should limit the use of utility software.⁵¹
- Core processing software:** Core processing software enables the processing of key banking functions (i.e., taking deposits and making loans) and other functions (e.g., statement rendering, payment processing, calculating interest, and customer relationship management [CRM]), and interfaces to other software (e.g., general ledger systems and reporting tools). This software should be appropriately restricted based on job responsibility and its use monitored because of the sensitive nature of the entity's and the customer's information and the impact on other systems (e.g., general ledger and customer and management reporting). Management should select core processing software with adequate capacity to support strategic goals and objectives (e.g., customer base growth or geographic diversity). The software should support usage spikes (e.g., daily, monthly, and quarterly), expected peak usage times (e.g., holidays), and future growth.
- Productivity software:** Productivity software can refer to any software that helps to produce and manage data and improve the user's productivity. Management should consider using productivity software in its infrastructure environment to enable personnel to perform their job functions. Examples can include word processing, spreadsheet, database, video conferencing, and presentation software. "The line between web applications and locally installed applications has blurred over time to the point where a number of web application providers offer web versions of common desktop productivity tools, including word processors, spreadsheets, and calendars.... As such, these web applications may need to support the ability to store and process mobile code associated with office documents (or any user-generated files), opening up web applications to many [risks associated with web applications]." ⁵² "Common management and operational controls used to safeguard systems against other security threats also apply to active content." ⁵³ These controls include IAM, configuration management, and monitoring of logs. There is a risk that data may fail to synchronize correctly, which could negatively affect data integrity. An attacking entity may intercept messages in transit and modify their contents, substitute other contents, or simply replay the transmission dialogue later in an attempt to disrupt the synchronization or integrity

⁵⁰ Utility software includes file compression, defragmentation, diagnostics, and performance optimization.

⁵¹ Some utility software can provide privileged access to other programs and data residing on the system.

⁵² Refer to [NIST SP 800-28 Version 2, Guidelines on Active Content and Mobile Code](#).

⁵³ [Ibid.](#)

of the information.⁵⁴ Mitigation strategies to address synchronization issues include version control, group collaboration, and other synchronization capabilities within a cloud (e.g., autosynch or file management).⁵⁵

- **Enterprise software:** Enterprise software helps management make better and more informed decisions through enterprise data aggregation. Enterprise software examples include communication, collaboration (e.g., SharePoint), CRM, digital and content creation, enterprise resource planning, project and portfolio management, and supply chain management. Enterprise software can encompass a vast array of subjects, methods, models, and reporting. Management should consider how enterprise software integrates in the entity's infrastructure environment. Because of the sensitive or critical nature of the information available within this type of software, management should limit access and editing capabilities and monitor user activity.
- **Security software:** Security software is designed with the goal of preventing an attacker from reaching the intended target or limiting the damage of an attack. The software can be designed to track the damage incurred from an attack. Malicious code continuously evolves; therefore, management should use security software that is current, deployed effectively, and designed to keep up with the evolution of malicious code. The software can be controlled by either a third-party service provider or the entity. Because of the sensitive security information contained within the software or technology assets being monitored by the software, administrative access to this type of software should be restricted. Security software types may include the following:
 - IAM.
 - Antivirus.
 - Encryption management.
 - Application firewall.
 - IDS/IPS.
 - Log management.
 - Security information and event management.
 - Patch and vulnerability management.

For more information, refer to the *IT Handbook's* "[Information Security](#)" booklet.

- **System auditing software:** System auditing software refers to automated programs that perform a variety of audit functions, such as database sampling and source code checks. Its purpose is to highlight exceptions to data and, in return, identify potential errors. Results can produce false positives and may require human intervention to verify that results are not accurate and make adjustments to reduce false positives over time. Management should use system auditing software to augment audit personnel and assist in the identification of gaps in infrastructure security and resilience. Once validated, audit results from the software can be used in conjunction with ML and AI. For example, the number of false positives can be reduced over time and the software can take certain actions to mitigate risk. Management

⁵⁴ [Ibid.](#)

⁵⁵ Refer to [NIST SP 800-146, Cloud Computing Synopsis and Recommendations](#).

should document software intended for system audit use and define its purpose to ensure continued usefulness and reliability. For more information, refer to the *IT Handbook's* "[Audit](#)" booklet.

V.C.2(a) *Open Source Software*

Unlike proprietary software, open source software⁵⁶ can be accessed, used, modified, and shared by anyone.⁵⁷ Management may leverage a variety of open source software. Open source software may provide several advantages, including cost and availability. Management should identify unique security issues (e.g., public availability of the code, ability for users to alter the code, licensing issues, difficulty in tracking patches, and publicized exploits) with the use of open source software. Management should implement security controls and procedures to mitigate risks, including the following:

- Defining acceptable use (or restriction) guidelines, if appropriate, for open source software, including documenting a process for modifying and reviewing the code.
- Restricting access to unapproved shareware sites.
- Using tools to help discover unapproved open source software.
- Identifying the type and version of open source software in use, where it is used within the entity, and its purpose.
- Implementing version and patch control guidelines for open source software in use.
- Monitoring for vulnerabilities of the open source software employed by the entity.

Open source components may be present in third-party software used by the entity; therefore, management should evaluate the implications of those components and address their use in contract provisions. Information regarding open source software or components should be evaluated by management during its software due diligence. Refer to the *IT Handbook's* "[Development and Acquisition](#)" booklet for further information.

V.C.2(b) *Mainframe Security Software*

Using a mainframe computer in the infrastructure environment presents specific security risks. Mainframes may provide a single point of control or access point to an entity's systems, applications, and information repositories. The risks include inappropriate user access, unauthorized access to mission-critical data, inappropriate audit log settings, inadequate monitoring and alerting, untimely patch management, and ineffective auditing of mainframe security. To mitigate these risks, management should implement the following:

- Access controls, including role-based access control, segregation of duties, and multifactor authentication.

⁵⁶ Examples of open source software include the following: CRM (e.g., Flowlu, HubSpot CRM, and YetiForce); project management (e.g., Trello); blockchain (e.g., Ethereum, Hyperledger, and IOTA); internet browser (e.g., Firefox); productivity (e.g., LibreOffice and GIMP); OS (e.g., Linux, BSD, and Unix); and security (e.g., Nessus, Snort, Nagios, Nmap, Metasploit, Wireshark, and Kali Linux).

⁵⁷ Refer to [NIST Suborder 6106.01, "Open Source Code."](#)

- Security controls (e.g., password complexity, inactivity timeout, and login restrictions).
- Encryption of sensitive information.
- Activity log settings that include user access, failed login attempts, and security setting changes.
- Real-time monitoring and alerting of mainframe activity.
- Timely patch management processes.
- Mainframe security auditing (e.g., regular review of security controls and validation of privileges, roles, and access profiles to limit excessive access and provide for timely removal of unnecessary access).

System and security administrator access (e.g., super user privileges) are necessary to perform specific mainframe activities; such access, however, creates a potential for misuse. Management should have an independent method to closely monitor the use of these privileged accounts.

There are several software-based access control security tools⁵⁸ available for managing security of critical mainframe system resources. These tools are generally add-on software products that provide security for a mainframe and protect system resources by granting access only to authorized users. Tools provide the ability to do the following:

- Identify, authorize, and authenticate users.
- Safeguard sensitive information.
- Log and report attempts of unauthorized access to sensitive information.
- Provide system and security administrator controls.

Mainframe experts may not be readily available. Therefore, management should maintain appropriate expertise to understand the unique security features of mainframe computers.

V.C.2(c) *Application Programming Interfaces*

APIs are software code that allows two or more different programs to communicate with each other. Entities use APIs (considered a form of middleware) to connect services and to transfer data. Broken, exposed, or compromised APIs can be exploited by malicious actors and used in data breaches (e.g., compromise of financial and personal data) or for other purposes (e.g., preventing availability) by exposing the endpoints or compromising the authentication tokens. Security needs for APIs should be assessed and implemented to mitigate risks of exposing sensitive customer or entity information.⁵⁹ Therefore, management should address authorization, authentication, and encryption; API security tools and gateways with controls for requests and responses; sensitive data filtering; restriction on size and number of resources requested; identification of API request checkpoints for information leaving the network; and appropriate API logging and monitoring. Examples of security controls include the following:

⁵⁸ Examples of industry tools include [Resource Access Control Facility \(RACF\) from IBM](#), [CA Access Control Facility \(ACF2\) from Broadcom](#), and [CA Top Secret from Broadcom](#).

⁵⁹ The [OWASP API Security Project](#) discusses API security issues and controls.

- Secure IPs (e.g., HTTPS) to encrypt data during transmission from the web browser to a web server.
- Password hashing to validate the integrity of the message.
- Restriction of secret information (e.g., API keys, session tokens, and user IDs) from website addresses to prevent unnecessary information transmission.
- Industry standard authorization protocols⁶⁰ to securely authenticate users.
- Strong validation to ensure a user knows what to input (i.e., client-side validation) and on the web server to ensure data are accurate and in the correct format (i.e., server-side validation) to help mitigate malicious attacks.
- Time stamping of API requests to provide traceability of the request.
- Rate limiting of API calls to protect against malicious attacks (e.g., DDOS).
- API traffic monitoring to determine the locations from where requests originate allowing the ability to take action (e.g., monitor activity or block IP addresses).
- API gateways configured appropriately throughout the entity's IT environment to facilitate principles of least privilege to information and services.

There are three primary types of APIs. An entity may use more than one of the following within its infrastructure:

- **Internal or private APIs:** Internal or private APIs are restricted from external access. They are used by internal teams or business units to access internal data, services, and tools. Advantages of using internal APIs include the following:
 - Standardization of connections to internal services (e.g., eliminating hard-coded connections).
 - Decreased code development time through use of existing and already tested APIs.
 - Control over coding practices (e.g., secure coding).
 - Access restrictions over the API.
 - Auditability of API access and requests.
 Management should implement an appropriate level of security before internal APIs are made available for use by other entity business units.
- **Public or open APIs:** Public or open APIs (also referred to as third-party APIs) are accessible by external parties (e.g., developers). External parties register for access with the entity and, in return, receive an API key.⁶¹ In some cases, however, no registration is required. Management should implement adequate security and restrictions to protect sensitive customer and entity data. Management should perform appropriate testing to verify the adequacy of security controls before and after going public.
- **APIs between customers and unaffiliated third parties:** In this situation, the relationship is between the customer and a third party (e.g., a fintech firm that is separate from the financial institution where the customer has the account). This type of API has a specific purpose and may have a fee associated with its usage. As part of its customer awareness

⁶⁰ For an example refer to Internet Engineering Task Force, [RFC 7591, OAuth 2.0 Dynamic Client Registration Protocol](https://tools.ietf.org/html/rfc7591), DOI 10.17487/RFC7591, July 2015.

⁶¹ An API key allows access to certain services and data.

program,⁶² management should make security awareness information (including the protection of customer information) available to its customers. The security awareness information should address protections available and not available when the customer allows access to its data through the use of unaffiliated third-party API services. Better-informed customers bolster the safety and soundness of an entity, consumer financial protection, and compliance with applicable laws and regulations.

V.C.3 Software Hosting

Software can be hosted internally at the entity, externally at the entity's third-party service provider, or in a combination of the two (e.g., using cloud infrastructure to manage capacity or for continuity and resilience purposes). Risks associated with software hosting include internal and external malicious actors. Threat modeling may help management determine the relevant risks from these actors and implement appropriate security controls to mitigate those security risks. Refer to the *IT Handbook's* "[Information Security](#)" booklet for more information.

- **Internally hosted software:** Internally hosted (also referred to as on-premise) software refers to software that the entity hosts and manages. Usually, the internal IT department is responsible for software administration. When hosting software internally, there is a risk that the entity personnel does not have the appropriate skills and expertise to effectively manage the hosting environment. Management should identify personnel (e.g., internal or third party) with relevant skills and expertise and allocate resources to provide necessary training to maintain their knowledge. If the entity develops software, management should use a system development life cycle that incorporates security to limit the number and severity of vulnerabilities in the software.
- **Externally hosted software:** Externally hosted software (also known as hosted services) is hosted at an entity's third-party service provider. Access generally occurs through an internet connection. Hosted services may include core processing, web hosting (e.g., online banking and website), off-site backup, and virtual desktop infrastructure. Possible risks with externally hosted software include a lack of control over the infrastructure and any changes made to it by the third-party service provider. Management should have contract provisions addressing the notification of infrastructure changes and the third party's use of any subcontractors (sometimes referred to as "fourth parties"). For more information, refer to the *IT Handbook's* "[Outsourcing Technology Services](#)" booklet.
- **Hybrid hosted software arrangement:** A hybrid hosted software arrangement refers to an agreement involving software that resides at the entity (on premise) and on the third-party service provider's servers (e.g., productivity software as a service). Examples of this arrangement include the following:
 - Internally deployed software at the entity where all data are maintained on the third-party service provider's servers.

⁶² See FFIEC [Authentication in an Internet Banking Environment](#) and FFIEC [Supplement to Authentication in an Internet Banking Environment](#) for additional information.

- Software intellectual property hosted on the third-party service provider's servers and available in an "offline"⁶³ implementation (e.g., productivity software) at the entity. The software has the ability to synchronize once the user has reconnected to the third-party service provider.
- Use of a cloud service provider's infrastructure for additional capacity or for continuity and resilience purposes, when necessary, although most of the infrastructure is managed at the entity.

When operating in a hybrid hosted software arrangement, the entity may not have complete access to the software intellectual property or its data. For hybrid and externally hosted software, if full functionality of the software or data is necessary and the connection to the third-party service provider is interrupted, the entity could experience significant loss (e.g., data, functionality, or business), depending on the arrangement. Even though a level of offline functionality may be available to the entity, that functionality may be limited. When an entity depends on the third-party service provider's ability to function adequately, management should perform an adequate risk assessment to prepare for a potential service interruption.

V.D Environmental Controls

Environmental controls are mitigating strategies designed to detect and prevent against natural, mechanical, and man-made risks and threats to the entity's buildings and facilities and the affected personnel and infrastructure within them. Environmental controls include the following:

- HVAC.
- Smoke and fire.
- Water.
- Power.

Without effectively designed and implemented environmental controls, an entity's infrastructure may be exposed to risks that could reduce system resilience and reliability.⁶⁴ Environmental controls help management identify and mitigate infrastructure and operational issues, such as loss of connectivity and availability of processing caused by theft, fire, flood, mechanical failure, and power failures, in a timely manner. Management should develop, document, and implement environmental control policies and procedures to safeguard facilities, technology, data, and people. For more information, refer to the *IT Handbook's* "[Business Continuity Management](#)" booklet.

Remote monitoring systems are available to monitor the entity's infrastructure environmental controls and allow management to receive timely notifications and monitoring reports. Alerts can be sent via email or text message. These systems can be managed and monitored internally or through a third-party service provider. Any environmental controls (including IoT devices used

⁶³ Offline in this manner means that the application is still available for use when disconnected from the third-party service provider.

⁶⁴ Refer to ISO/IEC 27002:2013 [Information Security Management Chapter 11: Physical and Environmental Security](#).

for environmental monitoring) that can be managed through remote access, whether by a third-party service provider or not, should have appropriate access controls, monitoring of remote access activity, and regular review of privileges. Third-party service provider access for maintenance (e.g., system repair) and administrative purposes (e.g., billing) also should be appropriately controlled. For more information, refer to the *IT Handbook's* "[Outsourcing Technology Services](#)" and "[Information Security](#)" booklets.

V.D.2 Heating, Ventilation, and Air Conditioning

Management should implement controls to maintain appropriate temperature and humidity levels at facilities (e.g., data centers and server rooms) hosting the entity's IT infrastructure. Management should monitor HVAC. Automatic temperature and humidity controls help management identify and mitigate fluctuations that may adversely affect IT infrastructure. Commensurate with risk to the entity, management should consider implementing automated monitoring and mitigating controls that provide an alarm or notification of significant temperature changes. Management also should consider the entity's need for redundant HVAC equipment components. For more information, refer to the *IT Handbook's* "[Business Continuity Management](#)" booklet.

V.D.3 Smoke and Fire

Risks of smoke and fire to an entity's infrastructure include failed or suppressed performance of systems or complete destruction of its infrastructure. Various methods are available to detect, suppress, or extinguish fire (e.g., portable fire extinguishers or systems for air sampling, active fire suppression, wet pipe, dry pipe, pre-action,⁶⁵ gas, chemical,⁶⁶ or oxygen-removal). Management should evaluate the following:

- Determining the most appropriate smoke and fire detection systems for the entity, based on the design and contents of its facilities and infrastructure.
- Installing smoke and fire detectors in appropriate locations throughout the facility (e.g., data centers, business offices, and computer rooms).
- Implementing devices and systems for smoke detection, fire suppression, and fire detection that are supported by an independent energy source.
- Inspecting facilities for potential fire hazards using authorized and qualified inspectors and resolving identified deficiencies within an agreed-upon time frame.
- Training personnel on their roles and responsibilities.

All systems should be evaluated for their advantages and disadvantages. For example, wet pipe, dry pipe, or pre-action systems will suppress fire, but they may create problems associated with water in the facility. To provide continuous protection of facility assets, the fire suppression

⁶⁵ According to [NIST NCSTAR 1-4B, Fire Suppressions Systems](#), pre-action systems are different than both wet-pipe and dry-pipe sprinkler systems. In pre-action systems, water is not normally stored in the system piping like a wet-type sprinkler system. The water is kept out of the system of piping by a pre-action (deluge) valve until the system response is required as a result of the opening of a sprinkler and/or the activation of a detection device.

⁶⁶ These systems are also known as clean agent systems.

system should be operational even after business hours. If an entity's fire suppression system includes oxygen removal, management should be aware of potential risks to personnel with that system type and implement compensating personnel protection controls. Smoke and fire detection provisions should be addressed in the contract for the entity's third-party hosted infrastructure.

V.D.4 Water

Water use (e.g., fire suppression system, break room, restrooms, and HVAC systems) in the facility can cause damage to an entity's infrastructure. Water damage caused by environmental issues (e.g., flood or hurricane) is addressed in the *IT Handbook's* "[Business Continuity Management](#)" booklet. Water leaks under raised floors or in ceilings are not easily visible and can cause serious damage to computer equipment and cabling. For this reason, management should consider use of water detectors in both spaces to alert management in a timely manner. Commensurate with risk to the organization, management should consider automated mechanisms to detect the presence of water near IT infrastructure and provide alerts to appropriate personnel.

V.D.5 Power

Power compatibility and quality issues (e.g., appropriate power supply, power surges or sags, or inconsistent power delivery) can damage computer equipment or cause data loss or corruption. Management should take reasonable steps to protect computing equipment from inconsistent and "dirty power"⁶⁷ sources as equipment should have a consistent power source. Management should consider a long-term alternate power supply for information systems that provides the necessary operational capability in the event of extended power loss.⁶⁸ Long-term backup power can be manually or automatically activated. Management should consider using the following:

- Independent electrical feeds drawing from separate power grids. When multiple feeds or backup power generators are used, automatic fail-over to a live power source should be considered. When power is available only through one grid or one provider, management should evaluate and mitigate the risk in other ways (e.g., using generator(s) or batteries).
- Methods to monitor, condition, or stabilize the electricity source voltage to minimize the effects of power fluctuations with specialized devices (e.g., surge protectors or capacitors).
- Appropriate power configurations based on the entity's power needs.
- Alternative, or backup, power sources for IT facilities independent of local power grids. Those sources could include a combination of uninterruptible power supply (also referred to as UPS) and generators⁶⁹ powered by diesel or natural gas, and management should consider

⁶⁷ Refer to Martzloff, François, "[A New IEC Standard on the Measurement of Power Quality Parameters.](#)" The report uses dirty power to describe a power line where disturbances (e.g., outages, voltage spikes, and drop-outs) occur. NIST, 2000.

⁶⁸ Refer to [NIST SP 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations - PE-11 Emergency Power.](#)

⁶⁹ The generator should run on something other than electricity.

the risks of these options. These may be used to mitigate disruptions, allow an orderly power down of systems, or transition systems to a longer-term alternate power source.

- Processes to power down IT systems in an orderly manner to maintain critical information for later recovery, in cases where power cannot be maintained (e.g., during emergencies).
- Automated emergency lighting that activates to illuminate the entity's critical infrastructure, evacuation routes, and emergency exits, in the event of a power outage or disruption.

V.E Physical Access Controls

Physical access controls are mitigations that protect an entity's facilities, physical assets, and technology assets.⁷⁰ Unauthorized access can negatively affect the confidentiality, integrity, and availability of the entity's information and technology assets and the business operations supported by them. Therefore, management should consider physical access controls when building or modifying an entity's infrastructure environment. Management should implement appropriate physical access controls such as the following for the infrastructure and for locations that house the infrastructure:

- Generate and maintain a list of approved individuals with authorized physical access to the facilities housing IT infrastructure.
- Validate access authorizations before granting access to restricted spaces (e.g., data centers, computer rooms, and sensitive work areas).
- Issue credentials (e.g., badges, ID cards, and smart cards) for entity personnel and visitor badges for non-entity personnel (e.g., third-party service provider personnel).
- Maintain and review logs of individuals that access restricted spaces.
- Monitor physical intrusion alarms and surveillance equipment.
- Escort visitors and monitor visitor activity.
- Secure combinations, keys, and other physical access devices, and change combinations or keys when combinations are compromised, keys are lost, or staff is transferred or terminated. Any electronic user credentials should be removed or updated in a timely manner.
- Review inventory of physical access devices at regular intervals.
- Review access lists regularly and remove access for individuals who no longer require access.
- Implement alternative physical access processes in case electronic controls fail (e.g., during power failures).

⁷⁰ Refer to [NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations - PE-3 Physical Access Control](#).

VI OPERATIONS

Operations are the performance of activities comprising methods, principles, processes, procedures, and services that support business functions. For the purposes of this booklet, IT operations include the tactical management of technology assets and daily delivery of services to capture, transmit, process, and store transactions and information that support the entity's overall business processes.

The operational environment includes the systems and facilities that the entity uses to run its business processes and operations. Operations functions are sometimes referred to as “back-office” functions because they are traditionally carried out in locations away from customer-facing functions. Operations functions are the “nerve center” of an entity and encompass the day-to-day processing and support functions, service delivery and service management, and control processes to support both the operations and overall mission of the entity. The operational environment is addressed in the following subsections:

- Operational controls.
- IT operational processes.
- Service and support processes.
- Ongoing monitoring and evaluation processes.

VI.B Operational Controls

Action Summary

Management should develop and implement operational controls to safeguard the entity's operational environment. These controls should be designed to protect the overall environment, including the physical facilities, infrastructure supporting the entity's operations, systems and software, and personnel.

Examiners should review for the following:

- Effective controls over the entity's operating centers, including physical and logical controls.
- Defined and appropriately administered authorization boundaries containing the entity's systems, software, and information.
- IAM methods used to appropriately identify and authenticate authorized users.
- Personnel controls (e.g., hiring and retention practices, maintaining appropriate skillsets and knowledge, and activity monitoring processes) to maintain an effective workforce.
- Controls allowing for the use of personally owned devices.

Operational controls are the day-to-day procedures and mechanisms used to protect operational systems and software. Operational controls affect the system and software environment. Because

the system and software environment(s) are the foundation for the entity's business processes, management should define processes and implement controls to protect the entity's operational environment(s). This includes the use of operating centers, authorization boundaries, IAM controls, personnel controls, and controls for the use of personally owned devices.

VI.B.1 Operating Centers

Operating centers can be physical or cloud-based and either entity-owned or outsourced. In entity-owned operating centers, management is responsible for the physical location as well as the on-premise equipment and systems. Operating centers may be owned and managed by a third party or may be on the entity's premises but managed by a third party. In outsourced operating centers, management may be responsible for the equipment, but not the physical location. If a third party is involved in operating center activities, the contract should specify equipment ownership and responsibility. Regardless of the operating center type or its ownership, management remains responsible for the oversight of those activities. Typical operating centers include the following:

- **Data center:** The location where the entity houses and maintains its processing, data, storage, and communications systems and equipment. Data centers may be on premise, at a third-party location, co-located, or operate in the cloud.
- **Network operations center (also referred to as NOC):** The NOC is the organization responsible for monitoring the health and performance of the network, including analyzing and maintaining network traffic.
- **Security operations center (also referred to as SOC):** The SOC is the organization responsible for monitoring the entity's network for security issues and responding to cyber attacks.

In smaller or less complex entities, there may not be separate operating centers. For example, the entity may have only a server room or closet. The key responsibilities and functions (e.g., security and network management) in operating centers should still be addressed.

Management should maintain operating centers in physical locations less prone to environmental threats (e.g., away from flood plains or terrorist targets). Management should use appropriate security and environmental controls within its infrastructure to meet the entity's operational needs:

- Smoke, water, and power detection and mitigation devices and systems, as well as fire suppression systems.
- Security zones to limit access within restricted spaces.
- Physical security controls (e.g., security partitions that reach the ceiling and windows that do not open).
- Devices to restrict and log access to the site (e.g., badges, access cards and systems, keypads, and cameras).
- Procedures outlining appropriate site maintenance (e.g., dust-free environment, limitation of paper or cardboard box storage, and restrictions on flammable chemicals or materials).

Management should designate responsibilities for implementing these security and environmental controls. Whether centralized or decentralized, operating center responsibilities also should include training staff to operate and maintain the entity's equipment and systems (e.g., monitoring of environmental systems and procedures for manual intervention and overrides), deploying appropriate connectivity, and managing incidents and events. As part of its responsibilities, operating center personnel often provide logistical support for disaster recovery and business continuity testing for the operating center and business lines. Logistical support may include switching processing from production to alternate sites and systems. Refer to the *IT Handbook's* "[Business Continuity Management](#)" booklet for more information.

VI.B.2 Authorization Boundary

An authorization boundary is important in maintaining the confidentiality, integrity, and availability of the entity's sensitive customer and corporate information. Within each boundary are discrete, identifiable technology assets that represent the building blocks of the information system. In conjunction with the entity's ITAM inventories, management should define the necessary authorization boundaries and implement appropriate security controls. Maintaining multiple authorization boundaries can help mitigate the spread of malware infiltration during a breach. Management should implement appropriate controls (e.g., VPN or demilitarized zone) over internal and external communication systems within and across the entity's authorization boundaries and with third parties (e.g., service providers and other external entities). Authorization boundaries are composed of the following:

- Physical, logical, and environmental controls.
- Perimeter protection devices.
- Internal and external communication systems.
- People and processes supporting the entity's missions and business functions.

Defining authorization boundaries provides management with the ability to centrally and consistently manage its systems and facilities. It enhances visibility across the entity's segmented infrastructure and operations environment for mitigation, maintenance, and incident response within a particular authorization boundary.

VI.B.3 Identity and Access Management

IAM encapsulates people, processes, and products, including technology, to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources. Management should implement appropriate IAM to provide access to the entity's resources. Given the sensitivity of the data residing on the entity's assets, management should consider enhanced authentication, especially for privileged access. Management should consider its implementation of cloud services and address the unique access control requirements for cloud environments (refer to the "[Access Control Considerations](#)" section of this booklet). Regardless of the type of operational environment, management should maintain a policy and implement related standards and procedures to identify users and restrict their access (e.g., physical, logical, cloud-based, or privileged) by job function and operational need. For more information, refer to the *IT Handbook's* "[Information Security](#)" booklet.

VI.B.4 Personnel Controls

Personnel controls are critical given the reliance on the operating centers for entity operations. Safe and sound operations rely on skilled personnel, appropriate training, and suitable technology solutions. In coordination with the operations and human resources functions, management should ensure that processes for employee recruitment, hiring, and placement provide for thorough applicant screening and background checks at the time of employment. Background checks should be performed periodically during employment at a frequency consistent with the sensitivity of the position. In addition, management should implement the following personnel controls:

- Clearly define duties, responsibilities, expectations, and accountability to help minimize employee turnover. Turnover disrupts workflow, degrades service and production quality, and increases training resource demands. Staff stability improves employee morale and the effectiveness of operations.
- Implement dual control and segregation of duties to prevent any one person from performing a complete process. The implementation of dual controls and segregation of duties deter employee dishonesty, fraud, or harm to the entity's information and technology assets and serve as a quality control mechanism.
- Independently monitor activities to prevent personnel from validating the accuracy of their own work or that of a superior.
- Implement rotation of duties to facilitate cross-training, improve depth of personnel skill, and augment succession planning.

Adequate segregation of duties is a challenge in smaller or less complex entities. In such circumstances, appropriately implemented rotation of duties can be an effective compensating control. Management should closely review and monitor activities to provide effective supervision, facilitate training, and validate control effectiveness.

VI.C IT Operational Processes

Action Summary

Management should implement effective IT operational processes to reduce the number of potential operational failures and minimize the impact of issues that occur. Management should evaluate the effectiveness of those IT operational processes and adjust them as needed.

Examiners should review for the following:

- Appropriate preventive maintenance or operational restoration processes for equipment within the facilities that support the entity's business objectives.
- Configuration management processes.
- Effective vulnerability and patch management processes.
- Backup and replication processes that facilitate recovery.
- Scheduling processes to manage and effectively use IT resources (e.g., hardware and processing time).
- Capacity management processes that support the entity's current and future strategic objectives.
- Log management processes that allow management to capture system, software, and physical access activities.
- Processes for the appropriate disposal of data and media.

VI.C.1 Maintenance

Maintenance is any act that either prevents the failure or malfunction of equipment or restores its operating capability. Preventive maintenance allows management to proactively address situations that may cause issues or disruptions. Preventive maintenance on equipment minimizes equipment failure and can lead to early detection of potential problems. It can include minor maintenance, such as cleaning peripheral equipment, and more extensive maintenance provided by the manufacturer, vendor, or maintenance contractor. Preventive maintenance includes general housekeeping to keep the data center and its equipment clean and orderly. Unless specifically authorized by management, computer operators should not repair equipment or perform other than the most routine maintenance. Even if computer operators have the requisite knowledge and experience, many hardware and software warranties disclaim liability for unauthorized maintenance or alteration. Routine maintenance by data center employees should be performed according to manufacturers' recommendations.

Maintenance schedules may vary considerably depending on the number and variety of IT systems and the volume of work processed. Preventive maintenance should follow a predetermined schedule. Operations employees should document both internal routine (if any)

and externally provided maintenance in logs and other records. Management review of these records will aid in monitoring any maintenance performed.

Usually, the manufacturer or vendor performs maintenance under contract. For leased equipment, maintenance may be part of the lease arrangement. When equipment is owned or leased from a third party, management should obtain a separate maintenance or service agreement between the entity and the equipment manufacturer or the third party. The service or maintenance agreement should detail the preventive maintenance to be performed, provide for repair services, and include a schedule for maintenance, as well as a time frame for repair.

Management should schedule time and resources for preventive maintenance and coordinate that schedule with production. During scheduled maintenance, management should:

- Limit the service representative's access to the minimum necessary for maintenance on the system.
- Have at least one computer operator present when the service representative is in the computer room or data center.
- Review system activity logs to monitor access to programs or data during maintenance.

When an entity uses hardware from more than one manufacturer, it may be helpful to have an arrangement with a single contractor to manage the entity's preventive maintenance and repair services. The contract or agreement should guarantee timely performance of maintenance.

Some vendors can perform computer maintenance online. Operations personnel should be aware of the online maintenance schedule, so it does not interfere with normal operations and processing. Whether maintenance occurs online or in person, the entity's operations and information security personnel should follow established security procedures to ensure they grant only the necessary access to authorized maintenance personnel at predetermined times to perform specific tasks.

Operations personnel should maintain a log of all hardware or software problems and downtime encountered between maintenance sessions. A periodic report on the nature and frequency of problems is an important management tool and can be valuable for vendor selection, equipment benchmarking, replacement decisions, or planning for increased equipment capacity. Refer to the *IT Handbook's* "[Outsourcing Technology Services](#)" booklet for additional information on managing activities performed by third-party service providers.

VI.C.2 Configuration Management

Configuration management is a collection of activities focused on establishing and maintaining the integrity of IT products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. For a configuration management process to be effective, management should have policies, standards, and procedures and define and implement appropriate configuration settings. In the context of configuration management, configuration settings are the set of parameters that can be changed in hardware, software, or

firmware that affect the security posture and/or functionality of the information system.⁷¹ Defining and applying configuration settings on IT products are important components in operational assurance, along with assessing security controls and conducting a continuous monitoring program. Management should ensure that systems and software used to support the operations of the entity not only have appropriate configuration management capabilities, including configuration of audit log settings, but that the configuration management is enforced. Refer to the *IT Handbook's* "[Information Security](#)" and "[Development and Acquisition](#)" booklets for more information on configuration management.

VI.C.3 Vulnerability and Patch Management

Vulnerability management is a process to continuously acquire, assess, and take action on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Part of vulnerability management is patch management. Patch management is the systematic notification, identification, deployment, installation, and verification of OS and application software code revisions.⁷² Vulnerability and patch management are shared responsibilities among an entity's operations and information security personnel. Management should establish procedures to stay abreast of system vulnerabilities and software vendor patches, test the patches in a segregated environment, and install them when appropriate. Refer to the *IT Handbook's* "[Information Security](#)" booklet for more information on vulnerability and patch management.

VI.B.3(a) Vulnerability Management

To have systems that are operationally functional and secure and perform as intended, management should implement a vulnerability management program that identifies systems and software vulnerabilities, prioritizes the vulnerabilities and the affected systems in order of risk, and performs timely remediation, according to the risk associated with the vulnerability. The program should include an entity's systems and software⁷³ operating in the cloud for which the entity is responsible and those managed by the entity on its premises. Management should monitor industry third parties (e.g., United States Computer Emergency Readiness Team [US-CERT⁷⁴], NIST, and Financial Services Information Sharing and Analysis Center [FS-ISAC⁷⁵]) that report vulnerability exposures and address any relevant exposures within the entity's systems and software.

⁷¹ Refer to [NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations - PE-3 Physical Access Control](#).

⁷² Examples of software code revisions include patches, hot fixes, and service packs.

⁷³ Examples of systems and software include a port, web application, database, wireless, Bluetooth, and container orchestration.

⁷⁴ The [US-CERT](#) is an organization within the Department of Homeland Security's (DHS) Cyber Security and Infrastructure Security Agency (CISA).

⁷⁵ Refer to [FS-ISAC](#).

Management should implement a process to periodically assess systems and software for vulnerabilities using scanners that are updated with a current vulnerability list. The scans should include all systems and software in the entity's hardware, software, and telecommunications inventories. As with other software tools and utilities, management should implement appropriate controls over vulnerability scanning tools. Controls to protect against unauthorized use or access to sensitive information through the tools include separation of duties, logical security, configuration management, and log review.⁷⁶ The team or person performing the scans should use a dedicated account for authenticated vulnerability scans,⁷⁷ which should not be used for any other administrative activities.

Vulnerabilities are not limited to system or software. Inadequate operational processes can create additional vulnerabilities, exposing entities to unnecessary risk. These vulnerabilities can include weaknesses in security procedures, physical layout, or internal controls that malicious users could exploit to gain unauthorized access to systems or information or to disrupt critical services. Management should have a method to track and report on the remediation progress of all identified vulnerabilities.

VI.B.3(b) *Patch Management*

An important function within operations is patch management. In conjunction with other cyber hygiene practices, a patch management program will allow management to proactively address technology-related system vulnerabilities. An entity's change management procedures should include documentation of any patch installations.

Keeping up with patches in a timely manner is labor-intensive and difficult to manage even for less complex entities; therefore, management should implement automated patch management systems and software to ensure that all network components (e.g., servers, VMs, routers, switches, mobile devices, and firewalls) are appropriately updated. Management should maintain a record of the versions in place and regularly monitor the internet and other resources for information on product enhancements, security issues, patches or upgrades, or other problems with versions of the software in the entity's inventory. Management should be aware of and communicate with its third-party service providers on the need to integrate the entity's patch management program with the third-party service provider's patches or other changes. Refer to the *IT Handbook's* "[Outsourcing Technology Services](#)" booklet. For entities using a cloud environment, management may employ a highly automated update and patch process. Systems and software are often completely rebuilt rather than updated or patched. Refer to the *IT Handbook's* "[Information Security](#)" booklet for more information on patch management.

⁷⁶ Refer to the [Center for Internet Security](#) (also referred to as CIS) Control 3, Continuous Vulnerability Management.

⁷⁷ The University of California at Berkeley's Information Security Office defines an authenticated scan as an essential tool to obtain accurate vulnerability information on covered devices by authenticating to scanned devices to obtain detailed and sensitive information about the OS and installed software, including configuration issues and missing security patches.

VI.C.4 Backup and Replication Processes

A backup is a copy of files and programs made to facilitate recovery. For systems, the backup process includes copying information to a redundant system (e.g., hardware, services, devices, or media) that can provide the same processing capability when the primary system is unavailable. Backups give management the ability to recover operations within a specified time frame, allowing business continuity with limited disruption. Replication involves the use of redundant software or hardware elements to provide availability and fault-tolerant capabilities. Backup and replication processes are shared responsibilities among an entity's operations and business continuity personnel. The decision to implement a specific backup method, including replication, should be based on the risk and criticality of the systems and data.

Management should maintain the following:

- Policies, standards, and procedures that document the entity's backup methodologies, delineate responsibilities of personnel, and promote uniform performance throughout the entity.
- Inventories of backup media, storage location, and access controls for the media or physical location.
- Documented periodic physical reviews to confirm that all relevant backup material is available.
- Procedures to verify adherence to backup schedules.
- Processes to regularly test backup copies for readability.
- Capability to restore operations to a previous trusted state.
- Backups of configurations and data off-site and on a separate system or media.
- VM versioning, replication, and life cycle policies for backup processes.
- Data encryption and access controls to protect backup or replicated data from unauthorized access, destruction, or corruption.⁷⁸
- Proper sanitization⁷⁹ and disposal of data when they are no longer needed to prevent the disclosure of information to unauthorized users.

For entities that rely on third-party service providers, including cloud service providers, to manage backup and replication processes, management should validate that the third-party service provider performs the processes above.

Refer to the *IT Handbook's* "[Business Continuity Management](#)" and "[Information Security](#)" booklets for more information on backup and replication processes.

⁷⁸ Refer to the U.S. Department of Homeland Security's [Cloud Security Strategy: .gov Cloud Security Baseline](#).

⁷⁹ [NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations](#), states that "sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal."

VI.C.5 Scheduling

In IT, job scheduling is the planning and managing of the execution of software tasks that are required as part of an IT service. IT operations management is responsible for scheduling, which is often automated using software tools that run batch or online tasks at specific times of the day, week, month, or year. Scheduling allows management to allocate resources to limit downtime and ensure adequate use of servers and processing equipment. Management should implement policies, standards, and procedures for creating and changing job schedules and analyzing and maximizing the entity's resources. Automated scheduling tools can help improve management's ability to analyze and maximize scheduling efficiency. In addition to routine scheduling, these tools may be used to assign priorities and allocate computer resources to non-routine processing.

VI.C.6 Capacity Management

Capacity management is the process of planning and monitoring an entity's technology resources to support current and future strategic objectives. It involves the use of baseline performance data to model and project an entity's future needs. Capacity management should be closely integrated with the budgeting and strategic planning processes. Management should implement capacity management processes that address internal factors (e.g., growth, mergers, acquisitions, new product lines, and implementation of new technologies) and external factors (e.g., shift in customer preferences, competitor capability, and market requirements).

Capacity management activities can be supported by automated tools to allow management to more easily analyze the information it receives. Management should routinely assess capacity against baselines to ensure adequate performance in the following:

- Platform processing speed.
- Primary working memory⁸⁰ for each platform's central processing unit (CPU).
- Additional data storage capacity.
- Voice and data communication bandwidth.

Management should analyze capacity trends to ensure that capacity continues to meet entity needs. When appropriate, management should analyze help desk records to determine whether incidents were caused by capacity issues. Management should periodically analyze projected versus actual capacity to determine whether capacity planning processes are appropriate or should be adjusted.

As part of its planning processes, management should consider testing applications and systems to verify that they will meet the entity's demands during periods of high volume. Periodically, IT management should meet with business line management to determine whether future projects may affect the entity's capacity needs. When building or acquiring new technology, management should consider flexibility to accommodate the entity's future capacity requirements. As a part of

⁸⁰ For the purposes of this booklet, primary working memory refers to the temporary storage or memory needed to run software applications that is shipped with the CPU and is generally supplemented by additional data storage (i.e., long-term storage).

sound capacity planning, management should evaluate third-party service providers' performance in combination with internal performance to help determine whether existing demands are being met and future demands can be achieved.

VI.C.7 Log Management

Log management is the process to generate, transmit, store, analyze, and dispose of log data. With respect to operations, a log is a record of events occurring within an entity's systems and networks. Management should have a process to use logs to identify, track, analyze, and resolve problems that occur during day-to-day operations. Logs may record activity performed on the entity's systems and software (e.g., OS, software application, network device, or security system). The entity may use specifically designed monitoring software or devices to capture logs. Logs are often used to track user access, system messages, and device performance and capacity. Examples of logs include:

- Occurrence (e.g., successful backups, last malware scanned, signature updates, patch installation, and system events).
- Anomaly (e.g., failed backups, failed log-on attempts, and suspicious activity).
- Usage (e.g., capacity).
- Activity (e.g., intrusion detection and protection actions taken, authentication success and failure, and blocked traffic).

Analyzing logs allows management to troubleshoot problems, investigate malicious activity, understand the entity's baseline activities, and support improvement activities. A challenge of log management is balancing the amount of data collected, the storage and capacity available, the ability to analyze the data, and the capability to respond to issues raised through that analysis. At times, the amount of data collected can make it difficult to identify anomalies. Another issue management should address is identifying and dispositioning false positives. Once false positives are identified, management should adjust logging parameters to minimize the volume of false positives in future log reviews. Log management is a shared responsibility among an entity's operations and information security personnel. Management should implement policies, standards, and procedures for log management activities that address the following:

- Objectives for logging.
- Types of logs to be collected.
- Controls to restrict access to log settings.
- Response time for log review (e.g., real-time).
- Retention time frames and storage policies of logs.
- Escalation processes for anomalies.

Management should configure logging to match the entity's risk and complexity and identify and address anomalies. Because logs can be large and difficult to analyze by humans, management should consider using tools to automate log analysis and extract important events or patterns. Automated tools can help identify anomalies and automatically alert management to potential issues or events. Management should implement controls to protect logs to preserve their

integrity and prevent log information from being misused. Refer to the *IT Handbook's* "[Information Security](#)" booklet for more information.

VI.C.8 Disposal of Data and Media

Management should implement policies, standards, and procedures to address media⁸¹ and equipment disposal or transfer. Disposal processes are a shared responsibility among several of an entity's functions, including operations, information security, and third-party service provider management. Controls involved in the disposal process should be risk-based relative to the sensitivity of the information as defined by the entity's data classification⁸² policy and the type of media used. The procedures should define methods for disposal based on the type of data to be removed. For example, management may choose to physically destroy media that contain customer sensitive information to prevent data recovery and misuse. Management should consider using techniques to remove data even when transferring the media between internal departments, as not all internal departments require access to sensitive or confidential information. For example, often media is reused after an employee leaves the entity; if someone in a customer-facing function with access to sensitive customer information leaves the entity, the information should be removed from the laptop before issuing it to other employees. Management should have appropriate procedures for the disposal of equipment (e.g., printers), which may contain residual data. Periodically, management should perform a review to ensure the timely disposal of decommissioned equipment.

The disposal of records stored on electronic media presents unique challenges because residual data can remain on the media after erasure. As technology evolves, techniques previously used may no longer be effective. For example, degaussing was an effective tool to remove data stored on magnetic media, but degaussing is not effective for non-magnetic media, such as flash drives. Even magnetic media has evolved to a point that additional techniques beyond degaussing should be considered. Because data can be recovered, additional disposal techniques (e.g., data destruction) should be applied to remove sensitive information. Refer to the *IT Handbook's* "[Information Security](#)" booklet for more information.

⁸¹ In the context of this booklet, media includes physical media (e.g., paper), electronic media (e.g., hard drives, disks, and removable drives), and virtualized copies.

⁸² For example, the Information Security Standards direct each financial institution to develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of "customer information" and "consumer information." Refer to 12 CFR 30, appendix B (OCC); 12 CFR 208, appendix D-2 and 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA).

VI.D Service and Support Processes

Action Summary

Management should develop and implement service and support processes. These processes should be designed to support an entity's strategic goals and objectives by preventing issues, ensuring continuous reliability and resilience, and supporting users (e.g., business lines, personnel, and customers).

Examiners should review for the following:

- Effective planning processes for service management that consider services offered, SLAs and contractual provisions, known limitations, and metrics and measurements.
- Communication processes with business line management.
- Operational support processes, controls, and mechanisms to report transmission and processing errors.
- Processes to document and track issues through resolution.
- Documented event, incident, and problem management processes.

VI.D.1 Service Management

Service management is the process of overseeing and managing an entity's activities and resources to allow management of IT functions to support and service the entity's strategic goals and objectives. The success of service management is normally gauged by the overall quality of service and proactive identification and resolution of problems. Service management functions should be designed with an emphasis on preventing issues and ensuring continuous reliability and resilience where possible. As part of its planning, management should consider the following:

- Services offered and SLAs, operational level agreements (OLAs), or contractual provisions.
- Activities performed by third-party service providers.
- Known limitations that may affect service management functions and activities (e.g., capacity issues or resource constraints).
- Applicable legal and regulatory requirements.
- Resources (e.g., human, technical, equipment, and capacity) necessary to carry out service management functions and activities.
- Metrics and measurements used to evaluate service management effectiveness.

The service management function ensures that business functions have technology available to support business objectives and end users have the resources to perform their jobs efficiently and effectively. Many entities develop service catalogs to outline the services and functions offered. The catalogs often describe the services and dependencies between services or functions.

SLAs, referred to as OLAs when used for internal service delivery, often outline business line expectations for service management and support functions (e.g., uptime requirements and response times). Documented OLAs are less common in smaller or less complex entities; business line management, however, should still communicate and coordinate its business requirements to personnel responsible for the execution of service management functions. OLAs and requirements may act as a baseline for any SLAs with third-party service providers. When an entity uses third-party service providers, management should coordinate its processes with them to ensure seamless functionality to the entity's lines of business.

As technology continues to evolve, more entities are aligning IT with business processes to simplify IT activities and to increase business line satisfaction. For example, several entities have implemented staff self-service processes to handle support tasks, such as hardware or software requests or password resets.

Periodically, the process owners from both business and technology functions should meet to discuss known issues, changes in progress, and future changes. These meetings help ensure that service management continues to support operations and the lines of business.

VI.D.2 Operational Support

Operational support personnel perform activities that either directly or indirectly support the entity's lines of business. Management in the lines of business may not have insight into the activities performed by operational personnel or into supporting systems or software. Management should implement the following:

- Processes to verify that incoming data transmissions and processing are complete and accurate.
- Controls to verify that external data transmissions and processing are securely received in accordance with entity policies, procedures, and standards.
- Controls to verify that data were not corrupted during transmission or as a result of processing failures.
- Mechanisms to report transmission and processing errors.

Operational support personnel should report any errors or problems with the systems or software to management in the lines of business and provide frequent updates on the resolution of issues.

VI.D.3 IT Support

IT support provides the entity's personnel and clients with technical assistance; troubleshooting advice regarding software, hardware, or networks; and assistance with events, incidents, or problems. In some entities, this function may be referred to as client support, help desk, or service desk. IT support may consist of dedicated staff trained in problem resolution, equipped with issue tracking software, and supported with knowledge-based systems that serve as a resource for common problems. In smaller or less complex entities, IT support may consist of a single person or a small staff or provided through a contract with a third-party service provider.

Larger or more complex entities often use documented service requests within a system to track their activities and the actions taken. Smaller or less complex entities often track and fulfill business requests through less formal processes. A tracking system helps management prioritize issues, track problems through resolution, and analyze the problem database for systemic concerns. A tracking system can be used to monitor IT support performance. Some tracking systems allow users to monitor problem resolution. Known issues and related fixes or resolutions should be documented in the system.

IT support should record and track incoming issues, whether handled by human operators or automated systems. Tracking requests creates a historical record and allows management to perform trend analysis. The tracking system documentation should include the following:

- User name and contact information.
- Problem description.
- Request type and category.
- Affected system (e.g., hardware, software, or other device).
- Prioritization code.
- Current status toward resolution.
- Individual or group responsible for resolution.
- Root cause, when identified.
- Target resolution time frame.
- Comments related to user interaction (e.g., number of calls for resolution) with IT support and any other pertinent information (e.g., resolution attempts).

Management should maintain well-trained and knowledgeable IT support personnel to effectively support clients and users. If IT support software is used, IT support personnel should have appropriate training to perform their duties. IT support should follow procedures to authenticate users to prevent unauthorized access to information or credentials. The entity may choose to use different levels of authentication depending on the method of contact (e.g., telephone, website, or chat), the problem reported, the type of action requested, or the platform, system, or data involved. Management should consider layered security and supplemental authentication techniques,⁸³ including out-of-band methods for changes to account maintenance activities (e.g., address or password changes) and for those involving high-risk transactions⁸⁴ to limit attempted fraud through social engineering or identify theft. Refer to the *IT Handbook's* "[Information Security](#)" booklet for more information.

If the IT support function is outsourced, management should include management's IT support expectations and responsibilities for the third-party service provider in the contract. Responsibilities may include information access level, functions it will perform, controls for security and confidentiality, and reporting and metrics to be provided. Refer to the *IT Handbook's* "[Outsourcing Technology Services](#)" booklet for more information.

⁸³ Techniques include multifactor authentication, pre-established personal identification numbers (PIN) or passphrases, and call-backs at established numbers.

⁸⁴ Refer to the FFIEC's [Supplement to Authentication in an Internet Banking Environment](#).

VI.D.4 Event, Incident, and Problem Management

Entities face a variety of events, incidents, and problems throughout the normal course of business. Managing these situations is important to minimizing disruptions on the entity's daily operations and its ability to service customers. Therefore, management of these situations is a shared responsibility among several of an entity's functions, including operations, information security, business continuity management, and third-party service provider management. Entity management may define and execute event, incident, and problem management processes differently throughout the entity (e.g., within the IT environment, at the business unit level, or at the enterprise level). To minimize confusion, management should implement processes to coordinate and define roles and responsibilities and conduct testing to identify interdependencies.

Event management is the process used to track issues that occur in the IT infrastructure and detect and escalate those issues. Incident management is the process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible. Problem management is the process employed to manage the life cycle of an entity's problems. Its goal is to proactively prevent problems from becoming incidents and lessen the impact of incidents that management cannot prevent.

Management should implement processes to plan for and manage events, incidents, and problems. Management should establish and maintain appropriate processes and controls to help protect the entity from financial, operational, and other risks. These processes should include the following:

- Identifying the event, incident, or problem.
- Determining the impact (e.g., number of customers and employees affected, revenue lost, expenses incurred, and SLAs or OLAs breached).
- Assigning a severity rating based on risk (e.g., breach of confidentiality, integrity, or availability of customer or entity data).
- Performing root cause analysis to prevent repeat incidents.
- Identifying, logging, tracking, and analyzing events, incidents, and problems that occur during day-to-day operations.
- Maintaining contact information for individuals and groups (e.g., regulators, law enforcement, internal public relations, and affected lines of business) who should be notified and the circumstances under which they should be notified.
- Informing the help desk of the event, incident, or problem and how to respond (e.g., using a script to provide information on the situation).
- Resolving the event, incident, or problem, including approval processes for system or software changes to correct the issue.
- Documenting any interim actions, compensating controls, and, if necessary, risk acceptance for issues that cannot be immediately resolved.
- Developing longer-term action plans to monitor and address issues that cannot be resolved in a timely manner.
- Reporting on the progress of the action plans to senior management.

- Implementing procedures for escalation and reporting to management and stakeholders.
- Implementing procedures to correlate events to determine whether there are underlying issues preventing resolution and allowing events to recur.

Management should consider performing periodic trend analysis to determine whether there are recurring or related issues that may be tracked to a common root cause. This would allow management to maintain systems and software and make timely changes to prevent future issues. The analysis also helps management support continuous improvement processes (refer to the “[Continuous Improvement](#)” section of this booklet for more information).

Event, incident, and problem management plans should cover hardware, software, and security devices. Situations may include issues related to confidentiality (e.g., security breaches), integrity (e.g., out-of-balance conditions or logging issues), and availability (e.g., production program failures or database corruption). Processes to manage these and other situations should be communicated and readily available to appropriate personnel.⁸⁵ Processes should be coordinated and included within the entity’s incident response program, as discussed in the *IT Handbook’s* “[Information Security](#)” and “[Business Continuity Management](#)” booklets.

VI.E Ongoing Monitoring and Evaluation Processes

Action Summary

Management should develop processes to oversee operations functions, evaluate the effectiveness of controls, and identify opportunities for improvement.

Examiners should review for the following:

- Implementation of processes to monitor and report on control effectiveness.
- Stakeholder input into the types of reports and metrics produced.
- Defined objectives for IT, operations, and key performance indicators (KPI).
- KPIs that align with the entity’s ERM processes.
- Processes for reporting KPIs to the board.
- Implementation of corrective action plans when KPIs do not meet established targets.
- Processes to recommend changes in operations processes and controls.
- Strategies for service and process improvement and methods to measure the results of those improvement efforts.

⁸⁵ Appropriate personnel include IT operations personnel, entity management, internal audit, fraud and loss prevention department, information security, computer security incident response teams, and personnel from third-party service providers.

VI.E.1 Monitoring and Reporting

Management should implement processes to monitor IT operations and periodically report on the effectiveness of established controls to senior management and other stakeholders. They should have input into the types of reports and metrics produced and reports should be understandable and useful to them. Regular monitoring can help management identify risk within operations (e.g., ineffective controls, inefficient processes, insufficient or inefficient use of resources, and substandard service delivery). The operations team should report performance metrics to senior management and other stakeholders. Operations management should meet periodically with senior management and other stakeholders to assess the value of the monitoring and reporting and to identify any changes (e.g., stakeholders, requirements, objectives, and metrics).

Monitoring and reporting support proactive systems management activities to position the entity to meet its current needs and plan for periods of growth, mergers, or expansion of product lines. Examples of IT operations reports include the following:

- Hardware and data communications capacity utilization.
- System information (e.g., system availability, system response times, and on-time processing).
- Transaction processing completeness and accuracy.
- Security-related information, such as vulnerability management metrics.
- Service-level benchmarks compared to actual service performance.
- KPIs, discussed further in the next section.

Management should monitor third-party service providers as part of the entity's third-party risk management program. Reports from third-party service providers should include effectiveness of security controls, performance metrics, resolved versus outstanding issues, and root causes of problems. Management should monitor the third-party service provider's ability to meet defined SLAs, compliance with identified action plans when they are not met, and remuneration of penalty fees when appropriate.

Entities that have migrated to a cloud computing environment may find that traditional operations monitoring and reporting tools and techniques are no longer effective. For example, encryption or containers may impede the operation and accuracy of some tools. Management should explore the use of tools designed for cloud computing, either by the cloud service provider or external vendors. Some examples of these tools include cloud service provider-offered monitoring services and third-party applications (such as CASBs or agent-based monitoring).

VI.E.2 IT and Operations Key Performance Indicators

KPIs are measures that determine how well the process is performing in enabling the goal to be reached. Management should define objectives for IT and operations and KPIs to help management measure those objectives. KPIs should align with the entity's ERM processes and allow management to assess the performance of IT and operations across the entity.

Management should set KPI benchmarks it wants to achieve and analyze deviations from those benchmarks. The collection of KPIs should be automated to the extent possible. Examples of IT and operations KPIs may include the following:

- Resource utilization by application or time of day.
- Network availability (e.g., uptime).
- Response time, access types by service, or average connect time.
- Voice response unit call capacity.
- Mobile and internet banking capacity.
- System failures.
- Help desk performance metrics (e.g., number of calls answered, average talk and wait times, total ticket duration, mean time to resolve, and percent of first contact resolution).
- Virtualization metrics (e.g., memory availability and network bandwidth).
- Change management metrics (e.g., total number of changes and number of emergency or unplanned changes).

Information gained from analysis supports daily management of operations and early alerting of potential operational issues. As part of the entity's monitoring and review processes, management should regularly review KPI reports and provide appropriate reporting up to the board, if necessary. Management should implement corrective action plans to address the deviations or negative trends, assign individuals responsible, and monitor progress to completion. Periodically, management should meet with stakeholders to review the IT and operations KPIs. Management should determine whether the KPIs are appropriate indicators to demonstrate the ability to meet the entity's strategic objectives.

In conjunction with KPIs, a common method of measuring operational risk is through the use of key risk indicators (KRI). KRIs are a subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk. Refer to the *IT Handbook's* "[Management](#)" booklet for more information on KRIs.

VI.E.3 Control Self-Assessments

A control self-assessment, sometimes referred to as a risk control self-assessment, is a technique that allows managers and work teams directly involved in business units, functions, or processes to participate in assessing the entity's risk management and control processes. Management can use these assessments to monitor the effectiveness of IT operations controls as well as to gauge performance, assess the criticality of systems, and identify existing risks. Control self-assessments do not eliminate the need for independent audits. The results should be evaluated by management and used to continuously improve the entity's operations.

VI.E.4 Continuous Improvement

Continuous improvement is the ongoing effort to improve an entity's products, services, or processes to meet business objectives. An entity's reliance on technology involves continuous innovation and the need for updated and more advanced systems. Improvement efforts in

operations can be gradual (where management makes incremental changes over time) or all at once. Regardless, continuous improvement relies on management and personnel; therefore, management should have a process in place to recommend changes.

To improve the management and governance of operations, management should develop improvement strategies for operations and prioritize projects. Management should make decisions related to improvement based on the potential benefit and ease of implementation, with a focus on important IT processes and core competencies.

Management should have a process to measure the results of continuous improvement efforts. This can be accomplished by establishing a scorecard with KPIs to measure current performance and monitor the results of new improvements. Validating these measurements could include the following:

- Implementation of organizational structures that support improvement.
- Designation of risk management responsibilities.
- Facilitation for sharing vital business information.
- Communication of strategies and goals.

There are several types of continuous improvement, including for processes and services.

- **Process improvement:** Process improvement includes the actions taken to improve the quality of the organization's processes aligned with the business needs and the needs of other concerned parties. It should be an ongoing practice as part of the entity's continuous improvement efforts. Results can include improved quality, strengthened security, increased productivity and efficiency, and improved employee skills.
- **Service improvement:** Service improvement includes the actions taken to identify and execute methods to improve an entity's services and align them with its business objectives. It should be implemented enterprise-wide and augment the entity's ability to provide value to its stakeholders and customers. Management can facilitate the entity's continuous improvement efforts through the following:
 - Maturity assessments.
 - Gap analyses.
 - Benchmarking.
 - Improvement planning.

VII EVOLVING TECHNOLOGIES

Entities use a variety of evolving technologies (e.g., cloud, zero trust architecture [ZTA], AI and ML, and IoT) that may impact architecture, infrastructure, and operations functions. This section provides general information relating to these evolving technologies and, when appropriate, certain risks and control principles discussed in prior sections of this booklet.

VII.A Cloud Computing

Cloud computing environments are enabled by virtualization technologies, which allow cloud service providers to segregate and isolate multiple clients on a common set of physical or virtual hardware. NIST defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or third-party service provider interaction.”⁸⁶ Cloud systems provide several benefits, including scalability of resources and consistency in deployment of controls across systems and software.

For the purposes of this section of the booklet, when the term “cloud service provider” is used, it refers to the provider offering cloud computing services. When the term “entity” is used, it refers to the client receiving cloud computing services.

As defined by NIST, “cloud computing has five essential characteristics, three service models, and four deployment models.”⁸⁷

VII.A.1 Essential Characteristics

According to the NIST definition, cloud implementations take advantage of all of the following five “essential characteristics.”⁸⁸ Some entities may characterize their environment as “cloud computing” without it exhibiting all five characteristics. NIST describes the five essential characteristics as follows:

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each third-party service provider.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

⁸⁶ Refer to [NIST SP 800-145, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*](#).

⁸⁷ [Ibid.](#)

⁸⁸ [Ibid.](#)

- **Resource pooling:** The cloud service provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location (e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability (e.g., storage, processing, bandwidth, and active user accounts) appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency for the provider and consumer of the utilized service.

VII.A.2 Cloud Service Models

There are generally three key cloud service models⁸⁹ used in cloud computing implementations.⁹⁰ The optimal architecture for a given application or service is determined by consideration of the entity's requirements, including data classification, data residency, service or application availability, and interfaces with external services and data stores.

NIST describes the service models⁹¹ as follows:

- **Software as a service (SaaS):** SaaS allows entities to use applications running on a cloud infrastructure. The entity does not control or manage the applications or the environment in which the applications are running, including the network, servers, OSs, storage, or individual application capabilities. In this model, the end user and the entity generally have limited ability to customize the user interface of the cloud service, with the exception of some user-specific application configuration settings.
- **Platform as a service (PaaS):** PaaS provides entities with the ability to deploy applications created or acquired by the entity using programming languages, libraries, services, and tools supported by the cloud service provider. The entity does not manage or control the cloud infrastructure (e.g., network, servers, OSs, or storage); it does control the deployed applications and possibly the configuration settings.
- **Infrastructure as a service (IaaS):** IaaS provides entities with the ability to provision processing, storage, networks, and other fundamental computing resources where the entity is able to deploy and run software, which can include OSs and applications. The entity does not manage or control the underlying cloud infrastructure; it does control OSs, storage, and

⁸⁹ Refer to [NIST SP 500-316, Framework for Cloud Usability](#).

⁹⁰ There are a variety of other cloud service models (e.g., disaster recovery as a service, backup as a service, and desktop as a service). The focus for the purposes of this booklet are the key cloud service models used here as a baseline for most others.

⁹¹ Refer to [NIST SP 500-316, Framework for Cloud Usability](#).

deployed applications. Entities have the maximum flexibility to customize their cloud services and user interfaces.

Management may choose to leverage the cloud in different ways. Some entities outsource certain applications or processes, such as storage or data backup to the cloud (as part of SaaS). Others may choose to develop their own applications; these entities, however, rely on the cloud service provider to provide and maintain the OS (as part of PaaS). Still others may choose to outsource only the physical hardware to cloud service providers, while maintaining the OS and applications themselves (as part of IaaS).

VII.A.3 Cloud Deployment Models

As with cloud service models, management can deploy cloud services in different ways. NIST describes the deployment models as follows:⁹²

- **Private cloud:** The private cloud infrastructure is provisioned for exclusive use by a single entity with multiple business units. The private cloud infrastructure may be owned, managed, and operated by the entity, a third party, or some combination of the two, and it may exist on or off premises.
- **Community cloud:** The community cloud infrastructure is provisioned for exclusive use by a specific community (e.g., government agencies, financial services, or banks) of entities that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). The community cloud infrastructure may be owned, managed, and operated by one or more of the constituents in the community, a third party, or some combination of the two, and it may exist on or off premises.
- **Public cloud:** The public cloud infrastructure is provisioned for open use by the general public. The public cloud infrastructure may be owned, managed, and operated by a business or an academic or government organization, or some combination of the two. It exists on the premises of the cloud service provider.
- **Hybrid cloud:** The hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (e.g., private, community, or public) that are unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Entities may use more than one cloud service provider for different operations or to augment continuity and resilience for operations in the cloud. The use of multiple cloud service providers may reduce single-provider reliance. Entities may rely on cloud bursting⁹³ capabilities for situations requiring increased capacity or for business continuity purposes. Entities may use a cloud broker to act as an informed intermediary between management and the cloud service provider. The use of a cloud broker may also supplement the capabilities of entity management and staff.

⁹² Refer to [NIST SP 800-145, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*](#).

⁹³ The goal of cloud bursting is to maintain required service levels for an entity's data-center hosted process, by dynamically allocating or deallocating cloud computer or storage resources to service current demands.

VII.A.4 Shared Responsibilities

In cloud computing environments, entities may outsource the management of different controls over information and technology assets and operations to the cloud service provider. Careful review of the contract between the entity and the cloud service provider along with an understanding of the division of shared responsibilities and related risks are important for implementing appropriate controls. The contract defines the service-level expectations and control responsibilities for both the entity and the cloud service provider. To maintain security consistent with an entity's internal standards, there may be a need for controls in addition to those a cloud service provider contractually offers.

Depending on the service and deployment model used, management should understand the shared responsibilities associated with cloud computing. As presented by NIST, “compared to traditional IT systems, where one organization has control over the whole stack of computing resources⁹⁴ and the entire life cycle of the systems, cloud service providers and cloud consumers collaboratively design, build, deploy, and operate cloud-based systems. The split of control means both parties now share the responsibilities in providing adequate protections to the cloud-based systems.” It is important to understand what controls are implemented by the cloud service provider for the cloud service provider's own operations and what security controls are implemented and operated to ensure the security of the entity's content and applications.

For each service model, there are typically different shared responsibilities between the entity and the cloud service provider for implementing and managing controls. The following includes some of the controls that are the responsibility of either the entity or the cloud service provider, or both in some cases, depending on the service model and contract provisions.

- Managing the underlying cloud infrastructure systems (e.g., network, servers, or storage) or software.
- Managing and implementing controls over the hypervisor(s).
- Provisioning and configuring cloud platform resources.
- Implementing user-specific application configuration settings and user access and identity management.
- Managing entity data (e.g., classifying assets and employing encryption).
- Developing and deploying software residing on the cloud service provider's platforms.
- Managing the physical data center, including environmental controls (e.g., heating, cooling, and fire and flood protection), power, physical security, and data communications connections.
- Implementing controls over data access, theft of user credentials, regulatory compliance, and data leakage.

⁹⁴ [NIST SP 500-292, NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology](#), states, “In cloud computing, a stack of computing resources refers to the group of services that the institution purchases from a cloud computing service provider.”

Figure 5. Example of Shared Responsibilities in a Cloud Computing Environment

	On Premise Responsibility	IaaS Responsibility	PaaS Responsibility	SaaS (and Traditional Outsourcing) Responsibility
Risk Management (Mgmt) / Administrative Controls	Risk Mgmt Strategy	Risk Mgmt Strategy	Risk Mgmt Strategy	Risk Mgmt Strategy
	Policy	Policy	Policy	Policy
	Organization	Organization	Organization	Organization
	App. Administration	App. Administration	App. Administration	App. Administration
	IAM/Access Controls	IAM/Access Controls	IAM/Access Controls	IAM/Access Controls
Technical Controls	Applications	Applications	Applications	Applications
	Data	Data	Data	Data
	Runtime	Runtime	Runtime	Runtime
	Middleware	Middleware	Middleware	Middleware
	OS	OS	OS	OS
	Virtualization	Virtualization	Virtualization	Virtualization
	Servers	Servers	Servers	Servers
	Storage	Storage	Storage	Storage
Physical Controls	Networking	Networking	Networking	Networking
	Facility	Facility	Facility	Facility

Note: Based on a diagram from the Cloud Security Alliance, FFIEC members augmented the diagram by adding the layer of risk management and administrative controls. This chart is an example of how the responsibilities may be divided between the entity and the cloud service provider as defined in the contract. Dark blue boxes represent the entity's responsibility. White boxes represent the cloud service provider's responsibility. Boxes shaded in light blue are examples of responsibilities that may be assigned to either or both the entity and the cloud service provider.

Regardless of the environment or service model used, the entity retains overall responsibility for the safety and soundness of cloud services and the protection of sensitive customer and entity information.⁹⁵ Refer to the *IT Handbook's* “[Outsourcing Technology Services](#)” and “[Information Security](#)” booklets for more information on third-party service provider oversight.

VII.A.5 Risk Considerations for Cloud Computing

Cloud computing is exposed to the same threats, vulnerabilities, and risks as other technology environments, whether the cloud computing environment is managed internally at the entity or at a third-party service provider. Cloud computing may involve different security control configurations and processes than those employed in more traditional network architectures. Simply moving existing network technology to the cloud may not be appropriate. Controls, policies, and procedures may not translate effectively to a cloud-based environment. There are tools (e.g., cloud access security broker) designed specifically to assist with the implementation of security controls in a cloud environment.

⁹⁵ Refer to the Information Security Standards: 12 CFR 30, appendix B (OCC); 12 CFR 208, appendix D-2, and 12 CFR 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA).

Another risk consideration is the aspect of tenancy. Applications or services can exist in single or multi-tenant environments. Control requirements may vary by tenant, with some requiring a higher level of security than others. Misuse or abuse by one tenant could potentially weaken the security posture of other tenants. Inadvertent or deliberate failure of a security control could adversely affect other tenants in the same environment. For example, a DOS attack on the cloud service provider, or even a single tenant, could affect the other tenants.

Third-party assurance reviews (e.g., SOC reviews, penetration tests, and vulnerability assessments) can provide an understanding of the cloud service provider's control environment and its ability to meet an entity's control expectations (e.g., compliance with applicable laws and regulations). Refer to the FFIEC's joint statement⁹⁶ for more information.

VII.A.5(a) *Access Control Considerations*

"Access control dictates how subjects (i.e., users and processes) can access objects based on defined access control policies to protect sensitive data and critical computing objects in the cloud systems."⁹⁷ While cloud computing offers significant flexibility, security considerations can be complicated by the various service and delivery models and shared responsibilities. In general, access control considerations for IaaS are also applicable to PaaS and SaaS, and access control considerations for PaaS are also applicable to SaaS, although variations do exist.

Challenges of access control system design are tied to the essential characteristics of cloud computing mentioned previously, plus risk from data sharing. These challenges and risk considerations include those applied to the following elements in cloud environments:

- Network
- Hypervisor
- VMs
- APIs
- Multi-tenancy
- Attribute and role management
- Data replication and destruction

When addressing these elements, additional considerations of access control in a cloud environment include:

- Cloud virtualization adds access control and security management concerns, as risk may be compounded by the volume of VMs created and changed in the cloud.
- Access control lists for networks and network boundaries, hypervisors, VMs, and APIs to define and implement appropriate levels of access on different users.
- Access control security and privacy offered by the PaaS provider to protect the applications and data from potential leaks, such as data in OS memory caches.

⁹⁶ FFIEC, [Security in a Cloud Computing Environment](#).

⁹⁷ Refer to [NIST SP 800-210, General Access Control Guidance for Cloud Systems](#).

- In SaaS, the provider should not have unnecessary or inappropriate access to SaaS systems or customer data residing on or accessible by them.
- The design of access control should include multi-tenancy situations to ensure appropriate segregation of entity data from other clients' applications.

For more information on access control and security in cloud environments, refer to NIST.⁹⁸ Refer to the *IT Handbook's* "[Information Security](#)" and "[Outsourcing Technology Services](#)" booklets for additional information.

VII.B Zero Trust Architecture

According to NIST, ZTA is "an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement."⁹⁹ As an entity's complexity increases, the entity may operate several internal networks, remote offices with their own local infrastructure, remote or mobile personnel, and cloud services.¹⁰⁰ Legacy methods of perimeter-based network security may no longer be appropriate in a more complex IT environment. If an entity's perimeter-based and internal network security is not fully effective, a breach of the perimeter can allow unhindered lateral movement inside the network. These concerns have led to the development of a model for cybersecurity known as zero trust.¹⁰¹

ZTA assumes all networks are untrusted, including internal networks. Within ZTA, implicit trust is not granted to systems and users based on their physical or network location (e.g., LANs or the internet). Access to data resources is granted only when the resource is required and authentication (for both users and devices) is performed before the connection is established. ZTA focuses on protecting resources, rather than network segments using authentication and authorization, while minimizing reliance on implicit trust zones. Additionally, it focuses on reducing delays caused by authentication methods that are not located within an entity-owned network boundary.¹⁰²

Designing for zero trust enables entities to securely accommodate the complexity of a diverse set of business cases by informing virtually all access decisions and interactions between systems.¹⁰³ Management may consider adoption of zero trust principles in architecture decisions. ZTA principles include the following:¹⁰⁴

⁹⁸ [Ibid.](#)

⁹⁹ [NIST SP 800-207, Zero Trust Architecture.](#)

¹⁰⁰ [Ibid.](#)

¹⁰¹ [Ibid.](#)

¹⁰² [Ibid.](#)

¹⁰³ [Ibid.](#)

¹⁰⁴ Principles are derived from [NIST SP 800-207, Zero Trust Architecture.](#)

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual entity resources is granted on a per-session basis and in a secure manner regardless of network location, user, or device.
- Authentication and authorization for access to resources are determined by user and device analytics and behavioral attributes (e.g., network location, device characteristics, and access time or day) compared to deviations from baselined patterns.
- Rigorous access controls (e.g., using least privilege and granular trust zones around an entity's digital resources) are enforced. These controls include data-level protections, robust identity architecture, and strategic micro-segmentation.
- Owned and associated devices are monitored to ensure that they remain in the most secure state possible. The entity continually inspects, monitors, and logs network traffic and uses the information to improve its security posture.
- Evaluation of access requests and network traffic behaviors occurs in real time over the length of open connections while continually and consistently reassessing access to the entity's resources.

VII.C Microservices

Microservices are a set of containers that work together to compose an application. Essentially, each microservice is an independent building block used for building an application, including the communications and authentication. Each microservice is a mini application loosely coupled¹⁰⁵ to serve a singular function (e.g., database access or messaging) that can be integrated to collectively build an application. During the communication events of any pair of interactions (e.g., client-to-microservice, microservice-to-microservice, or microservice-to-egress service), each party has distinct identities and performs mutual authentication.

Each microservice typically implements one (rarely more) distinct business process or functionality (e.g., storing customer details or displaying a product catalog). NIST 800-204A¹⁰⁶ states that a microservice has two broad functions:

- Business logic, which implements the business functionalities, computations, and service composition or integration logic.
- Network functions, which manage the inter-service communication mechanisms and are built on top of the underlying OS level network stack.

Microservices software is used in architecture designs where complex applications are composed of small, independent services that exchange data and procedural requests. Microservices-based application architectures provide inherent scalability, agility of deployment, and availability of

¹⁰⁵ NIST SP 800-204, [Security Strategies for Microservices-based Application Systems](#), states, "For large applications, splitting the application into loosely coupled components enables independence between the developer teams assigned to each component. Each team can then optimize by choosing its own development platform, tools, language, middleware, and hardware based on their appropriateness for the component being developed."

¹⁰⁶ Refer to [NIST SP 800-204A, Building Secure Microservices-based Applications Using Service-Mesh Architecture](#).

tools to facilitate error-free configuration and deployment. Although a microservices-based application can be implemented purely as an enterprise application, it is generally identified as a cloud-native application that includes service-based architecture, API-driven communications, and container-based infrastructure.¹⁰⁷

The implementation of microservices infrastructure differs from legacy distributed systems as there are multiple services configured to operate at designated locations (IP address and port number). When using microservices-based applications, the following are key elements¹⁰⁸ to consider in the entity's infrastructure:

- There are a substantial number of services and many instances associated with each service with dynamically changing locations.
- The number of instances associated with a service can vary based on the load fluctuations using features such as autoscaling.
- A feature to discover a service while making a service request. A common approach to implementing this feature is the use of a service registry.¹⁰⁹
- Each of the microservices may be implemented in VMs or as containers, which may be assigned dynamic IP addresses, especially when they are hosted in an IaaS or SaaS cloud service.
- Load balancing is needed for multiple instances of the same service where the loads on these instances should be evenly distributed to avoid delayed responses or service crashes due to overload.¹¹⁰
- Microservices take advantage of a variety of features,¹¹¹ including:
 - Circuit breakers.¹¹²
 - Rate limiting, or throttling.
 - Version control.
 - Canary releases.¹¹³

The increasing adoption of microservices-based applications in cloud and large enterprise environments has prompted the identification of an infrastructure that provides a comprehensive,

¹⁰⁷ Refer to NIST SP 800-204, [Security Strategies for Microservices-based Application Systems](#).

¹⁰⁸ NIST discusses several key elements for consideration in [NIST SP 800-204A, Building Secure Microservices-based Applications Using Service-Mesh Architecture](#).

¹⁰⁹ A service registry consists of a directory where new service instances created for the microservices-based application register themselves while service instances going offline are deleted from it.

¹¹⁰ Refer to [NIST SP 800-204A, Building Secure Microservices-based Applications Using Service-Mesh Architecture](#).

¹¹¹ [Ibid.](#)

¹¹² Using circuit breakers involves setting a threshold for the failed responses from an instance of a microservice and cutting off forwarding requests to that instance when the failure is above the threshold (e.g., when the circuit breaker trips).

¹¹³ Canary releases serve as an early warning system for potential problems with the microservices.

consistent, and coordinated set of support services.¹¹⁴ Service mesh and API gateways are examples of this infrastructure. In operations related to microservices, there are additional security considerations,¹¹⁵ including the following:

- The sheer number of microservices results in more interconnections and more communication links to be protected, such as through the use of ingress and egress controllers.
- The short-term and promiscuous (i.e., used by many different applications and platforms) nature of microservices calls for secure service discovery mechanisms to make sure they are registered correctly when created and removed when replaced with a new version.
- The detailed level at which microservices are built should include the ability to support the entity's security and authorization policies.
- The supporting services (e.g., authentication, authorization, and security monitoring) for microservices-based applications should be coordinated through a dedicated infrastructure.
- There is no concept of a network perimeter.
- All microservices should be treated as non-trustworthy.

The detailed nature of microservices may prompt management to centrally define security policies and configurations to enable uniform, consistent implementation across all microservices.

VII.D Artificial Intelligence and Machine Learning

AI refers to the theory and development of systems that perform tasks or functions normally associated with human intelligence, such as reasoning, learning, and self-improvement. ML is a subset of AI in which components of AI systems are used to design a sequence of actions, which could improve upon and optimize algorithms automatically through experience, to perform tasks with limited human intervention.

AI algorithms can analyze large data sets quickly and identify complex patterns, which may be used to solve problems and generate predictions or categorizations. AI can allow management to personalize customer products and services and, in certain cases, analyze real-time data to help anticipate future customer behavior. AI can also augment decision-making by identifying patterns that a human may miss when analyzing data. The automation of recurring processes and decision making can result in operational and productivity efficiencies (e.g., time and personnel reduction) by reducing human intervention.

Entities may use AI for several activities, including the following examples:

- Detection and prevention of fraud or misconduct (e.g., anti-money laundering, account compromise, and insider fraud) to reduce losses.

¹¹⁴ Refer to [NIST SP 800-204A, *Building Secure Microservices-based Applications Using Service-Mesh Architecture*](#).

¹¹⁵ [Ibid.](#)

- Identification, notification, and mitigation of cybersecurity breaches.
- Facilitation of automated trading (e.g., algorithmic trading).¹¹⁶
- Automation and augmentation of loan origination process, including consumer credit scoring.
- Risk management and business decision-making.
- Strengthening security controls (e.g., logical and physical access anomaly analysis and use of facial recognition for authentication).
- Compliance with applicable laws and regulations.

There are a number of risks related to the use of AI or ML. It relies on large amounts of available data, which, if breached, can result in misuse of data, fraud, financial loss, or harm to consumers. There is the potential for human errors of omission or commission in the development of algorithms that can lead to incorrect decisions. Also, there is the potential for bias (intentional or unintentional) in algorithm development and use if it is not tested and validated, as well as used appropriately. For additional information on testing and validation in development, refer to the *IT Handbook's* "[Development and Acquisition](#)" booklet.

AI can lack transparency, or explainability, meaning the processing approach is difficult to follow and it can be unclear how inputs are translated into outputs. This lack of explainability can limit the understanding of the approach and affect the confidence in the reliability of the results of AI. It can also result in unintended consequences (e.g., noncompliance with applicable regulations or exceeding the entity's risk tolerance).

Another potential risk with AI is the ability to evolve on its own. This provides the ability to modify existing (or introduce new) AI variables or features without human interaction. This is known as dynamic updating, which can present challenges to monitoring and independently reviewing AI.

VII.E Internet of Things

IoT refers to the collection of technologies that allow information to be sent to and received from physical devices (e.g., security systems, HVAC systems, intelligent personal assistants, smart televisions, and other appliances), not considered previously to be IT assets, using the internet. These devices have the ability to send and receive data over a network without necessarily requiring human-to-human or human-to-computer interaction, using embedded computing capability and network connectivity and unique identifiers (e.g., IP address). IoT leverages cloud computing, mobile computing, big data, and other emerging technologies to deliver functionality. Data gathered through IoT can be used by the entity to aid in management's decision-making through improved statistical models and algorithms. IoT is found in every sector, ranging from mobile payment systems on watches and phones to internet-connected medical devices and home security devices.

¹¹⁶ In [algorithmic trading](#), firms use computers programmed with specific algorithms—sequences of steps—to identify trading opportunities and execute orders.

Because IoT includes computing devices connected to the internet and can execute code, there are a number of risks related to their use.¹¹⁷

- IoT devices interact with the physical world in ways conventional IT devices usually do not. IoT devices can make changes to physical systems; operational requirements for confidentiality, integrity, and availability of these devices, however, may be at odds with common cybersecurity and privacy practices for conventional IT devices. For example, security requirements for online and mobile payment channels often are more stringent than making purchases or payments using an intelligent personal assistant device.
- Many IoT devices cannot be accessed, managed, or monitored in the same ways as conventional IT devices. For example, most IoT devices do not support standardized mechanisms for centralized management. Administrators may not be able to fully manage an IoT device's firmware, OS, and applications. Unavailable features may include the ability to acquire, verify the integrity of, install, configure, store, retrieve, execute, terminate, remove, replace, update, and patch software. Some IoT devices lack application or human user interfaces for device use and management. When such interfaces do exist, they may not provide the functionality usually offered by conventional IT devices. In some cases, only manufacturers can perform maintenance, such as installing patches.
- An IoT device's software may be automatically reconfigured when an adverse event occurs, such as a power failure or a loss of network connectivity. For example, the security settings for an IoT device may all be reset to the default settings.
- The entity may not know what capabilities an IoT device can provide or is currently providing. The device may transfer data to manufacturer-provided cloud-based service processing and storage. Data may be sent to a cloud service to aggregate data from multiple IoT devices in a single location. These cloud services may provide access to portions of or all the devices' data, or even access to and control of the devices, for monitoring, maintenance, and troubleshooting purposes.
- There may be little or no information available about device ownership. The lack of accountability limits individuals' abilities to locate the source of and correct or delete information about themselves, or to address other problems (e.g., privacy).
- Data may still be available on some IoT devices after disposing of or transferring ownership of a device.
- IoT devices used in an entity may not be inventoried, registered, or otherwise provisioned via the normal IT processes. Previous iterations of those devices did not have networking capabilities (e.g., smart TVs that connect to an entity's network to provide teleconferencing capabilities). IoT devices often use protocols that cybersecurity and privacy controls for conventional IT cannot understand and analyze; therefore, standard network scanning devices may not recognize IoT devices (including personally owned IoT devices).

IoT devices have a number of often-unknown capabilities; therefore, it is important to understand those capabilities, the related risks, and the data devices can access. As IoT devices are relatively easy to install, it is important to understand how many devices there are and where they are used and should be considered in an entity's ITAM inventory process.

¹¹⁷ These risks are derived from [NIST IR 8228, *Considerations for Managing Internet of Things \(IoT\) Cybersecurity and Privacy Risks*](#).

APPENDIX A: EXAMINATION PROCEDURES

Examination Objectives

These examination procedures (also known as the work program) are intended to assist examiners in determining the quality and effectiveness of the entity's AIO functions and their related activities. Examiners are not limited¹¹⁸ by the examination procedures presented here and may choose to use only certain components of the work program based on the size, complexity, and nature of the entity's business. Depending on the examination scope and objectives, examiners may sample processes related to a particular line of business or review the process at an enterprise level.

Objective 1: Determine the appropriate scope and objectives for the examination.

1. Review past reports for outstanding issues or previous problems. Consider the following:
 - a. Regulatory reports of examination.
 - b. Internal and external audit reports.
 - c. Reports by independent risk management.
 - d. Independent assurance and security reports (e.g., penetration tests and vulnerability assessments) and internal reports that self-identify concerns related to AIO issues.
 - e. Regulatory, audit, and SOC reports on the entity's third-party service providers.
 - f. The entity's overall risk assessment and profile.
2. Review management's response to issues identified during or subsequent to the last examination. Consider the following:
 - a. Adequacy and timing of corrective action.
 - b. Resolution of root causes rather than symptoms.
 - c. Status of uncorrected issues.
 - d. Retesting to validate corrective action.
3. Interview management and review responses to pre-examination information requests to identify changes to the entity's technology related to new products and services that could affect the areas of review within AIO. Consider the following to identify changes:
 - a. Any significant changes in business strategy or activities that could affect the AIO environment (e.g., new lines of business or a decision to move from in-house to a cloud service provider).
 - b. Products or services delivered to either internal or external users.
 - c. Network diagrams, including configuration or component changes and the entity's internal and external connections.
 - d. Hardware, software, and telecommunications inventories.

¹¹⁸ Examiners may use system- or technology-specific technical references from authoritative sources, as appropriate.

- e. Loss of, addition to, or change in duties of key personnel, as well as any key management changes.
- f. Lists of third-party service providers and software vendors and the services or software provided.
- g. Changes to internal business processes.
- h. Changes based on industry changes or threat intelligence.

Objective 2: Management promotes and provides effective governance of AIO functions through defined responsibilities, accountability, and adequate resources to support these functions. (II, “Architecture, Infrastructure, and Operations Governance”)

1. Determine whether management implemented a process to continuously manage technology to support operational needs and mitigate AIO-related risks. Determine whether the entity’s risk management processes include the following governance mechanisms:
 - a. Delineation of board and senior management responsibilities.
 - b. Strategic planning.
 - c. ERM.
 - d. Delineation of other roles and responsibilities.
 - e. Policies, standards, and procedures.
 - f. Internal audit, independent reviews, and certifications.
 - g. Communications.
 - h. Board and senior management reporting.
2. Determine whether oversight includes the following:
 - a. Board and senior management consideration of the entity’s business objectives, including functions performed by affiliates and third-party service providers.
 - b. Management identification and evaluation of AIO-related risks, definition of short- and long-term objectives, and creation of policies and procedures to mitigate those risks.
 - c. Management consideration of security and resilience in the design of new products and services.
3. Determine whether board oversight includes the following:
 - a. Aligning AIO principles and practices with the board’s strategic plans and risk appetite.
 - b. Budgeting appropriate resources to support AIO activities.
 - c. Ensuring board members have appropriate knowledge of risks to provide a credible challenge to management.
 - d. Enabling appropriate management training on AIO to carry out its responsibilities and manage risk.
 - e. Reviewing AIO operating results and performance (e.g., audit reporting, testing results, and management and assessment reports).

4. Determine whether management oversight includes the following:
 - a. Validating through audits and other independent assessments that the following are comprehensive, meet enterprise-wide business and strategic plan objectives, and can assist in the identification of AIO-related risk.
 - Architectural designs and integration across the entity.
 - Infrastructure testing.
 - Operational testing.
 - b. Addressing risks self-identified by management, from AIO-related audits, and from other independent assessments.
 - c. Assessing and updating management's strategies and plans for AIO functions.
 - d. Promoting alignment and integration between functions of AIO.
5. Determine whether the board and senior management evaluate whether the IT strategic plan aligns with the enterprise-wide business and strategic plan, as well as established priorities and whether the planning addresses the following:
 - a. Participation of senior management by supporting AIO activities, confirming that those activities are in the IT strategic plan, reviewing the strategic planning process, and incorporating changes.
 - b. Responsibilities within the AIO functions through defining those responsibilities and determining the effectiveness of the IT strategic planning process.
 - c. Evaluation of architecture, including the entity's current architecture and whether it meets enterprise-wide business and strategic plan objectives.
 - d. Impact of IT infrastructure by understanding the relationship between IT infrastructure and the entity's needs.
 - e. Post-implementation evaluation of the performance and results of IT projects and initiatives to determine whether each project achieved the anticipated goals.
6. As part of the evaluation of question 5, determine whether management does the following:
 - a. Evaluates whether past and current IT performance demonstrates an ability to support IT strategic plans.
 - b. Takes steps to ensure and validate that IT services are delivered on time, within budget, and to business specifications.
 - c. Balances resource investments.
7. If an entity provides IT services internally or externally as a third-party service provider, determine whether management considers the following in the IT strategic planning process:
 - a. IT services strategy management that helps management to meet the needs of the entity while also providing for availability, capacity, continuity, and security.
 - b. Financial management for IT services to allocate the cost of providing services.
 - c. SPM that enables the entity to balance investment in AIO with the ability to meet business outcomes.

- d. Demand management, which balances customer demand for services with the capacity to meet that demand.
8. *This examination procedure may be coordinated with related examination procedures in the “[Management](#)” booklet.* Determine whether the entity’s ERM structure incorporates the functions of AIO. Evaluate whether, as part of ERM, there is the following:
 - a. Consistent and current review of the entity’s products, processes, applications, infrastructure, interconnectivity, and other related risks to business operations.
 - b. An effective risk management process for initiating and overseeing all AIO-related activities, including those that are outsourced, that includes:
 - Initial assessment of the AIO-related risk.
 - Architecture designed to meet the entity’s goals or objectives.
 - Infrastructure that supports the entity’s strategic objectives.
 - Identification of infrastructure assets (e.g., hardware and software) and associated interconnectivity critical to business and IT operations.
 - Ongoing monitoring that identifies and evaluates changes in risk and periodic updates to the risk profile assessment.
 - Roles, responsibilities, procedures, and reporting mechanisms for risk management in AIO activities.
 - Risk tolerances and risk and performance metrics for AIO activities.
 9. Determine whether management assigned responsibilities for the AIO functions based on the complexity of the architecture needs and assess the effectiveness of the entity’s separation of duties across the functions, particularly in situations where architecture responsibilities are combined with other functions. Evaluate the effectiveness of the assignment of the following responsibilities:
 - a. Architecture-related responsibilities:
 - Review of the centralization processes for the IT functions and understanding of interrelationships between the entity’s IT and business functions.
 - Development and maintenance of the enterprise model, including a common understanding, vocabulary, and blueprint for all stakeholders.
 - Responsibility for designing the IT architecture and accommodating IT changes.
 - Communication of challenges to the board and senior management.
 - Maintenance of representations (e.g., blueprints, network diagrams, and topologies) of the IT environment, review of existing infrastructure and operations to determine IT systems capabilities and needs.
 - Working with other members of management to evaluate architectural changes.
 - Maintenance and use of IT architecture knowledge.
 - Development of IT architecture policy and terminology.
 - Oversight of IT architecture product development, use, and refinement.
 - Maintenance and ownership of the IT architecture repository.
 - b. Data-related responsibilities:
 - Governance and use of information or data, protection of that data, and derivation of maximum value from it.

- Development of data-related policies, management of the data life cycle and the entity's data assets, oversight of compliance with applicable laws and regulations, and conformance with industry practices.
 - Provision of input to the chief architect in the design of IT systems to promote alignment with enterprise-wide business and strategic plan objectives.
 - Oversight of data management and data analysis and management of data-related projects.
 - Analysis of whether the entity's products and services meet enterprise-wide business and strategic plan objectives from a data perspective.
 - Use of data and reporting tools, maintenance of data quality, and promotion of data integrity.
 - Ownership of the entity's strategic use of data and communication of information and data analytics.
 - Definition of a data strategy, evaluation of data and its usage (including the consideration of data planning and the analytics platform), and development of metrics for monitoring data activities.
 - c. Operations-related responsibilities:
 - Oversight of the IT environment.
 - Management of the capacity, performance, and availability of the components used in an entity's infrastructure.
 - Support for line-of-business and functional operations.
 - Day-to-day operation and maintenance of infrastructure components.
 - Management of network infrastructure (e.g., network and connectivity, remote access, and telecommunications management) and server and device management (e.g., servers, storage, and devices).
 - Management of the IT environment (e.g., facilities, help desk, IAM, backup and replication, configuration management, resilience, and cyber and information security).
 - IT project management.
 - Database administration, systems analysis, client support, systems administration, and network administration.
10. Determine whether management documents, implements, and maintains policies, standards, and procedures related to AIO that address the following:
- a. Scope.
 - b. Responsibilities.
 - c. Accountability.
 - d. Authority.
 - e. Guidance to develop and maintain effective processes related to AIO.
11. Determine whether the board and senior management engage qualified audit or use other independent review functions to assess the AIO design, implementation, and operational effectiveness, including the adequacy of policies and procedures and the effectiveness of controls. Evaluate the appropriateness of the following:

- a. Review of the entity's AIO functions and activities and management's ability to oversee and control AIO-related risks.
 - b. Qualifications, training, and experience of auditor (or independent reviewer) in reviewing the functions and activities of AIO.
 - c. Independence of auditor from the AIO functions and activities being reviewed.
 - d. Reports to the board and senior management containing the results of audits or other independent reviews and an assessment of management's ability to oversee the entity's AIO functions and activities. Validate whether the review scope and frequency are appropriate for the complexity of the entity's AIO functions.
 - e. Whether auditors or reviewers:
 - Evaluate that management's AIO decisions align with the entity's business strategy, security, and resilience needs.
 - Leverage SOC and other external audit reports from third-party service providers.
 - Identify and report AIO issues to senior management and the board.
12. Determine whether management effectively communicates relevant AIO information to the entity's staff, applicable customers, and third parties.
13. Determine the effectiveness and comprehensiveness of board and senior management reporting related to AIO. Evaluate whether the following activities are performed:
- a. Management reports to the board periodically on the status of AIO initiatives, progress, issues, and metrics.
 - b. The board regularly monitors strategy, security, and resilience activities.
 - c. Board minutes reflect significant AIO-related discussions, credible challenge, and approvals.
 - d. Management measures performance and risks against defined baseline metrics.

The next 10 objectives (3–12) are related to section III, [“Common AIO Risk Management Topics.”](#) Each of these topics has its respective examination objective because there are risks from each area that affect the functions of AIO.

Objective 3: Management understands the common risks and mitigating controls related to data governance and data management. (III.A, [“Data Governance and Data Management”](#))

1. Determine whether management governs and manages data based on the entity-assigned data classification.
2. Evaluate whether management has an effective process for data removal or destruction when data are no longer used.
3. Evaluate whether business line management is consulted to assist in data classification, recovery standards development, and appropriate control validation.
4. Determine whether management has data governance and data management processes that include defining responsibility and processes for governing data, including the identification,

management, and oversight of any metadata, and promoting a culture that takes a data-centric approach.

5. Determine whether management identifies and classifies the entity's data effectively. Determine whether management does the following:
 - a. Identifies and understands the nature of the entity's data, including:
 - Sensitivity, criticality, and importance of the data.
 - Frequency, recurrence, and use of the data.
 - Format in which data are maintained.
 - b. Uses the results of the data classification process to implement controls to safeguard data, including sensitive data.
 - c. Understands where data reside and maintains the effectiveness of controls over that data.
 - d. Regularly updates the information and technology asset inventories for new assets, both internal assets and those residing at third-party service provider locations.
6. Determine whether management has effective database management, including the following:
 - a. Securely designs, builds, and operates databases.
 - b. Implements a process to secure and oversee databases.
 - c. Ascertains the effectiveness of database controls and updates the information asset and technology inventories.
 - d. Ensures databases are appropriately located and structured, have sufficient capacity, and are resilient.
 - e. Regularly monitors for new or changed databases and reports on misconfigured or out-of-compliance databases.
 - f. Understands how databases interconnect throughout the entity.
 - g. Focuses on identifying, managing, and securing the data; identifying business uses; and providing appropriate access regardless of how the data are stored.
 - h. Has appropriate staff (e.g., DBAs) that
 - Is responsible for database configuration, access controls, and maintenance, as well as training.
 - Monitors databases and maintains normal operations.
 - Works with information security staff.
 - Monitors for anomalous database activities.
 - Is familiar with procedures to protect sensitive information, restores normal operations, and notifies the information security officer when necessary.
 - i. Limits and independently monitors accounts belonging to DBAs.
7. Verify that management implemented effective database security controls, such as the following:
 - a. Changes passwords for default user accounts and, subsequently, disables or deletes those accounts where possible.
 - b. Tracks and monitors activity for default accounts that cannot be disabled or deleted.

- c. Restricts account access and limits privileges and permissions.
 - d. Implements password management tools or activities.
 - e. Employs an appropriate level of encryption according to the entity's data classification policy.
 - f. Configures and reviews audit logs.
 - g. Regularly monitors database activity logs.
 - h. Independently monitors DBA and privileged account activities.
 - i. Classifies data maintained within the database.
 - j. Restricts and monitors data extraction.
 - k. Implements and adheres to patch management processes.
 - l. Implements OS controls.
 - m. Monitors OS-level privileged account activities.
 - n. Manages application-level access.
8. Determine whether management considers design, placement, and effective security controls for non-production environments (e.g., development, test, and quality assurance). Consider the following:
- a. Independence of non-production environments from production environments to maintain data integrity and resilience.
 - b. Use of simulated synthetic data in non-production environments, when possible.
 - c. Controls to prevent testing in production environments to maintain confidentiality, integrity, and availability of data.
 - d. Use of masked or sanitized test data in non-production environments when production is used; if this is not feasible, approvals to use non-sanitized data with implementation of the same level of controls in non-production environments as in production environments.
9. Determine whether management appropriately considers the uses and risks of data analytics and performs the following:
- a. Limits access to analytics tools and related outputs.
 - b. Incorporates confidentiality, integrity, and availability when designing or selecting analytics tools.
 - c. Inventories the data sources, assesses the information type according to the entity's data classification policy, and appropriately secures those sources.
 - d. Develops design requirements and parameters for analytics.
 - e. Obtains sufficient knowledge for management and personnel to interpret dashboards and reports.
 - f. Considers the following when implementing and using data analytics:
 - Documentation of the data types maintained, data owners and users, and purposes of reports.
 - Determination of stakeholders' usage needs.
 - Determination of potential opt-in considerations, based on information type, in analytics reports.
 - Determination of disclosure requirements in the event of an incident.

- Implementation of access controls and activity monitoring over analytics tools and reports.
- Definition of processes to remove or destroy data when no longer used in the data analytics tools.
- Identification of data subject to applicable laws and regulations or other relevant industry standards.
- Identification of data analytics processes used to enable compliance with applicable laws and regulations.
- *This examination procedure may be coordinated with related examination procedures in the “[Information Security](#)” booklet.* If the entity uses big data, implementation of appropriate security policies, standards, and procedures, along with data access and security controls in accordance with the entity’s data classification policy.

Objective 4: Management implements appropriate ITAM processes to track, manage, and report on the entity’s information and technology assets. (III.B, “[IT Asset Management](#)”)

The examination procedures in this objective may be coordinated with related examination procedures in the “[Information Security](#)” booklet.

1. Determine whether management has a comprehensive inventory of its electronic (or digital) and physical information assets, in accordance with the Information Security Standards. Evaluate whether management specifically identifies its information assets, determines the appropriate classification of those assets, and protects them according to the entity’s data classification process.
2. Determine whether management implemented policies, standards, and procedures to govern all aspects of ITAM, including information and technology assets. Assess whether those processes include the following:
 - a. Identifying the technology assets the entity possesses and manages.
 - b. Determining each asset’s status (e.g., active or inactive).
 - c. Specifying the life cycle phase of those assets.
 - d. Regularly reviewing and validating the accuracy of the inventories.
 - e. Identifying personally owned technology assets that are allowed to connect to the entity’s network.
3. Determine whether management uses appropriate inventory mechanisms to effectively document, track, and oversee the entity’s information and technology assets, including its hardware and software. As part of the technology asset inventory, determine whether management considers IT assets that do not fall into traditional hardware or software inventories. Evaluate whether management has a process to periodically review and update the inventories. Assess the adequacy of management’s technology asset inventory process for the following:
 - a. Hardware inventory process that does the following:

- Identifies the entity's hardware assets.
 - Identifies equipment owned and managed by third parties on the entity's behalf.
 - Includes entity-owned and entity-managed virtual infrastructures.
 - Assigns a unique identifier for hardware assets.
 - Contains information about the network and telecommunications equipment.
 - Contains appropriate information on each piece of hardware.
 - b. Software inventory process that does the following:
 - Provides detailed information on software used in the entity's IT environment.
 - Contains appropriate information on the entity's software.
4. Assess whether each IT asset is captured in the entity's ITAM inventory, tracked throughout its operational life, and prepared for physical removal at the end of its useful life. Determine whether management implemented policies, standards, and procedures to identify assets and their EOL time frames, to track assets' EOLs, and to replace or upgrade the asset. Determine the effectiveness of EOL management through the following:
- a. Addresses EOL in contract provisions with its third-party service providers.
 - b. Adds assets to the inventories and tracks changes made to assets.
 - c. Conducts risk assessments to determine assets' EOLs.
 - d. Reviews EOL time frames for existing assets to determine accuracy and relevance.
 - e. Develops replacement plans for assets nearing obsolescence.
 - f. Establishes procedures for the secure destruction or data wiping of hardware and software.
 - g. Considers the following when reviewing new technology assets:
 - Incorporates EOL considerations in strategic planning.
 - Plans for obsolescence during initial project stages (e.g., during requests for proposals or proofs of concept).
 - Registers and tracks assets in the inventories and includes EOL information.
 - Develops plans for maintaining IT assets beyond EOL, if necessary.
5. Determine whether management understands and communicates the risks of shadow IT to entity personnel. Additionally, determine whether internal audit evaluates management's processes to monitor, identify, and remove unapproved devices, software, or services. Assess whether management performs the following:
- a. Establishes IT governance practices and security controls for shadow IT, including policies, standards, and procedures.
 - b. Includes shadow IT in security awareness training.
 - c. Considers the use of IT detection tools to monitor for and identify shadow IT.
 - d. Employs appropriate data protection and data loss prevention tools.
 - e. Considers appropriate methods to address shadow IT, including:
 - Identifying security risks associated with shadow IT in use and determining whether there is malicious intent.
 - Identifying the reason for its use.
 - Determining clients or processes supported by shadow IT.

- Verifying interconnectivity between shadow IT and third-party service providers or existing software integration.
 - Determining appropriate disposition of shadow IT.
 - Reviewing policies, processes, and tools to understand any gaps that may allow shadow IT to occur.
- f. Has processes to monitor, identify, and remove shadow IT that can be evaluated by internal audit.

Objective 5: Management understands the documentation maintained to represent the entity's IT and business environment. (III.C, ["IT and Business Environment Representations"](#))

1. Determine whether management documents and maintains accurate representations (e.g., network diagrams, data flow diagrams, business process flow diagrams, and business process narratives) of the current IT and business environments and employs processes to update the representations.
2. With the representations, assess whether management does the following:
 - a. Coordinates the development of representations among stakeholders.
 - b. Aligns diagrams and narratives with each other and across the entity's lines of business.
 - c. Periodically reviews documented diagrams and narratives to confirm the accuracy of the representations of the IT and business environment.
 - d. Provides for the resilience of this documentation by maintaining current and accurate backups.
 - e. Implements appropriate access and editing privileges to the representations.

Objective 6: Management fosters effective management of change across the AIO functions. (III.D, ["Managing Change in AIO"](#))

The examination procedures in this objective may be coordinated with related examination procedures in the ["Development and Acquisition"](#) booklet.

1. Determine whether the IT environment and its products and services, whether internally or externally provided, are adaptable to change, and stakeholders from across the entity have input into the change process.
2. Depending on the complexity of the change, determine the adequacy of the processes to manage the change. Verify that changes to any IT system or service are supported by an orderly, adaptable, documented, and measurable process.
 - a. If the entity implements more complex types of changes (e.g., core conversions, migrations to cloud-based environments, or implementing a system to support a new product), assess whether formal planning and management oversight processes are in place and adequate.

- b. If the entity implements less complex, but planned changes (e.g., implementation of patches), assess the appropriateness of the change process.
- 3. Determine whether the entity's policies, standards, and procedures address change management, including each step of the change process. Assess whether the process includes the following:
 - a. Categorization of changes by severity.
 - b. Specification of corresponding approval processes.
 - c. Identification of responsible staff, applicable stakeholder working groups, or entity committees.
 - d. Preservation of the IT environment's confidentiality, integrity, and availability.
 - e. Identification of metrics to track the efficiency and success of the change.
 - f. Implementation of changes with the goal of preserving confidentiality, integrity, and availability.
 - g. Incorporation of appropriate segregation of duties and monitoring throughout the change management process.
- 4. Review and evaluate the entity's change management process to implement changes that preserve systems' security and are based on the change type (e.g., planned, routine, and emergency). Determine whether management follows pre-defined processes, such as the following:
 - a. Request that includes the reasons for the change and details of the change.
 - b. Review of requests to determine viability, business practicality, and prioritization.
 - c. Approval through the appropriate documented hierarchy commensurate with the scope, cost, urgency, and overall risk.
 - d. Design and build, including formal processes to preserve integrity throughout the development life cycle and ensure adequate controls.
 - e. Testing, which documents that the change performs as intended, identifies flaws, and verifies that the change integrates with other systems.
 - f. Implementation that includes a formal process to deploy the change.
 - g. Verification and closure, including a post-implementation review and processes to document the change's closure.
- 5. When reviewing change management, evaluate the following transition processes:
 - a. Management implements a process to transition system changes from a strategic change management process to day-to-day operations.
 - b. Knowledge is adequately transferred to personnel who will be responsible for operating the systems and processes.
 - c. Change management processes allow for the transition of responsibilities and knowledge and are part of the overall system development life cycle.

Objective 7: Management maintains effective oversight of the entity's third-party service providers responsible for activities related to AIO functions. (III.E, "Oversight of Third-Party Service Providers")

1. Determine whether management identifies internal and external roles and responsibilities for AIO activities and implements processes to oversee those activities performed by third-party service providers. Assess whether management appropriately assigned and defined the responsibility and oversight of those activities.
2. Verify whether management identifies and addresses all risks according to contracts and other agreements (e.g., SLAs).
3. With respect to data destruction processes at the third-party service provider, determine the following:
 - a. Management is aware of the data destruction processes maintained by the entity's third-party services providers, including cloud service providers.
 - b. SLAs outline adequate third-party service providers' data destruction measures.
4. Determine whether management reviews independent audit or other assurance reports demonstrating the third-party service provider's ability to meet the entity's AIO needs.
5. Verify that management reports to the board on the effectiveness of any AIO activities performed by third-party service providers. Assess whether the reporting included any issues uncovered through the entity's third-party risk management processes.

Objective 8: Management adequately considers and implements resilience as part of the entity's risk mitigation strategy for AIO. (III.F, "Resilience")

1. Evaluate whether management integrates the entity's AIO functions into the entity's BCM program to mitigate threats, respond to and recover from disruptions, and incorporate lessons learned to strengthen the entity's resilience.
2. Determine whether management designs, implements, and operates its IT systems and processes to provide resilience for critical business activities. Assess whether management does the following:
 - a. Determines its reliance on people, processes, and technology, including third-party service providers, to assist in its assessment of risk.
 - b. Ensures the entity's business strategy and reliance on business functions drive the design for the entity's resilience.
 - c. Designs systems and software with resilience and information and cybersecurity at the beginning of the architecture process.
 - d. Uses infrastructure that supports varying levels of resilience depending on the criticality of the systems and software to ongoing business operations.

- e. Implements infrastructure to allow for secure remote administration and maintenance, for situations where personnel are unable to perform operations on site.
- f. Addresses resilience in operations to prevent data loss, protect sensitive customer information from unauthorized disclosure or manipulation, minimize disruption to service delivery, and prevent the loss of situational awareness of the entity's operations. Evaluate whether this operational resilience includes having:
 - Operational controls.
 - Operational processes (e.g., vulnerability and patch management).
 - Service delivery and support processes (e.g., resilience in supply chain).
 - Ongoing monitoring and evaluation capabilities (e.g., monitoring for indicators of an APT).
- g. Avoids making assumptions on the resilience of the entity's systems simply because they are operating in the cloud.
- h. Identifies assets, applications, and services located in the cloud, if operating in the cloud.
- i. Verifies that resilience is covered in contracts with cloud service providers.

Objective 9: Management has appropriate AIO processes for managing remote access.
(III.G, "[Remote Access](#)")

1. Evaluate whether management considers the implications of remote access in AIO and does the following:
 - a. Designs for remote access capabilities, including:
 - Plans for the methods and access points to maintain security and control access to entity resources.
 - Considers appropriate methods (e.g., tunneling, web portals, direct application access, and remote desktop access).
 - Considers protection of communications and security needs (e.g., encryption, authentication, access restrictions, application security, and activity monitoring).
 - b. Uses remote access technologies that can be protected.
 - c. Employs effective risk mitigation for remote access, including:
 - Remote access policy that includes tiered levels of remote access and risk-based security controls.
 - IAM based on job type and access and appropriate authentication techniques.
 - Encryption technologies to protect communications.
 - Securely configured and patched remote access servers.
 - Secure entity-owned telework client devices.
 - Controls on the use of personally owned devices used to remotely access entity resources.

Objective 10: Management incorporates AIO considerations into the decision to use and use of personally owned devices. (III.H, “[Personally Owned Devices](#)”)

1. Determine whether management adequately considered AIO in the decision to allow the use of personally owned devices. Specifically, evaluate the effectiveness of the following:
 - a. Due diligence to determine types of devices that can be used.
 - b. Consideration of the architecture of the entity’s IT systems, such as where and how the devices will access the bank’s network.
 - c. Determination of additional infrastructure needed to support the secure use of personally owned devices.
 - d. Controls needed to adequately safeguard the network.
 - e. Use of technical policy enforcement to manage or restrict devices used.

Objective 11: Management incorporates AIO considerations into the design, implementation, and use of file exchange. (III.I, “[File Exchange](#)”)

1. Determine whether management considers risks related to exchange files and implements effective mitigation, such as the following:
 - a. Identification of user needs for exchanging files, both internally and externally.
 - b. Design of client server architecture to provide for confidentiality, integrity, availability, and resilience.
 - c. Identification of the infrastructure, including the appropriate systems and software, necessary to support file exchange activities.
 - d. Inclusion of appropriate infrastructure to support monitoring of the entity’s file exchange activities.
 - e. Implementation of appropriate operational controls, such as:
 - Monitoring for authorized file exchange.
 - Use of detection controls.
 - Use of only a trusted provider for third-party file exchange and storage solutions.
 - Consideration of solutions that provide visibility into cloud applications.
 - Definition of appropriate policies, standards, and procedures for file exchange activities.
 - Provision of training to employees on approved solutions.

Objective 12: Management designs, applies, and aligns its IT architecture to meet the strategic and business objectives of the enterprise. (IV, “[Architecture](#)”)

1. Determine whether management established enterprise-wide architecture principles that balance the mitigation of risks to various stakeholders and align with the entity’s strategic goals and business objectives; meet the entity’s needs for confidentiality, integrity, and availability; and adhere to the entity’s policies, standards, and procedures. Determine whether the architecture design involves the following:

- a. Consideration of the entity's architecture requirements for its existing technology and any planned changes.
 - b. Understanding by business units of their portion of the design.
 - c. Alignment with management's defined mission and any strategic initiatives for architecture.
 - d. Identification of the entity's IT assets, external constraints, industry IT architecture trends, and the entity's needs for the desired future state.
2. Determine whether management has policies, standards, and procedures to govern the entity's architecture design process and whether the design process addresses the following:
 - a. Definition of responsibilities and decision-making.
 - b. Identification of functional requirements.
 - c. Assessment of alignment with the entity's IT and strategic plans.
 - d. Evaluation of the inventory of current IT assets and the purpose of those assets.
 - e. Performance of a cost-benefit analysis of the architecture plan or project.
 - f. Acquisition of approvals for the initiative.
 - g. Implementation and maintenance of the architecture.
 - h. Resolution of disputes or architectural issues.
3. Evaluate the adequacy of the entity's documented and approved architecture plan. Consider whether management considers the following in relationship to the plan:
 - a. Alignment with the entity's strategic plan and support for the business and strategic objectives of the entity.
 - b. Development of policies, standards, and procedures to govern architecture initiatives and changes to the architecture plan.
 - c. Inclusion of processes for obtaining approvals, making changes to the plan, and reporting, as appropriate.
 - d. Alignment of the formality of the architecture plan and processes with number and complexity of the architecture initiatives.
 - e. For larger or more complex architecture changes, maintenance of a project management process that includes the following:
 - Planning.
 - Execution.
 - Closeout.
4. With respect to design objectives, determine whether management does the following:
 - a. Uses defined terminology.
 - b. Evaluates its needs and considers:
 - Collaboration between IT and business units.
 - Prioritization of investments.
 - Comparison of existing architecture with anticipated future changes.
 - Establishment of processes to evaluate and procure technology.
 - Storage, backup, and capacity needs to accommodate the entity's strategic plans.

- Type of applications the architecture will support.
 - c. Includes the following aspects in its architecture design:
 - Performance and reliability.
 - Integrity.
 - Availability and resilience.
 - Scalability.
 - Flexibility.
 - Security and privacy.
 - Interoperability and integration.
 - Ability to integrate and align with one or more third-party service providers.
 - Testing internally and with third-party service providers, as appropriate.
 - Auditability.
 - Advancements in technology.
 - d. Includes considerations for avoiding the potential for shadow IT and the capability to monitor and alert for its use.
 - e. Considers how evolving technologies (e.g., cloud, IoT, and AI/ML) can affect its design.
 - f. Plans for obsolescence, EOL, and decommissioning of systems.
- 5. Evaluate whether management has a process to determine appropriate deployment environments (e.g., in-house or serviced, virtualization and cloud, or hybrid) as part of the design process. Determine whether the process includes the following considerations:
 - a. Identification of risks and benefits of each type of deployment environment.
 - b. Use of physical versus virtual components in the design.
 - c. Type of virtualization solution and design risks associated with the following elements:
 - VMs and the design of secure virtual infrastructures to provide the ability to oversee the interconnectivity and segmentation of VMs.
 - Hypervisors and the design of where the hypervisors sit and the connectivity between hypervisors and VMs.
 - Containers, including the design for storing data outside of the container and implementation of vulnerability management processes, segmentation, and the ability to monitor containers.
 - Microservices, including a design process that allows for the use of microservices as an integrated component to overall IT operations and the ability to address the risks of security, reliability, and latency in the entity's development process.
 - d. Placement and selection of storage, design of network topology, availability of bandwidth, and need for management reporting systems, as well as implementation of monitoring tools.
- 6. In larger or more complex entities, determine whether management considered using EA to align its architecture with the entity's strategic plans and business functions. Describe management's implementation of EA and use of architecture frameworks, if appropriate. Regardless of entity size, determine whether management incorporated the following:
 - a. Evaluation of approaches to implement and build security and resilience throughout its architecture.

- b. Analysis of the functionality, including security and resilience, of legacy systems and identification of gaps.
- c. Identification of necessary roles to support the EA function.

Objective 13: Management implements an IT infrastructure that achieves and promotes the objectives of confidentiality, integrity, and availability, and meets the entity's business objectives. (V, "Infrastructure")

1. Determine whether the entity's IT infrastructure implementation includes considerations for server and data redundancy and resilience of telecommunications lines.
2. *This examination procedure may be performed in coordination with the examination procedures in Objective 4 (ITAM).* Determine whether management has effective processes related to ITAM to track and monitor all hardware assets (whether or not they are connected to the network) to maintain an accurate and current record of the technology assets in its environment. As part of these processes, determine whether management does the following:
 - a. Identifies unauthorized technology assets and determines their disposition.
 - b. Evaluates how unauthorized devices gained access and whether any compromise occurred.
 - c. Updates the related policy or procedures or provides additional training.
3. *This examination procedure may be performed in coordination with the examination procedures in Objective 4 (ITAM).* Determine whether management documents and maintains a current inventory of network and telecommunications hardware and software and the standard network configuration for them. Additionally, determine whether management does the following:
 - a. Implements appropriate redundancy capabilities for the entity's telecommunications infrastructure.
 - b. Understands the limitations of the entity's third-party telecommunications providers' infrastructure.
 - c. Documents the network's baseline configuration, including processes to review and approve changes.
 - d. Regularly assesses and documents compliance with the entity's baseline configuration.
 - e. Appropriately controls networked devices by managing ports, protocols, and services and maps them to the devices on the technology asset inventory.
 - f. Installs the latest version of security-related updates on network devices, when appropriate.
 - g. Maintains standard images of the entity's servers and stores them securely. Uses clean (i.e., trusted) images to restore the server if a server needs to be rebuilt and documents, reviews, and approves deviations from the standard image.
 - h. Implements security and monitoring throughout the entity's network, analyzes incoming and outgoing data traffic, and alerts authorized personnel if anomalous activity is detected. Additionally, determine whether the following security and monitoring mitigation strategies are in place:

- Use of software tools to protect against and monitor internet-accessible services or open ports.
 - Implementation of firewalls and port filtering.
 - Deployment of IDS/IPS.
 - Use of internal tools to detect, identify, and prevent misuse by entity personnel.
 - i. Performs administrative activities from dedicated workstations.
 - j. Uses multi-factor authentication over encrypted network connections for administrators accessing and managing network devices.
 - k. Monitors telecommunications traffic and periodically reviews network devices.
 - l. Appropriately controls telecommunications equipment, including:
 - Physically securing it and restricting and monitoring access to it.
 - Following enterprise change control standards.
 - Following entity policies, standards, and procedures for identification, authorization, and authentication to access telecommunications systems.
 - m. Designs and builds telecommunications infrastructure components for resilience (e.g., implement route diversity), including selecting infrastructure components and telecommunications providers that help avoid a single point of failure.
 - n. Addresses voice communications risks through development and acquisition processes, and in written policies, standards, and procedures. If the entity uses VoIP for voice communications, determine whether management performs a comprehensive risk assessment to ensure confidentiality, integrity, and availability in voice communications.
 - o. Implements physical and logical controls in the VoIP environment, evaluates options for backup systems, and considers control solutions specific to VoIP, such as VoIP-ready firewalls.
 - p. Monitors incoming and internal data communications traffic for problems.
 - q. Implements redundant telecommunications services and establishes work-around procedures for situations where needed.
4. Evaluate whether management determines the types of software needed to implement the entity's strategic objectives and considers the software's scalability, interoperability, and portability. As part of its software infrastructure planning, determine whether management performs the following:
- a. Tracks and monitors the entity's software assets.
 - b. Maintains an accurate and current record of its software assets (e.g., with a software inventory).
 - c. Periodically reviews existing software.
5. *This examination procedure may be performed in coordination with related examination procedures in the "[Development and Acquisition](#)" booklet.* Determine whether management appropriately chooses software (e.g., to meet the entity's infrastructure and operational requirements) and considers whether to develop software internally or obtain it from a third party.

- a. With internally developed software, evaluate whether management is responsible for maintaining the software, and entity personnel have the resources and expertise to stay abreast of vulnerabilities and develop software updates and patches.
 - b. With externally developed software, evaluate whether management performed the following:
 - Determined whether COTS software meets the entity's needs and security requirements or if it will integrate with existing software and require further configuration.
 - Determined whether custom software was designed to integrate with the existing enterprise software, hardware, and data, and whether management considered issues related to obsolescence, patching, and availability of expertise.
 - c. Regardless of the type of externally developed software selected, determine whether management performed the following:
 - Approved the selected software's use and determined that it met the entity's infrastructure requirements and strategic objectives.
 - Allocated resources to support the software (e.g., financial and personnel) and determined that personnel have the expertise to maintain and patch the software.
6. *This examination procedure may be performed in coordination with related examination procedures in the "[Development and Acquisition](#)," "[Information Security](#)," and "[Outsourcing Technology Services](#)" booklets.* Determine whether management is aware of and implements risk mitigations for general risks (e.g., software vulnerabilities and unauthorized access) associated with software in the entity's infrastructure environment. With respect to specific software types, determine whether management does the following:
- a. For OS software:
 - Oversees and maintains the OS, including testing and installing patches when appropriate.
 - Restricts and monitors administrator access to the OS.
 - Limits the use of utility software.
 - b. For core processing software:
 - Restricts software based on job responsibility.
 - Monitors its use.
 - Selects core processing software with adequate capacity.
 - Chooses software that can support usage spikes, expected peak usage times, and future growth.
 - c. For productivity software:
 - Considers the use of it to enable personnel to perform their job functions.
 - Safeguards systems against security threats and employs IAM, configuration management, and log monitoring.
 - Employs mitigation strategies to address synchronization issues.
 - d. For enterprise software:
 - Considers how enterprise software integrates in the entity's infrastructure environment.
 - Limits access and editing capabilities.
 - Monitors user activity.

- e. For security software:
 - Uses security software that is current, deployed effectively, and designed to keep up with the evolution of malicious code.
 - Restricts administrative access to this type of software.
- f. For system auditing software:
 - Uses system auditing software to augment audit personnel.
 - Uses the software to assist in the identification of gaps in infrastructure security and resilience.
 - Documents software for system audit use and defines its purpose.
- g. For open source software:
 - Identifies security issues with its use.
 - Implements security controls and procedures to mitigate risks, including the following:
 - Defining acceptable use (or restriction) guidelines and documenting a process for modifying and reviewing the code.
 - Restricting access to unapproved shareware sites.
 - Using tools to help discover unapproved open source software.
 - Identifying the type and version of open source software in use, where it is used within the entity, and its purpose.
 - Implementing version and patch control guidelines for open source software in use.
 - Monitoring for vulnerabilities of the open source software employed by the entity.
 - Evaluates implications of open source components in third-party software and addresses their use in contract provisions.
 - Evaluates open source software components during software due diligence.
- h. For mainframe security software:
 - Implements access controls (e.g., role-based access, segregation of duties, and multi-factor authentication).
 - Uses security controls.
 - Encrypts sensitive information.
 - Enables activity log settings (e.g., user access, failed login attempts, and security setting changes).
 - Implements real-time monitoring and alerting.
 - Performs timely patch management.
 - Verifies mainframe security auditing (e.g., regular review and validation of security controls, privileges, roles, and access profiles).
 - Independently monitors privileged accounts (e.g., system and security administrators).
 - Maintains appropriate mainframe security expertise.
- i. For APIs:
 - Assesses and implements security needs for APIs.
 - Addresses authorization, authentication, and encryption.
 - Implements API security tools and gateways with controls for requests and responses.
 - Performs sensitive data filtering.

- Places restrictions on size and number of resources requested.
 - Identifies API request checkpoints for information leaving the network.
 - Performs appropriate API logging and monitoring.
 - Implements other security controls (e.g., secure IPs, password hashing, restriction of secret information, authorization protocols, validation mechanisms, time stamping, rate limiting, API traffic monitoring, and API gateway configuration) as appropriate for internal APIs.
 - Implements adequate security and restrictions over the use of public APIs to protect sensitive customer and entity data and performs appropriate testing to verify the adequacy of security controls over a third party's APIs.
 - As part of its customer awareness program, makes security awareness information available to its customers using unaffiliated third-party API services. Determine whether the information addresses protections available and not available when the customer allows access to its data.
7. *This examination procedure may be performed in coordination with related examination procedures in the “[Outsourcing Technology Services](#)” booklet.* Determine whether management performs the following, depending on the type of software hosting involved:
- a. For internally hosted software, determine whether management:
 - Identifies personnel (e.g., internal or third-party) with relevant skills and expertise.
 - Allocates resources for necessary training to maintain knowledge.
 - Follows a system development life cycle that incorporates security if the entity develops software in-house.
 - b. For externally hosted software, determine whether management:
 - Has contract provisions addressing the notification of infrastructure changes and the third party's use of any subcontractors.
 - c. For hybrid hosted software arrangements, determine whether management:
 - Performs an adequate risk assessment to prepare for a potential service interruption.
8. *This examination procedure may be performed in coordination with related examination procedures in the “[Business Continuity Management](#)” booklet.* Determine whether management developed, documented, and implemented environmental control policies, standards, and procedures to safeguard facilities, technology, data, and people. Specifically, determine whether management has effective environmental controls to identify and mitigate risks from infrastructure and operational issues. Evaluate whether remotely available environmental controls (including IoT devices used for environmental monitoring), whether by a third-party service provider or not, have appropriate access controls, monitoring of remote access activity, and regular review of privileges. Additionally, determine whether third-party service provider access for maintenance and administrative purposes are appropriately controlled.
9. Review the effectiveness of management's mitigation of the risks associated with the following:
- a. HVAC controls, including:

- Maintaining appropriate temperature and humidity levels.
- Monitoring HVAC.
- Implementing automated monitoring and providing an alarm or notification of significant temperature changes.
- Considering the entity's need for redundant HVAC equipment components.
- b. Smoke and fire mitigation strategies, including:
 - Appropriate smoke and fire detection systems.
 - Smoke and fire detectors in appropriate locations.
 - Devices and systems for smoke detection, fire suppression, and fire detection supported by an independent energy source.
 - Inspections of facilities for potential fire hazards and resolution of identified deficiencies.
 - Training.
 - Evaluation of all systems for their advantages and disadvantages.
 - Knowledge of potential risks of fire suppression systems.
 - Contract provisions for smoke and fire detection in third-party hosted infrastructure situations.
- c. Water detection controls, including:
 - Use of water detectors in raised floors or in ceilings to alert management.
 - Consideration of automated mechanisms to detect the presence of water and provide alerts.
- d. Power issues mitigation, including:
 - Steps to protect computing equipment from inconsistent and dirty power sources.
 - Consideration of long-term alternate power supply to provide operational capability during extended power outages.
 - Appropriate power configurations based on the entity's power needs.
 - Use of independent electrical feeds drawing from separate power grids and automatic fail-over to a live power source, where multiple feeds or backup power generators are used.
 - Evaluation and mitigation of the risk from one grid or one provider in other ways (e.g., using generator(s) or batteries).
 - Methods to monitor, condition, or stabilize the electricity source voltage and minimize effects of power fluctuations.
 - Use of alternative power sources independent of local power grids.
 - Processes to power down IT systems in an orderly manner to maintain critical information for later recovery, in cases where power cannot be maintained (e.g., during emergencies).
 - Activation of automated emergency lighting of critical infrastructure, evacuation routes, and emergency exits.
- e. Physical access controls, including:
 - List of approved individuals with authorized physical access to the IT infrastructure facilities.
 - Validation of access authorizations before granting access to restricted spaces.
 - Use of credentials for entity personnel and visitor badges for visitors.
 - Logs of individuals that access restricted spaces.
 - Use of physical intrusion alarms and surveillance equipment.

- Visitor escorts and visitor activity monitoring.
- Security over combinations, keys, and other physical access devices; processes to change combinations or keys as needed; and removal of electronic user credentials, when appropriate.
- Inventory of physical access devices at regular intervals.
- Regular reviews of access lists and removal of unnecessary access.
- Alternative physical access processes if electronic controls fail.

The next four objectives (14–17) are related to [section VI, “Operations.”](#) Examination objectives for this section were divided into four sub-sections: “Operational Controls,” “Operational Processes,” “Service and Support Processes,” and “Ongoing Monitoring and Evaluation Processes,” following the layout in the booklet.

Objective 14: Management develops and implements operational controls to safeguard the entity’s operational environment. (VI.A, [“Operational Controls”](#))

The examination procedures in this objective may be performed in coordination with related examination procedures in the [“Information Security”](#) booklet.

1. With respect to operating centers, describe the entity’s operating center type and key responsibilities and determine whether functions such as security and network management are addressed. Evaluate the appropriateness of the entity’s processes and controls, such as the following:
 - a. Responsibility for the physical location as well as the on-premise equipment and systems in entity-owned versus outsourced operating centers.
 - b. Contract(s) specifying equipment ownership and responsibility, if management of the operating center is outsourced.
 - c. Operating centers located in areas less prone to environmental threats.
 - d. Appropriate security and environmental controls within the entity’s infrastructure, including:
 - Use of smoke, water, and power detection and mitigation devices and systems, as well as fire suppression systems.
 - Use of security zones limiting access within restricted spaces.
 - Implementation of physical security controls.
 - Use of devices to restrict and log access to the site.
 - Procedures for appropriate site maintenance.
 - e. Responsibilities for implementing security and environmental controls.
 - f. Operating center responsibilities, including:
 - Training staff to operate and maintain the entity’s equipment and systems.
 - Deploying appropriate connectivity.
 - Managing incidents and events.
2. Determine whether management defines the entity’s authorization boundary(ies) and implements appropriate security controls according to the contents of the authorization boundary, including controls over the following:

- a. Internal and external communication systems within and across the entity's authorization boundary(ies).
 - b. The connection between the entity and its third parties.
 - c. Physical, logical, and environmental controls.
 - d. Perimeter protection devices.
 - e. People and processes supporting the entity's missions and business functions.
3. Determine whether management implements appropriate IAM processes and does the following:
 - a. Appropriately provides access to the entity's resources.
 - b. Considers enhanced authentication, especially for privileged access.
 - c. Considers its implementation of cloud services and addresses the unique access control requirements for cloud environments, as appropriate.
 - d. Maintains a policy and implements related standards and procedures to identify users and restrict their access.
4. Determine whether management has processes for employee recruitment, hiring, and placement and provides for thorough applicant screening and background checks at the time of employment. Review the following and evaluate their effectiveness:
 - a. Performance of background checks at an appropriate frequency.
 - b. Definition of duties, responsibilities, expectations, and accountability.
 - c. Implementation of dual control and segregation of duties.
 - d. Independently monitoring activities.
 - e. Implementation of rotation of duties.
 - f. Reviewing and monitoring of activities performed during rotation of duties.

Objective 15: Management implements effective IT operational processes to reduce the number of potential operational failures and minimize the impact of issues that occur. (VI.B, "IT Operational Processes")

The examination procedures in this objective may be performed in coordination with related examination procedures in the "Information Security" and "Outsourcing Technology Services" booklets.

1. Determine whether management has assigned responsibility for the performance of maintenance on the entity's equipment. Evaluate whether the following is effective:
 - a. Routine maintenance by data center employees is performed according to manufacturers' recommendations.
 - b. Preventive maintenance follows a predetermined schedule.
 - c. Operations employees document both internal routine (if any) and externally provided maintenance in logs and other records.
 - d. Management reviews maintenance records.

- e. For equipment owned or leased from a third party, management obtains a separate agreement to manage maintenance. The agreement includes:
 - Preventive maintenance to be performed.
 - Provisions for repair services.
 - Schedule for maintenance and time frame for repair.
 - f. Management provides time and resources for scheduled preventive maintenance, which includes:
 - Limiting the service representative's access to the minimum necessary.
 - Having at least one computer operator present when the service representative is on site.
 - Reviewing system activity logs to monitor access to programs or data during maintenance.
 - Following established security procedures to ensure representatives have only the necessary access at predetermined times to perform specific tasks.
 - g. If there is an arrangement with a contractor to manage the entity's preventive maintenance and repair services, the contract or agreement guarantees timely performance of maintenance.
 - h. If computer maintenance is performed online, the online maintenance schedule is available to prevent interference with normal operations and processing.
 - i. Maintain a log of all hardware or software problems and downtime encountered between maintenance sessions.
2. Evaluate whether management has policies, standards, and procedures for configuration management and defines and implements appropriate configuration settings. In addition, verify whether management does the following:
 - a. Appropriately defines and applies configuration settings on IT products at the entity.
 - b. Ensures that systems and software used to support entity operations have appropriate configuration management capabilities, including configuration of audit log settings, and enforces configuration management.
 3. Determine whether management establishes procedures to stay abreast of system vulnerabilities and software vendor patches, tests patches in a segregated environment, and installs them when appropriate. Additionally, determine the effectiveness of the following:
 - a. Management implements a vulnerability management program that identifies systems and software vulnerabilities, prioritizes the vulnerabilities and the affected systems in order of risk, and performs timely remediation according to the risk of the vulnerability. The vulnerability management program includes the following:
 - Systems and software operating in the cloud for which the entity is responsible as well as those managed by the entity on its premises.
 - Processes to monitor industry third parties (e.g., US-CERT, NIST, and FS-ISAC) that report vulnerability exposures and address any relevant exposures within the entity's systems and software.
 - Processes to periodically assess systems and software for vulnerabilities using scanners with current vulnerability lists.

- Vulnerability scans of all systems and software in the entity’s hardware, software, and telecommunications inventories.
 - Appropriate controls over vulnerability scanning tools, including controls to protect against unauthorized use or access to sensitive information.
 - Use of dedicated accounts for authenticated vulnerability scans.
 - Methods to track and report on nonconformance to entity policies and the timeliness and remediation progress of all identified vulnerabilities, including those related to security procedures, physical layout, or internal controls.
 - b. Management implements a patch management program that includes documentation of any patch installations. The patch management program includes the following:
 - Processes to document patch installations as part of the entity’s change management procedures.
 - Systems and software for automated patch management or other demonstrated effectiveness in keeping up with patch identification, testing, and installation.
 - Records of the system and software versions in place and regular monitoring of online and industry resources for information on product enhancements, security or other issues, patches, or upgrades.
 - Communication and integration with the entity’s third-party service providers to align the entity’s patch management program with those of the third-party service providers.
4. *This examination procedure may be coordinated with the examination procedures in the “[Business Continuity Management](#)” and “[Information Security](#)” booklets. Determine whether management implements backup methods, including replication, based on the risk and criticality of the systems and data.*
- a. As part of its backup and replication processes, determine whether management maintains the following:
 - Policies, standards, and procedures.
 - Inventories of backup media, storage location, and access controls for the media or physical location.
 - Documented periodic physical reviews to confirm that all relevant backup material is available.
 - Procedures to verify adherence to backup schedules.
 - Processes to regularly test backup copies for readability.
 - Capability to restore operations to a previous trusted state.
 - Backups of configurations and data off-site and on a separate system or media.
 - VM versioning, replication, and life cycle policies for backup processes.
 - Data encryption and access controls to protect backup or replicated data from unauthorized access, destruction, or corruption.
 - Proper sanitization and disposal of data when it is no longer needed to prevent the disclosure of information to unauthorized users.
 - b. When using third-party service providers for backup and replication, determine whether management validates that the third-party service provider performs the processes above.

5. To meet scheduling needs, determine whether management implements policies, standards, and procedures for creating and changing job schedules and analyzing and maximizing the entity's resources.
6. Determine whether management implements adequate capacity management processes. Additionally, evaluate whether the processes provide for the following:
 - a. Integration with the budgeting and strategic planning processes.
 - b. Addressing internal and external factors.
 - c. Routine assessment of capacity against baselines to ensure adequate performance in the following:
 - Platform processing speed.
 - Primary working memory for each platform's CPU.
 - Additional data storage capacity.
 - Voice and data communication bandwidth.
 - d. Analysis of capacity trends (e.g., increasing capacity usage) to understand capacity usage.
 - e. Analysis of help desk records, as appropriate, for capacity issues.
 - f. Periodic analysis of projected versus actual capacity.
 - g. Verification through testing to ensure systems and software meet the entity's demands during periods of high volume.
 - h. Meeting between IT management and business line management to determine future projects that may impact capacity needs.
 - i. Consideration of flexibility to accommodate the entity's future capacity requirements.
 - j. Evaluation of third-party service providers' performance in combination with internal performance to determine whether capacity can meet existing and future demands.
7. Determine whether management has a log management process to use logs to identify, track, analyze, and resolve problems that occur during day-to-day operations. Describe how management collects and collates logs and how management uses logs to respond to issues. Evaluate how management addresses the following:
 - a. Identification and disposition of false positives and adjustment of logging parameters to minimize the volume of false positives in future log review.
 - b. Implementation of policies, standards, and procedures for log management activities that address the following:
 - Objectives for logging.
 - Types of logs to be collected.
 - Controls to restrict access to log settings.
 - Response time for log review.
 - Retention time frames and storage policies of logs.
 - Escalation processes for anomalies.
 - c. Configuration of logging to match the entity's risk and complexity of the entity and identify and address anomalies.
 - d. Consideration of tools to automate log analysis and extract important events or patterns.
 - e. Implementation of controls to protect logs.

8. Determine whether management implements policies, standards, and procedures to address media and equipment disposal or transfer. Evaluate whether management addresses the following:
 - a. Controls involved in the disposal process that are risk-based relative to the sensitivity of the information as defined by the entity's data classification policy and the type of media used.
 - b. Defined methods for disposal based on the type of data to be removed.
 - c. Consideration of techniques to remove data even when transferring the media between internal departments.
 - d. Implementation of appropriate procedures for the disposal of equipment (e.g., printers).
 - e. Performance of periodic reviews to ensure the timely disposal of decommissioned equipment.
 - f. Application of additional disposal techniques (e.g., data destruction) to remove sensitive information when traditional removal methods are not fully effective.

Objective 16: Management develops and implements service and support processes to support an entity's strategic goals and objectives by preventing issues, ensuring continuous reliability and resilience, and supporting users. (VI.C, "Service and Support Processes")

1. Determine whether management designs the entity's service management functions with an emphasis on preventing issues and ensuring continuous reliability and resilience where possible. Evaluate whether management performs the following:
 - a. Considers the following as part of its service management planning:
 - Services offered and SLA, OLA, or contractual provisions.
 - Activities performed by third-party service providers.
 - Known limitations (e.g., capacity or resources) that may affect service management activities.
 - Applicable legal and regulatory requirements.
 - Resources necessary to carry out service management functions and activities.
 - Metrics and measurements used to evaluate service management effectiveness.
 - b. Utilizes documented OLAs or another method to communicate and coordinate the entity's business requirements to personnel responsible for the execution of service management functions.
 - c. Coordinates its processes with third-party service providers, when used, to ensure seamless functionality to the entity's lines of business.
 - d. Coordinates meetings between process owners from both business and technology functions to discuss known issues, changes in progress, and future changes.
2. As part of the entity's operational support processes, determine whether the following is performed:
 - a. Management implements the following:
 - Processes to verify that incoming data transmissions and processing are complete and accurate.

- Controls to verify that external data transmissions and processing are securely received.
 - Controls to verify that data were not corrupted during transmission or processing failures.
 - Mechanisms to report transmission and processing errors.
 - b. Operational support personnel report errors or problems with the systems or software and provide updates on resolution.
- 3. Determine whether the entity has an IT support function. If there is, evaluate it for the following:
 - a. Processes for recording and tracking incoming issues, whether handled by human operators or automated systems.
 - b. Tracking system documentation that includes:
 - User name and contact information.
 - Problem description.
 - Request type and category.
 - Affected system.
 - Prioritization code.
 - Current status toward resolution.
 - Individual or group responsible for resolution.
 - Root cause, when identified.
 - Target resolution time frame.
 - Comments related to user interaction with IT support and other information.
 - c. Well-trained and knowledgeable IT support personnel.
 - d. Appropriate training for IT support personnel to perform their duties, if IT support software is used.
 - e. Procedures to authenticate users to prevent unauthorized access to information or credentials.
 - f. Layered security and supplemental authentication techniques for changes to account maintenance activities and for high-risk transactions.
 - g. For outsourced IT support functions, management's IT support expectations and responsibilities for the third-party service provider are included in the contract.
- 4. *This examination procedure may be coordinated with related examination procedures in the "[Business Continuity Management](#)" and "[Information Security](#)" booklets.* Determine whether management has processes to manage events, incidents, and problems. Evaluate the effectiveness of the following:
 - a. Implementation of entity processes to plan for and manage events, incidents, and problems, including:
 - Coordinating and defining roles and responsibilities.
 - Conducting testing to identify interdependencies.
 - b. Establishment and maintenance of appropriate processes and controls, including:
 - Identifying the event, incident, or problem.
 - Determining the impact.

- Assigning a severity rating based on risk.
 - Performing root cause analysis.
 - Identifying, logging, tracking, and analyzing events, incidents, and problems.
 - Maintaining contact information for individuals and groups for notification purposes.
 - Informing the help desk of the event, incident, or problem and how to respond.
 - Resolving the event, incident, or problem, including approval processes for system or software changes to correct the issue.
 - Documenting any interim actions, compensating controls, and risk acceptance for issues that cannot be immediately resolved.
 - Developing longer-term action plans to monitor and address issues.
 - Reporting on the progress of the action plans to senior management.
 - Implementing procedures for escalation and reporting.
 - Implementing procedures to correlate events.
- c. Performance of periodic trend analysis to find recurring or related issues that may be tracked to a common root cause.
 - d. Maintenance of management plans that cover hardware, software, and security devices.
 - e. Communication of processes to manage events, incidents, and problems to appropriate personnel.
 - f. Coordination and inclusion of processes with the entity's incident response program.

Objective 17: Management develops processes to oversee operations functions, evaluate the effectiveness of controls, and identify opportunities for improvement. (VI.D, "Ongoing Monitoring and Evaluation Processes")

1. Determine whether management implements processes to monitor IT operations and periodically reports on the effectiveness of established controls to senior management and other stakeholders. Evaluate the following:
 - a. Senior management and other stakeholders have input into the types of reports and metrics produced, and reports are understandable and useful to them.
 - b. The operations team reports performance metrics to senior management and other stakeholders.
 - c. Operations management meets periodically with senior management and other stakeholders on monitoring and reporting.
 - d. If the entity has outsourcing arrangements, evaluate whether management does the following:
 - Monitors third-party service providers as part of the entity's third-party risk management program.
 - Receives reports that include effectiveness of security controls, performance metrics, resolved versus outstanding issues, and root causes of problems in reports from third-party service providers.
 - Monitors third-party service provider's ability to meet defined SLAs, compliance with identified action plans when they are not met, and remuneration of penalty fees when appropriate.

- e. If an entity has outsourcing arrangements in the cloud, determine whether management explores the use of tools designed for cloud computing.
2. Determine whether management defines objectives for IT and operations and KPIs to help management measure those objectives. Additionally, evaluate whether management does the following:
 - a. Aligns KPIs with the entity's ERM processes and uses those KPIs to assess the performance of IT and operations across the entity.
 - b. Sets KPI benchmarks to achieve and analyzes deviations from those benchmarks.
 - c. Automates the collection of KPIs, where possible.
 - d. Has a useful set of KPIs.
 - e. Regularly reviews KPI reports and provides appropriate reporting up to the board.
 - f. Implements corrective action plans to address deviations or negative trends, assigns individuals responsible, and monitors progress to completion.
 - g. Meets with stakeholders to review IT and operations KPIs to determine whether they are appropriate indicators of the ability to meet the entity's strategic objectives.
3. Determine whether management uses control self-assessments, risk control self-assessments, or other methods to monitor the effectiveness of IT operations controls and gauge performance, assess the criticality of systems, and identify existing risks. Determine whether management evaluates results and uses them to continuously improve the entity's operations.
4. Determine whether management has a continuous improvement process in place to recommend changes to the entity's IT environment. Evaluate whether management does the following:
 - a. Develops improvement strategies for operations and prioritizes projects.
 - b. Bases improvement decisions on the potential benefit and ease of implementation, with a focus on important IT processes and core competencies.
 - c. Maintains a process to measure the results of continuous improvement efforts and includes the following:
 - Ongoing practice of process improvement.
 - Enterprise-wide practice of service improvement that augments the ability to provide value to its stakeholders and customers.

Objective 18: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the examiner-in-charge regarding the following:
 - a. Apparent violations of laws and regulations.
 - b. Significant issues warranting inclusion in the report of examination.
 - c. Proposed Uniform Rating System for IT (URSIT) support and delivery component rating and the potential impact of the examiner's conclusions on composite or other URSIT component ratings.
 - d. Potential impact of the examiner's conclusions on the entity's risk assessment(s).

2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.
3. Document conclusions in a memorandum to the examiner-in-charge that provides report-ready comments for all relevant sections of the report of examination and clarifying guidance to future examiners.
4. Organize work papers to show clear support for significant findings by examination objective.

APPENDIX B: GLOSSARY

The purpose of the glossary is to define technical terms used in the *FFIEC IT Examination Handbook* booklets in the context of supervisory activities for the entities over which FFIEC members have supervisory authority. The FFIEC members strive to align terminology in the glossary with appropriate authoritative standards, including the [NIST Computer Security Resource Center Glossary](#) (NIST Glossary) as the primary source for cyber-related definitions, as appropriate. FFIEC members employed the following process to select, modify, or develop definitions.

When a NIST definition existed:

- If NIST had a defined term and modifications to the definition were unnecessary, the FFIEC members included the NIST definition in this glossary. When multiple NIST definitions were available for the same term, the FFIEC members selected a definition for supervisory purposes.
- If NIST had a defined term, but the definition needed additional clarity for supervisory purposes to assist with the identification of safety and soundness and enterprise risks related to IT, the FFIEC members included both the NIST definition and the FFIEC-adapted definition. Definitions of this nature are labeled “FFIEC Adapted for Supervisory Purposes” in this glossary’s source column.

When a NIST definition did not exist or the definition was not appropriate for supervisory purposes:

- If NIST did not have a defined term, but there was an appropriate authoritative third-party source (e.g., the ISO Glossary), the FFIEC members included that authoritative definition.
- If NIST did not have a defined term and there was not an appropriate authoritative third-party source, the FFIEC members developed a definition for supervisory purposes. Definitions of this nature are labeled “FFIEC Developed for Supervisory Purposes” in this glossary’s source column.

Note: Due to the constantly evolving nature of IT and its associated risks, the FFIEC members may update definitions to maintain alignment with other government agencies and the financial services industry.

Term	Definition	Source
A		
Access control	Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space.	NIST Glossary
Add-on	Additional code that provides extra features to a program, extends certain functions, or provides additional capabilities.	FFIEC Developed for Supervisory Purposes

Term	Definition	Source
Anomaly-based detection	The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.	NIST SP 800-94 Rev. 1
Antivirus software	A program specifically designed to detect many forms of malware and prevent them from infecting computers, as well as cleaning computers that have already been infected.	NIST Glossary
Application	A system for collecting, saving, processing, and presenting data by means of a computer. The term application is generally used when referring to a component of software that can be executed. The terms application and software application are often used synonymously.	NIST Glossary
Application firewall	A firewall that uses stateful protocol analysis to analyze network traffic for one or more applications.	NIST Glossary
Application programming interface (API)	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.	NIST Glossary
	Software code that allows two or more different programs to communicate with each other.	FFIEC Adapted for Supervisory Purposes
Architecture	Refers to the manner in which the strategic design of the hardware and software infrastructure components (e.g., devices, systems, and networks) are organized and integrated to achieve and support the entity's business objectives.	FFIEC Developed for Supervisory Purposes
Artificial intelligence (AI)	Refers to the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action—whether digitally or as the smart software behind autonomous physical systems.	U.S. Department of Defense
Authentication	A process that establishes the source of information, provides assurance of an entity's identity or provides assurance of the integrity of communications sessions, messages, documents or stored data.	NIST Glossary
	A process designed to establish the source of the information, validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.	FFIEC Adapted for Supervisory Purposes
Authorization	The granting or denying of access rights to a user, program, or process.	NIST Glossary
Authorization boundary	All components of an information system to be authorized for operation by an authorizing official, and excludes separately authorized systems, to which the information system is connected.	NIST Glossary
Availability	Ensuring timely and reliable access to and use of information.	NIST Glossary
B		
Backup	A copy of files and programs made to facilitate recovery, if necessary.	NIST Glossary
Bandwidth (utilization)	The range between the highest and lowest transmittable frequencies. It equates to the transmission capacity of an electronic line and is expressed in bytes per second or Hertz (cycles per second).	ISACA Glossary

Term	Definition	Source
Baseline configuration	A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.	NIST Glossary
Big data	Extensive datasets—primarily in the characteristics of volume, variety, velocity, and/or variability—that require a scalable architecture for efficient storage, manipulation, and analysis.	NIST Big Data Interoperability Framework: Volume 1
Blacklist	A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity.	NIST Glossary
C		
Capacity management	The process of planning and monitoring an entity’s technology resources to support current and future strategic objectives.	FFIEC Developed for Supervisory Purposes
Capacity planning	Systematic determination of resource requirements for the projected output, over a specific period.	NIST Glossary
Capture	The act of recording in a permanent file.	Merriam-Webster
Central processing unit (CPU)	Computer hardware that houses the electronic circuits that control/direct all operations of the computer system.	ISACA Glossary
Change control	Change control is the process through which all requests to change the approved baseline of a project, program, or portfolio are captured, evaluated and then approved, rejected, or deferred.	Association for Project Management
	Change control is the process through which all requests to change the approved baseline of a project, program, or portfolio are documented, evaluated and then approved, rejected, or deferred. Change control is an element in an overall change management process.	FFIEC Adapted for Supervisory Purposes
Change management	The continuous process of maintaining the integrity of hardware, software, firmware, and documentation and controlling and approving changes (e.g., addition, modification, or elimination) to information or technology assets or related infrastructure.	U.S. CERT
Cloud access security broker (CASB)	A software tool or service that sits between an entity’s on-premises infrastructure and a cloud service provider’s infrastructure as a “gatekeeper” to monitor activity and enforce the entity’s security policies (e.g., authentication, single sign-on, authorization, credential mapping, and encryption) as the cloud-based resources are accessed.	FFIEC Developed for Supervisory Purposes
Cloud broker	An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between cloud service providers and cloud consumers.	NIST SP 500-291
Cloud bursting	The ability of an entity with in-house infrastructure to use the public cloud during peak periods.	FFIEC Developed for Supervisory Purposes
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g.,	NIST Glossary

Term	Definition	Source
	networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	
Cloud service provider	Referred to as a cloud provider. A service provider who offers customers storage or software solutions available via a public network, usually the internet.	(ISC)² Certified Cloud Security Professional Study Guide
	A third-party service provider who offers clients services over the public internet. Examples of services could be applications (SaaS), operating systems (PaaS), or infrastructure (IaaS).	FFIEC Adapted for Supervisory Purposes
Commercial off-the-shelf (COTS) software	A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public. It is also referred to as off-the-shelf.	NIST Glossary
Community cloud	The community cloud infrastructure is provisioned for exclusive use by a specific community (e.g., government agencies, financial services, or banks) of entities that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). The community cloud infrastructure may be owned, managed, and operated by one or more of the constituents in the community, a third party, or some combination of them, and it may exist on or off premises.	NIST Glossary
Compromise	The unauthorized disclosure, modification, substitution, or use of sensitive data (e.g., keying material and other security related information).	NIST Glossary
Confidentiality	The property that sensitive information is not disclosed to unauthorized entities.	NIST Glossary
Configuration	The selection of one of the sets of possible combinations of features of a system.	NIST Glossary
	The selection of combinations of conditions, parameters, features, and specifications of a system.	FFIEC Adapted for Supervisory Purposes
Configuration management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.	NIST Glossary
Configuration settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.	NIST Glossary
Container	A method for packaging and securely running an application within a virtualized environment.	NIST Glossary
Content filtering	The process of monitoring communications such as email and web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.	NIST Glossary
Continuous improvement	In operations, the ongoing effort to improve an entity's products, services, or processes to meet business objectives.	FFIEC Developed for Supervisory Purposes

Term	Definition	Source
Cyber risk	Risk of financial loss, operational disruption, or damage from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system.	NIST Glossary
	Risk of financial loss, operational disruption, or damage from the failure of the digital technologies employed for informational and/or operational functions introduced to a system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system.	FFIEC Adapted for Supervisory Purposes
D		
Dashboard	A tool that consolidates and communicates information relevant to the entity in near real-time. It is generally visual and often uses a variety of charts.	NIST SP 800-137
Data	A representation of information as stored or transmitted.	NIST Glossary
	A physical or digital representation of information processed, stored (at rest), or transmitted (in transit).	FFIEC Adapted for Supervisory Purposes
Data analytics	The systematic process of evaluating and organizing data sets to draw insights, make predictions, and reveal trends using logical analysis.	FFIEC Developed for Supervisory Purposes
Data center	A facility that houses virtual and/or physical information technology infrastructure(s) (e.g., computer, server, and networking systems and components) designed to store, process, and serve large amounts of data in support of an entity's strategic and business objectives. A data center may be a dedicated facility or an area or room that contains computer, server, and networking systems and components, and may be private or shared (e.g., a co-location facility).	FFIEC Developed for Supervisory Purposes
Data classification	Categorizing data based on its level of sensitivity (e.g., confidentiality, integrity, or availability), value, and criticality to the entity.	FFIEC Developed for Supervisory Purposes
Data communications	The transfer of data over networks using a combination of telecommunication services and network devices.	FFIEC Developed for Supervisory Purposes
Data governance	A set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority and management and decision-making parameters related to the data produced or managed by the enterprise.	NIST Glossary
Data management	The practice of putting into place policies, procedures and best practices to ensure that data is understandable, trusted, visible, accessible and interoperable.	DHS Lexicon Terms and Definitions
	The practice of putting into place policies, procedures, and best practices to ensure that data are understandable, trusted, visible, accessible, and interoperable to ensure that user needs are met.	FFIEC Adapted for Supervisory Purposes
Database	A repository of information or data, which may or may not be a traditional relational database system.	NIST Glossary

Term	Definition	Source
	A repository of information or data organized to be accessed, managed, and updated.	FFIEC Adapted for Supervisory Purposes
Denial of service (DOS) attack	An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.	ISACA Glossary
Device	A piece of equipment or a mechanism designed to serve a special purpose or perform a special function.	Merriam-Webster
Dirty power	A term used to describe a power line where disturbances (e.g., outages, voltage spikes, and drop-outs) occur.	A New IEC Standard on the Measurement of Power Quality Parameters
Distributed denial of service (DDOS)	A denial of service technique that uses numerous hosts to perform the attack.	NIST Glossary
Domain name	A domain name is a human-friendly name (such as “www.dhs.gov”) that is resolved (i.e., translates domain names into Internet Protocol [IP] addresses) by a network of domain name service servers to a specific IP address, which is in turn, associated with a single host (referring to a single server or server cluster).	DHS Directives System
	A unique identifier for a network address.	FFIEC Adapted for Supervisory Purposes
Domain name system (DNS)	A distributed computing system that enables access to Internet resources by user-friendly domain names rather than IP addresses, by translating domain names to IP addresses and back. Also known as domain name service (DNS).	NIST SP 800-81-2
Dynamic host configuration protocol (DHCP)	A protocol used by networked computers (clients) to obtain IP addresses and other parameters, such as the default gateway, subnet mask and IP addresses of domain name system servers from a DHCP server. The DHCP server ensures that all IP addresses are unique. IP address pool management is done by the server and not by a human network administrator.	ISACA Glossary
E		
Encryption	Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.	NIST Glossary
End-of-life (EOL)	With respect to technology, a time frame usually defined by a technology vendor to describe when an asset has reached the end of its useful life cycle and when the vendor will no longer maintain and support the asset or continue to sell or license it.	FFIEC Developed for Supervisory Purposes
Enterprise architecture	The description of an enterprise’s entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise’s boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise’s overall security posture.	NIST Glossary

Term	Definition	Source
Enterprise resource planning system	A packaged business software system that allows an enterprise to automate and integrate the majority of its business processes, share common data and practices across the entire enterprise, and produce and access information in a real-time environment.	ISACA Glossary
Event	Occurrence or change of a particular set of circumstances.	NIST Glossary
	An occurrence or change in circumstances that may affect operations. An event can be physical, cyber, or a combination of both.	FFIEC Developed for Supervisory Purposes
F		
False positive	A result that has been mistakenly identified as a problem when, in reality, the situation is normal.	ISACA Glossary
File exchange	(Also known as file sharing) A method of sending and receiving files inside the entity and with other parties through email attachments, file sharing services, and other means.	NIST Security Considerations for Exchanging Files Over the Internet
Firewall	A gateway that limits access between networks in accordance with local security policy.	NIST Glossary
Functional testing	Testing that verifies that an implementation of some function operates correctly.	NIST Glossary
G		
Gateway	An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.	NIST Glossary
H		
Hardening	A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services and utilities from the system. (Referred to as system hardening)	ISACA Glossary
	A process intended to eliminate as many security risks as possible by implementing security controls (e.g., changing default passwords, enabling security settings, and protecting privileged accounts), patching vulnerabilities, turning off nonessential services, and removing all nonessential software programs, protocols, and utilities from the system.	FFIEC Adapted for Supervisory Purposes
Hardware	The physical components of an information system.	NIST Glossary
Hashing	The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.	NIST Glossary
Help desk	A service offered via telephone/Internet by an enterprise to its clients or employees that provides information, assistance and troubleshooting advice regarding software, hardware or networks.	ISACA Glossary
Hub	A common connection point for devices in a network. Hubs commonly are used to pass data from one device (or segment) to another.	NIST Glossary
Hybrid cloud	The hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (e.g., private, community, or public) that	NIST Glossary

Term	Definition	Source
	are unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).	
Hybrid-hosted-software arrangement	An agreement where software resides at both the entity (also referred to as on-premise) and on the third-party service provider's servers (e.g., software as a service).	FFIEC Developed for Supervisory Purposes
Hypervisor	The virtualization component that manages the guest operating systems (OSs) on a host and controls the flow of instructions between the guest OSs and the physical hardware.	NIST Glossary
I		
Identity and access management (IAM)	Encapsulates people, processes, and products to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources.	ISACA Glossary
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	NIST Glossary
Incident management	The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible.	FFIEC Developed for Supervisory Purposes
Information security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	NIST Glossary
Information technology asset management (ITAM)	Refers to a set of policies and procedures that an organization uses to track, audit, and monitor the state of its IT assets, and maintain system configurations.	NIST SP 1800-5
Infrastructure	System of facilities, equipment, and services needed for the operation of an organization.	ISO 22300:2018(en)
	The physical elements, products, and services necessary to provide and maintain ongoing operations to support business activity and includes the maintenance of physical facilities.	FFIEC Adapted for Supervisory Purposes
Infrastructure as a service (IaaS)	IaaS provides entities with the ability to provision processing, storage, networks, and other fundamental computing resources where the entity is able to deploy and run software, which can include operating systems and applications. The entity does not manage or control the underlying cloud infrastructure; however, it has control over operating systems, storage, and deployed applications. Entities have the maximum flexibility to customize their cloud services and user interfaces.	NIST SP 500-316
Integrity	A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored.	NIST Glossary

Term	Definition	Source
Interdependencies	When two or more departments, processes, functions, or third-party providers interact to successfully complete a task, business function, or process.	FFIEC Developed for Supervisory Purposes
Internet of things (IoT)	Refers to the collection of technologies that allow information to be sent to and received from physical devices (e.g., security systems, HVAC systems, intelligent personal assistants, and kitchen appliances), that were not traditionally thought of as IT assets, using the internet. These devices have the ability to send and receive data over a network without necessarily requiring human-to-human or human-to-computer interaction using embedded computing capability and network connectivity and unique identifiers (e.g., IP address).	FFIEC Developed for Supervisory Purposes
Intrusion detection system (IDS)	A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.	NIST Glossary
Intrusion prevention system (IPS)	A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.	NIST Glossary
IP address	A unique binary number used to identify devices on a TCP/IP network.	ISACA Glossary
IT infrastructure	A subset of infrastructure that includes hardware, network and telecommunications, software, IT environmental controls (e.g., power, cooling, and ventilation), and physical access.	FFIEC Developed for Supervisory Purposes
J		
Jailbreaking (also known as rooting)	To allow the device's owner to remove manufacturer or carrier restrictions, to gain full access to the root of the operating system and access all the features.	FFIEC Developed for Supervisory Purposes
Job scheduling	Generally an automated process to allocate system resources and execute processes based on the priority and processing resources available.	FFIEC Developed for Supervisory Purposes
L		
Latency	Time delay in processing voice packets.	NIST Glossary
	Time delay in processing voice and data packets.	FFIEC Adapted for Supervisory Purposes
License	A permission granted by competent authority to engage in a business or occupation or in an activity otherwise unlawful.	Merriam-Webster
Load balancing	Load balancers distribute HTTP requests over multiple Web servers, allowing organizations to increase the capacity of their Web site by transparently adding additional servers. Load balancers act as virtual servers, receiving all HTTP requests to the Web site. These requests are forwarded, based on the load balancer's policy, to one of the servers that hosts the Web site. The load balancer's policy attempts to ensure that each server receives a similar number of requests. Many load balancers are capable of monitoring the servers and compensating if one of the servers becomes unavailable.	NIST SP 800-44 v.2

Term	Definition	Source
	The distribution of processing (e.g., network traffic, processing requests or power) across equipment to ensure that any one device is not overwhelmed by high demand.	FFIEC Adapted for Supervisory Purposes
Local area network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.	NIST Glossary
Log	A record of events occurring within an entity's systems and networks.	NIST Glossary
Log management	The process to generate, transmit, store, analyze, and dispose of log data.	NIST Glossary
Loose coupling	An approach to designing systems so that linked components of networks, software, and services can be scaled to operate as independently as possible, in order to avoid issues with one component adversely affecting others.	FFIEC Developed for Supervisory Purposes
M		
Machine learning (ML)	The process of using an algorithm(s) to help computers learn without being explicitly programmed and identify patterns within data. Those patterns are then used to create a data model that can make predictions.	FFIEC Developed for Supervisory Purposes
Mainframe	A large, high-speed computer, especially one supporting numerous workstations or peripherals.	ISACA Glossary
Maintenance	Any act that either prevents the failure or malfunction of equipment or restores its operating capability.	NIST Glossary
Malicious code	Unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses.	DHS, CISA Security Tip (ST18-004)
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.	NIST Glossary
Man in the middle (MitM) attack	An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them.	NIST Glossary
Masking	The process of systematically removing a field or replacing it with a value in a way that does not preserve the analytic utility of the value, such as replacing a phone number with asterisks or a randomly generated pseudonym.	NIST Glossary
Media access control (MAC)	Applied to the hardware at the factory and cannot be modified, MAC is a unique, 48-bit, hard-coded address of a physical layer device, such as an Ethernet local area network (LAN) or a wireless network card.	ISACA Glossary
Media access control (MAC) address	A unique identifier assigned to network interfaces for communications on the physical network segment.	ISACA Glossary
	A unique identifier assigned to network interfaces for communications on the physical network segment. MAC is a 48-bit,	FFIEC Adapted for Supervisory Purposes

Term	Definition	Source
	hard-coded address applied to the hardware at the factory and cannot be modified.	
Metadata	Data about data. For file systems, metadata is data that provides information about a file's contents.	NIST Glossary
	Data about data. Examples of metadata include purpose of the data, creator or owner of the data, file size, location where the data were created, and source of the data.	FFIEC Adapted for Supervisory Purposes
Microservices	A set of containers that work together to compose an application.	NIST Glossary
Mobile computing	Extends the concept of wireless computing to devices that enable new kinds of applications and expand an enterprise network to reach places in circumstances that could never have been done by other means. Mobile computing is comprised of personal digital assistants (PDAs), cellular phones, laptops and other technologies of this kind.	ISACA Glossary
Mobile device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source.	NIST Glossary
Multi-factor authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password or personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device or token); or (iii) something you are (e.g., biometric).	NIST Glossary
Multi-tenancy	Design where one or more entities and their information and technology assets reside in a shared environment. The instances (tenants) are logically isolated, but physically integrated.	FFIEC Developed for Supervisory Purposes
N		
Network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.	NIST Glossary
Network attached storage (NAS)	Dedicated storage devices that centralize storage of data. These storage devices generally do not provide traditional file, print, or application services. These devices could be physical or virtual.	ISACA Glossary
Network backbone	The main communication channel of a network that interconnects one or more network segments and provides a path for the exchange of data between devices. A backbone can span any geographic area.	FFIEC Developed for Supervisory Purposes
Network diagram	A network diagram (also called a network map or network topology) is a visual representation of nodes and connections in a computer network.	FFIEC Developed for Supervisory Purposes
Network operations center (NOC)	The central location or department responsible for monitoring the health and performance of the network, including analyzing and maintaining network traffic, telecommunications, and network disruptions.	FFIEC Developed for Supervisory Purposes

Term	Definition	Source
Network performance	Refers to the speed and response time of a network.	FFIEC Developed for Supervisory Purposes
Node	Point at which terminals are given access to a network.	ISACA Glossary
Non-production environment	Systems (e.g., applications, infrastructure, networks, operating systems) that are not used for production purposes. For example, systems that are used as development or test environments for new software or technologies or changes to existing software or technologies.	FFIEC Developed for Supervisory Purposes
O		
Open source software	Open source software is software that can be accessed, used, modified, and shared by anyone.	NIST S 6106.01
Operating system (OS)	The software “master control application” that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.	NIST Glossary
Operational controls	The day-to-day procedures and mechanisms used to protect operational systems and software. Operational controls affect the system and software environment.	NIST Glossary
Operational level agreement (OLA)	An internal agreement covering the delivery of services that support the IT organization in its delivery of services.	ISACA Glossary
Operational resilience	The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.	NIST Glossary
	The ability of an entity’s personnel, systems, telecommunications networks, activities, or processes to resist, absorb, and recover from or adapt to an incident that may cause harm, destruction, or loss of ability to perform mission-related functions.	FFIEC Adapted for Supervisory Purposes
Operations	The performance of activities comprising methods, principles, processes, procedures, and services that support business functions.	FFIEC Developed for Supervisory Purposes
Operations management	The process of overseeing the methods, activities, or performance of practical work, and application of principles, processes, procedures, and services of an entity, utilizing business resources.	FFIEC Developed for Supervisory Purposes
Out-of-band	Communication between parties utilizing a means or method that differs from the current method of communication.	NIST Glossary
P		
Packet	A logical unit of network communications produced by the transport layer.	NIST Glossary
Packet sniffers	Software that monitors network traffic on wired or wireless networks and captures packets.	NIST Glossary

Term	Definition	Source
Patch	Fixes to software programming errors and vulnerabilities.	ISACA Glossary
Patch management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.	NIST Glossary
Penetration testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.	NIST Glossary
Physical access controls	Mitigations that protect an entity's facilities, physical assets, and technology assets.	NIST 800-53 Rev. 5
Platform	A computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run.	NIST Glossary
Platform as a service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.	NIST Glossary
Policies	Statements, rules or assertions that specify the correct or expected behavior of an entity.	NIST Glossary
Port	The entry or exit point from a computer for connecting communications or peripheral devices.	NIST Glossary
Portability	1) The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. 2) The ability of software or of a system to run on more than one type or size of computer under more than one operating system.	ATIS Telecom Glossary
Power sag (aka voltage sag)	A brief reduction in voltage, often caused by a short circuit, overload or loose connection.	FFIEC Developed for Supervisory Purposes
Primary working memory	For the purposes of this booklet, primary working memory refers to the temporary storage or memory needed to run software applications that is shipped with the CPU and is generally supplemented by additional data storage (i.e., long-term storage).	NIST Glossary
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single entity with multiple business units. The private cloud infrastructure may be owned, managed, and operated by the entity, a third party, or some combination of them, and it may exist on or off premises.	NIST Glossary
Problem	In IT, the unknown underlying cause of one or more incidents.	ISACA Glossary
Procedures	A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.	ISACA Glossary

Term	Definition	Source
Process improvement	Process improvement includes the actions taken to improve the quality of the organization's processes aligned with the business needs and the needs of other concerned parties.	ISO/IEC 33001:2015(en)
Promiscuous mode	A configuration setting for a network interface card that causes it to accept all incoming packets that it sees, regardless of their intended destinations.	NIST SP 800-94
Protocol	A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems.	NIST Glossary
Provisioning	The activity of obtaining the equipment and resources you need for a particular activity.	Cambridge Dictionary
	The activity of obtaining, modifying, and making available the equipment, resources, software, or services a user needs to carry out a particular activity.	FFIEC Adapted for Supervisory Purposes
Public cloud	The public cloud infrastructure is provisioned for open use by the general public. The public cloud infrastructure may be owned, managed, and operated by a business, academic, government organization, or some combination of them. It exists on the premises of the cloud service provider.	NIST Glossary
Q		
Query	In databases, a request for data or information from a table or combination of tables.	FFIEC Developed for Supervisory Purposes
R		
Rate limiting	A process used to control the rate of network traffic (e.g., incoming and outgoing). Its purpose is to prevent a failure of service (e.g., from a DOS attack or system overload).	FFIEC Developed for Supervisory Purposes
Release	A collection of new and/or changed configuration items, which are tested and introduced into a production environment together.	NIST Glossary
Remote access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).	NIST Glossary
Replication	Involves the use of redundant software or hardware elements to provide availability and fault-tolerant capabilities. In a database context, replication involves the sharing of data between databases to reduce workload among database servers, thereby improving client performance while maintaining consistency among all systems.	ISACA Glossary
Report	A detailed account or statement. For the purposes of IT, the report provides analysis that supports informed decision-making.	Merriam-Webster
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.	NIST Glossary
Role-based access	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.	NIST Glossary

Term	Definition	Source
Router	On a network, a device that determines the best path for forwarding a data packet toward its destination. The router is connected to at least two networks and is located at the gateway where one network meets another.	NIST Glossary
	A device that determines the best path for forwarding a data packet toward its destination on a network or between networks. The router is connected to at least two network segments and is located at the gateway where one network segment meets another.	FFIEC Adapted for Supervisory Purposes
Routing	In computer networking, the process of selecting a path for traffic within a network or between multiple networks.	FFIEC Developed for Supervisory Purposes
S		
Sanitization	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.	NIST Glossary
Scalability	Refers to how well a hardware and software system can adapt to increased demands. For example, a scalable network system would be one that can start with just a few nodes but can easily expand to thousands of nodes. Scalability can be a very important feature because it means the entity can invest in a system with confidence they will not quickly outgrow it.	FFIEC Developed for Supervisory Purposes
Scheduling	A method used in the information processing facility to determine and establish the sequence of computer job processing.	ISACA Glossary
Security	The state in which the integrity, confidentiality, and accessibility of information, service or network entity is assured.	NIST Glossary
Security operations center (SOC)	The centralized unit or department responsible for monitoring and improving the entity's network for security issues and preventing, detecting, and responding to potential incidents or cyber attacks.	FFIEC Developed for Supervisory Purposes
Server	A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).	NIST Glossary
Service improvement	The actions taken to identify and execute methods to improve an entity's services and align them with its business objectives.	FFIEC Developed for Supervisory Purposes
Service level agreement (SLA)	Defines the specific responsibilities of the service provider and sets the customer expectations.	NIST Glossary
	A formal agreement between two parties that records a common understanding about products or services to be delivered, priorities, responsibilities, guarantees, and warranties between the parties. In addition, the agreement describes the nature, quality, security, availability, scope, and timeliness of delivery and response of the parties, the point(s) of contact for end-user problems, and the metrics by which the effectiveness of the process is monitored and approved, and may include other measurable objectives. The agreement should cover not only expected day-to-day situations, but also unexpected or adverse events, as the need for the service may vary.	FFIEC Adapted Definition for Supervisory Purposes

Term	Definition	Source
Service management	The process of overseeing and managing an entity's activities and resources to allow management of IT functions to support and service the entity's strategic goals and objectives. Activities involved in this process include planning, designing, transitioning, delivering, and improving services.	FFIEC Developed for Supervisory Purposes
Shadow IT	Refers to unauthorized hardware and other devices, software, or services operating in an entity's IT environment.	FFIEC Developed for Supervisory Purposes
Signature	A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.	NIST Glossary
Signature-based detection	The process of comparing signatures against observed events to identify possible incidents.	NIST SP 800-94 Rev. 1
Single point of failure	An element in the design, configuration or implementation of a system that can cause the entire system to fail if it stops working.	FFIEC Developed for Supervisory Purposes
Social engineering	The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.	NIST Glossary
Software	Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.	NIST Glossary
Software as a service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.	NIST Glossary
Standard image	The approved set of server configurations, applications, and systems, which can be used to deploy servers consistently and rebuild them more easily and quickly, when necessary.	FFIEC Developed for Supervisory Purposes
Standards	Rules, conditions, or requirements describing the following information for products, systems, services or practices: (i) Classification of components. (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures.	NIST Glossary
Stateful protocol analysis	The process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.	NIST SP 800-94 Rev. 1
Storage area network (SAN)	A variation of a local area network (LAN) that is dedicated for the express purpose of connecting storage devices to servers and other computing devices. SANs centralize the process for the storage and administration of data. These devices could be physical or virtual.	ISACA Glossary
Structured data	Data that has a predefined data model or is organized in a predefined way.	NIST SP 1500-1 Rev. 2

Term	Definition	Source
Supply chain	A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.	NIST Glossary
Supply chain risk management	The implementation of processes, tools, or techniques to minimize the adverse impact of attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.	NIST Glossary
	The implementation of processes, tools, or techniques to minimize the adverse impact of attacks that allow the adversary to exploit vulnerabilities inserted prior to installation. This is done in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).	FFIEC Adapted for Supervisory Purposes
Switch	A network device that filters and forwards packets between LAN segments.	NIST Glossary
System	A combination of interacting elements organized to achieve one or more stated purposes.	NIST Glossary
System and organization controls (SOC)	The suite of services practitioners may provide relating to system-level controls of a service organization and system- or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the AICPA enables the introduction of new internal control examinations that may be performed (a) for other types of organizations, in addition to service organizations, and (b) on either system-level or entity-level controls of such organizations.	AICPA
System development life cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.	NIST Glossary
T		
Tele-communications	The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.	NIST Glossary
Tenant	One who has the occupation or temporary possession of lands or tenements of another.	Merriam-Webster
	In the context of a computing environment, a customer that utilizes assets (e.g., shared applications or computing resources) or occupies space of another (e.g., cloud service provider).	FFIEC Adapted for Supervisory Purposes
Test	An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in an IT plan.	NIST Glossary

Term	Definition	Source
Third-party service provider	Any independent party to whom an entity outsources activities that the entity itself is authorized to perform, including a technology service provider.	FFIEC Developed for Supervisory Purposes
Timestamp	A token or packet of information that is used to provide assurance of timeliness; the timestamp contains timestamped data, including a time, and a signature generated by a Trusted Timestamp Authority.	NIST Glossary
Transmission	An act, process, or instance of transmitting.	Merriam-Webster
	The act of sending or conveying data, voice, audio, or video from one person or place to another.	FFIEC Adapted for Supervisory Purposes
Transmission control protocol/internet protocol (TCP/IP)	A set of communications protocols used for the exchange of information over networks and especially over the Internet.	Merriam-Webster
Trojan horse (trojan)	A useful or seemingly useful program that contains hidden code of a malicious nature that executes when the program is invoked.	NIST Glossary
Trusted timestamp authority	An entity that is trusted to provide accurate time information.	NIST Glossary
Tunneling	Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.	NIST Glossary
U		
Uninterruptible power supply (UPS)	A device with an internal battery that allows connected devices to run for at least a short time when the primary power source is lost.	NIST Glossary
Unstructured data	Data that does not have a predefined data model or is not organized in a predefined way.	NIST SP 1500-1 Rev. 2
Uptime	Time during which a piece of equipment (such as a computer) is functioning or able to function.	Merriam-Webster
Useful life	The normal expected operating life of an asset.	Internal Revenue Service
Utility software (utilities)	Type of system software that allow users to perform maintenance types of tasks, usually relating to managing a computer's devices or programs. Most OSs include several utility programs, including file compression, defragmentation, diagnostics, and performance optimization.	FFIEC Developed for Supervisory Purposes
V		
Virtualization	The simulation of the software and/or hardware upon which other software runs.	NIST Glossary
Virtual machine (VM)	Software that allows a single host to run one or more guest operating systems.	NIST Glossary

Term	Definition	Source
	A simulated environment created by virtualization using software that allows a single host to run one or more guest operating systems.	FFIEC Adapted for Supervisory Purposes
Voice over internet protocol (VoIP)	A technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.	Federal Communications Commission (FCC)
Voice response unit (VRU)	An automated telephone answering system consisting of hardware and software that allows a caller to interact with a phone keypad or through voice recognition. Sometimes referred to as an interactive voice response (IVR) unit.	FFIEC Developed Definition for Supervisory Purposes
Vulnerability	Weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.	NIST Glossary
Vulnerability assessment	Systematic examination of an information system or product to determine the adequacy of security and privacy measures, identify security and privacy deficiencies, provide data from which to predict the effectiveness of proposed security and privacy measures, and confirm the adequacy of such measures after implementation.	NIST Glossary
Vulnerability management	Vulnerability management (continuous) is a process to (continuously) acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	Center for Internet Security Glossary
W		
Web portal	Provides a single point of entry into the [service-oriented architecture] for requester entities, enabling them to access Web services transparently from any device at virtually any location.	NIST Glossary
Whitelist	A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline.	NIST Glossary
Workstation	A computer used for tasks such as programming, engineering, and design.	NIST Glossary
Worm	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.	NIST Glossary
Z		
Zero trust architecture	An enterprise cybersecurity strategy that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement.	NIST SP 800-207

APPENDIX C: ABBREVIATIONS

ACF2	Access Control Facility
AI	artificial intelligence
AICPA	American Institute of Certified Public Accountants
AIO	architecture, infrastructure, and operations
API	application programming interface
BYOD	bring your own device
CDO	chief data officer
CFPB	Consumer Financial Protection Bureau
CIO	chief information officer
CIS	Center for Internet Security
COTS	commercial off-the-shelf
CPU	central processing unit
CRM	customer relationship management
CTO	chief technology officer
DBA	database administrator
DHCP	dynamic host configuration protocol
DNS	domain name system or domain name service
DDOS	distributed denial of service
DOS	denial of service
EA	enterprise architecture
EOL	end-of-life
ERM	enterprise risk management
ERP	enterprise resource planning
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FRB	Board of Governors of the Federal Reserve System
HVAC	heating, ventilation, and air conditioning
IaaS	infrastructure as a service
IAM	identity and access management
IDS/IPS	intrusion detection and prevention system
IoT	internet of things
IP	internet protocol
ISO	International Organization for Standardization
IT	information technology
ITAM	information technology asset management
KPI	key performance indicator
KRI	key risk indicator
LAN	local area network
MAC	media access control
MAN	metropolitan area network
ML	machine learning
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
NOC	network operations center

OCC	Office of the Comptroller of the Currency
OS	operating system
PaaS	platform as a service
PCI DSS	Payment Card Industry Data Security Standard
PIN	personal identification number
PSTN	public switched telephone network
RACF	Resource Access Control Facility
SaaS	software as a service
SAN	storage area network
SCM	supply chain management
SIEM	security information and event management
SLA	service-level agreement
SLC	State Liaison Committee
SOC	security operations center
SOC	system and organization controls
SOX	Sarbanes–Oxley Act
SPM	service portfolio management
TCP/IP	transmission control protocol/internet protocol
TOGAF	The Open Group Architecture Framework
UPS	uninterruptible power supply
VM	virtual machine
VoIP	voice over internet protocol
VPN	virtual private network
WAN	wide area network
ZTA	zero trust architecture

APPENDIX D: REFERENCES

Laws

- 12 U.S.C. 1861–1867, “Bank Service Company Act”
- 12 U.S.C. 1882, “Bank Protection Act”
- 12 U.S.C. 5481(14) and (26), 5514, 5515, and 5531, “Consumer Financial Protection Act of 2010”
- 15 U.S.C. 1681w, “Fair and Accurate Credit Transactions Act”
- 15 U.S.C. 6801 and 6805(b), “Gramm–Leach–Bliley Act”
- 18 U.S.C. 1030, “Fraud and Related Activity in Connection With Computers”

Consumer Financial Protection Bureau

Regulations

- 12 CFR 1005, “[Electronic Fund Transfers \(Regulation E\)](#)”
- 12 CFR 1016, “[Privacy of Consumer Financial Information \(Regulation P\)](#)”
- 12 CFR 1022, “[Fair Credit Reporting Act \(Regulation V\)](#)”

Guidance

- CFPB Compliance Bulletin and Policy Guidance; “[2016-02: Service Providers](#)” (October 2016)

Federal Deposit Insurance Corporation

Regulations

- 12 CFR 304.3(d), “[Notification of Performance of Bank Services, Form FDIC 6120/06](#)”
- 12 CFR 326, subpart A, “[Minimum Security Procedures](#)”
- 12 CFR 332, “[Privacy of Consumer Financial Information](#)”
- 12 CFR 364, appendix A, “[Interagency Guidelines Establishing Standards for Safety and Soundness](#)”
- 12 CFR 364, appendix B, “[Interagency Guidelines Establishing Information Security Standards](#)”
- 12 CFR 364, supplement A to appendix B, “[Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#)”

Guidance

- FIL-103-2020, “[Sound Practices to Strengthen Operational Resilience](#)” (November 2, 2020)
- FIL-52-2020, “[FFIEC Joint Statement on Risk Management for Cloud Computing Services](#)” (April 30, 2020)
- FIL-25-2020, “[Identification of Essential Critical Infrastructure Workers During the COVID-19 Response Efforts](#)” (March 26, 2020)

- FIL-14-2020, [“Interagency Statement on Pandemic Planning”](#) (March 6, 2020)
- FIL-19-2019, [“Technology Service Provider Contracts”](#) (April 2, 2019)
- FIL-63-2018, [“Cybersecurity Preparedness Resource”](#) (October 19, 2018)
- FIL-16-2018, [“FFIEC Issues Joint Statement: Cyber Insurance and Its Potential Role in Risk Management Programs”](#) (April 10, 2018)
- FIL-68-2016, [“FFIEC Cybersecurity Assessment Tool: Frequently Asked Questions”](#) (October 18, 2016)
- FIL-43-2016, [“Information Technology Risk Examination \(InTREx\) Program”](#) (June 30, 2016)
- FIL-37-2016, [“FFIEC Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks”](#) (June 7, 2016)
- FIL-55-2015, [“Cybersecurity Awareness Resources”](#) (November 23, 2015)
- FIL-28-2015, [“Cybersecurity Assessment Tool”](#) (July 2, 2015)
- FIL-13-2015, [“FFIEC Joint Statements on Destructive Malware and Compromised Credentials”](#) (March 30, 2015)
- FIL-49-2014, [“Technology Alert: GNU Bourne-Again Shell \(Bash\) Vulnerability”](#) (September 29, 2014)
- FIL-16-2014, [“Technology Alert: OpenSSL “Heartbleed” Vulnerability”](#) (April 11, 2014)
- FIL-13-2014, [“Technology Outsourcing: Informational Tools for Community Bankers”](#) (April 7, 2014)
- FIL-11-2014, [“Distributed Denial of Service \(DDoS\) Attacks”](#) (April 2, 2014)
- FIL-44-2008, [“Third-Party Risk: Guidance for Managing Third-Party Risk”](#) (June 6, 2008)
- FIL-77-2006, [“Authentication in an Internet Banking Environment: Frequently Asked Questions”](#) (August 21, 2006)
- FIL-103-2005, [“FFIEC Guidance: Authentication in an Internet Banking Environment”](#) (October 12, 2005)
- FIL-84-2002, [“Financial and Banking Information Infrastructure Committee’s Interim Policy on the Sponsorship of Private Sector Financial Institutions in the GETS Card Program”](#) (August 6, 2002)
- FIL-50-2001, [“Bank Technology Bulletin on Outsourcing”](#) (June 4, 2001)

Federal Reserve

Regulations

- Regulation H, 12 CFR 208, appendix D-1, [“Interagency Guidelines Establishing Standards for Safety and Soundness”](#)
- Regulation H, 12 CFR 208, appendix D-2, [“Interagency Guidelines Establishing Information Security Standards”](#)
- Regulation H, 12 CFR 208.61, [“Bank security procedures”](#)
- Regulation K, 12 CFR 211.5 and 211.24 (i), [“Protection of Customer and Consumer Information”](#)
- Regulation Y, 12 CFR 225, Appendix F, [“Interagency Guidelines Establishing Information Security Standards”](#)

Guidance

- SR Letter 20-24, “[Interagency Paper on Sound Practices to Strengthen Operational Resilience](#)” (November 2, 2020)
- SR Letter 20-6, “[Identification of Essential Critical Infrastructure Workers in the Financial Services Sector During the COVID-19 Response](#)” (March 27, 2020)
- SR Letter 20-3/CA Letter 20-2, “[Interagency Statement on Pandemic Planning](#)” (March 10, 2020)
- SR Letter 16-11, “[Supervisory Guidance for Assessing Risk Management at Supervised Institutions With Total Consolidated Assets Less than \\$50 Billion](#)” (June 8, 2016)
- SR Letter 15-9, “[FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors](#)” (July 2, 2015)
- SR Letter 13-19/CA Letter 13-21, “[Guidance on Managing Outsourcing Risk](#)” (December 5, 2013)
- SR Letter 13-16, “[End of Microsoft Support for Windows XP Operating System](#)” (October 7, 2013)
- SR Letter 12-17 / CA 12-14, “[Consolidated Supervision Framework for Large Financial Institutions](#)” (December 17, 2012)
- SR Letter 11-9, “[Interagency Supplement to Authentication in an Internet Banking Environment](#)” (June 29, 2011)
- SR Letter 06-13, “[Questions and Answers Related to Interagency Guidance on Authentication in an Internet Banking Environment](#)” (August 16, 2006)
- SR Letter 05-19, “[Interagency Guidance on Authentication in an Internet Banking Environment](#)” (October 13, 2005)
- SR Letter 05-23/ CA 05-10, “[Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#)” (December 1, 2005)
- SR Letter 04-17, “[FFIEC Guidance on the Use of Free and Open Source Software](#)” (December 6, 2004)
- SR Letter 01-15, “[Standards for Safeguarding Customer Information](#)” (May 31, 2001)
- SR Letter 00-17, “[Guidance on the Risk Management of Outsourced Technology Services](#)” (November 30, 2000)
- SR Letter 99-8, “[Uniform Rating System for Information Technology](#)” (March 31, 1999)
- SR Letter 98-9, “[Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations](#)” (April 20, 1998)
- SR Letter 96-14, “[Risk-focused Safety and Soundness Examinations and Inspections](#)” (May 24, 1996)

National Credit Union Administration

Regulations

- 12 CFR 748, “[Security Program, Report of Suspected Crimes, Suspicious Transactions, Catastrophic Acts and Bank Secrecy Act Compliance](#)”
- 12 CFR 748, appendix A, “[Guidelines for Safeguarding Member Information](#)”

- 12 CFR 749, “[Guidelines for Safeguarding Member Information, Records Preservation Program and Appendices—Record Retention Guidelines; Catastrophic Act Preparedness Guidelines](#)”
- 12 CFR 749, appendix A, “[Record Preservation Program and Record Retention](#)”

Guidance

- NCUA Letter to Credit Unions 20-CU-03, “[Identification of Essential Critical Infrastructure Workers During COVID-19](#)” (March 2020)
- NCUA Letter to Credit Unions 20-CU-02, “[NCUA Actions Related to COVID-19](#)” (March 2020)
- NCUA Letter to Credit Unions 11-CU-09, “[Online Member Authentication Guidance Compliance by January 2012](#)” (June 2011)
- NCUA Letter to Credit Unions 07-CU-13, “[Evaluating Third-Party Relationships](#)” (December 2007)
- NCUA Letter to Credit Unions 06-CU-10, “[NCUAs Information System and Technology IST Program](#)” (June 2006)
- NCUA Letter to Credit Unions 06-CU-07, “[IT Security Compliance Guide for Credit Unions](#)” (April 2006)
- NCUA Letter to Credit Unions 06-CU-06, “[Influenza Pandemic Preparedness](#)” (March 2006)
- NCUA Letter to Credit Unions 05-CU-18, “[Guidance on Authentication in Internet Banking Environment](#)” (November 2005)
- NCUA Letter to Credit Unions 04-CU-14, “[Risk Management of Free and Open Source Software](#)” (November 2004)
- NCUA Letter to Credit Unions 03-CU-03, “[Wireless Technology](#)” (February 2003)
- NCUA Letter to Credit Unions 01-CU-20, “[Due Diligence Over Third-Party Service Providers](#)” (November 2001)
- NCUA Letter to Credit Unions 00-CU-11, “[Risk Management of Outsourced Technology Services](#)” (December 2000)

Risk Alerts

- NCUA Letter to Credit Unions 09-RISK-01, “[Information Systems & Technology](#)” (August 2009)
- NCUA Letter to Credit Unions 06-RISK-01, “[Disaster Planning and Response](#)” (April 2006)

Office of the Comptroller of the Currency

Regulations

- 12 CFR 5.30, “[Establishment, Acquisition, and Relocation of a Branch of a National Bank](#)”
- 12 CFR 5.31, “[Establishment, Acquisition, and Relocation of a Branch and Establishment of an Agency Office of a Federal Savings Association](#)”
- 12 CFR 30, appendix A, “[Interagency Guidelines Establishing Standards for Safety and Soundness](#)”

- 12 CFR 30, appendix B, “[Interagency Guidelines Establishing Information Security Standards](#)”
- 12 CFR 30, appendix D, “[OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches](#)”
- 12 CFR 30, appendix E, “[OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches](#)”
- 12 CFR 41.83, “[Proper Disposal of Records Containing Consumer Information](#)”

Guidance

- OCC Bulletin 2020-144, “[Sound Practices to Strengthen Operational Resilience](#)” (November 2, 2020)
- OCC Bulletin 2020-23, “[Pandemic Planning: Essential Critical Infrastructure Workers in the Financial Services Sector](#)” (March 25, 2020)
- OCC Bulletin 2020-13, “[Pandemic Planning: Updated FFIEC Guidance](#)” (March 6, 2020)
- OCC Bulletin 2020-10, “Third-Party Relationships: [Frequently Asked Questions to Supplement OCC Bulletin 2013-29](#)” (March 5, 2020)
- OCC Bulletin 2019-13, “[Recovery Planning](#)” (March 15, 2019)
- OCC Bulletin 2018-8, “[FFIEC Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs](#)” (April 11, 2018)
- OCC Bulletin 2017-7, “[Third-Party Relationships: Supplemental Examination Procedures](#)” (January 24, 2017)
- OCC Bulletin 2016-34, “[Cybersecurity: Frequently Asked Questions on the FFIEC Cybersecurity Assessment Tool](#)” (October 17, 2016)
- OCC Bulletin 2016-18, “[FFIEC Statement: Cybersecurity of Interbank Messaging and Wholesale Payment Networks](#)” (June 7, 2016)
- OCC Bulletin 2015-40, “Cybersecurity: [Joint Statement on Cyber Attacks Involving Extortion](#)” (November 3, 2015)
- OCC Bulletin 2015-31, “[Cybersecurity: FFIEC Cybersecurity Assessment Tool](#)” (June 30, 2015)
- OCC Bulletin 2015-20, “[Cybersecurity: Destructive Malware Joint Statement](#)” (March 30, 2015)
- OCC Bulletin 2015-19, “[Cybersecurity: Cyber Attacks Compromising Credentials Joint Statement](#)” (March 30, 2015)
- OCC Bulletin 2014-48, “[FFIEC Alert: Bourne-Again Shell \(Bash\) “Shellshock” Vulnerability](#)” (September 26, 2014)
- OCC Bulletin 2014-17, “[Joint Statement: Information Security Vulnerability in OpenSSL Encryption Tool \(Heartbleed\)](#)” (April 25, 2014)
- OCC Bulletin 2013-29, “[Third-Party Relationships: Risk Management Guidance](#)” October 17, 2016
- OCC Bulletin 2011-26, “[Authentication in an Internet Banking Environment: Supplement](#)” (June 28, 2011)
- OCC Bulletin 2008-16, “[Information Security: Application Security](#)” (May 8, 2008)

- OCC Bulletin 2006-35, “[Authentication in an Internet Banking Environment: Frequently Asked Questions](#)” (August 15, 2006)
- OCC Bulletin 2005-35, “[Interagency Guidance: Authentication in an Internet Banking Environment](#)” (October 12, 2005)
- OCC Bulletin 2004-47, “[FFIEC Guidance: Risk Management for the Use of Free and Open Source Software](#)” (October 27, 2004)
- OCC Bulletin 2003-14, “[Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System](#)” (April 8, 2003)
- OCC Bulletin 2003-13, “[Telecommunications Service Priority \(TSP\) Program: FBIIC Policy on Sponsorship of TSP for Private Sector Entities](#)” (March 27, 2003)
- OCC Bulletin 2002-33, “[Government Emergency Telecommunications Service \(GETS\): FBIIC Policy on Sponsorship of GETS Cards for Private Sector Entities](#)” (July 23, 2002)
- OCC Bulletin 2002-16, “[Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance](#)” (May 15, 2002)
- OCC Bulletin 1998-3, “[Technology Risk Management: Guidance for Bankers and Examiners](#)” (February 4, 1998)

Other References

- American Institute of Certified Public Accountants (AICPA), [SOC 2 Examinations and SOC for Cybersecurity Examinations: Understanding the Key Distinctions](#) (2017)
- Center for Internet Security (CIS), [Control 3: Continuous Vulnerability Management](#) (March 2017)
- Financial Services Information Sharing and Analysis Center, [FS-ISAC](#)
- International Organization for Standardization / International Electrotechnical Commission, [ISO/IEC 27002:2013, Information Security Management Section 11: Physical and Environmental Security](#) (October 2013)
- Internet Engineering Task Force (IETF), [RFC 7591 OAuth 2.0 Dynamic Client Registration Protocol](#) (July 2015)
- Martzloff, François, [A New IEC Standard on the Measurement of Power Quality Parameters](#) (2000)

National Institute of Standards and Technology (NIST) Resources:

- [National Checklist Program](#)
- [NIST Glossary](#)
- [SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations](#) (September 2020)
- [ITL Bulletin, Security Considerations for Exchanging Files Over the Internet](#) (August 2020)
- [SP 800-207, Zero Trust Architecture](#) (August 2020)
- [SP 800-210, General Access Control Guidance for Cloud Systems](#) (July 2020)

- [SP 800-204A, Building Secure Microservices-based Applications Using Service-Mesh Architecture](#) (May 2020)
- [ITL Bulletin, Security for Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Solutions](#) (March 2020)
- [SP 800-160 Volume 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach](#) (November 2019)
- [NIST Big Data Interoperability Framework: Volume 1, Definitions](#) (October 2019)
- [SP 800-204, Security Strategies for Microservices-based Application Systems](#) (August 2019)
- [IR 8228, Considerations for Managing Internet of Things \(IoT\) Cybersecurity and Privacy Risks](#) (June 2019)
- [S 6106.01, Open Source Code](#) (December 2018)
- [SP 1800-5, IT Asset Management](#) (September 2018)
- [SP 500-316, Framework for Cloud Usability](#) (December 2015)
- [SP 800-146, Cloud Computing Synopsis and Recommendations](#) (May 2012)
- [SP 500-292, NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology](#) (September 2011)
- [SP 800-145, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology](#) (September 2011)
- [SP 800-125, Guide to Security for Full Virtualization Technologies](#) (January 2011)
- [SP 800-28, Guidelines on Active Content and Mobile Code](#) (March 2008)
- [NCSTAR 1-4B, Fire Suppression Systems](#) (September 2005)
- [SP 800-58, Security Considerations for Voice Over IP Systems](#) (January 2005)
- Open Web Application Security Project (OWASP) Foundation, [OWASP API Security Project](#) (2019)
- U.S. Department of Defense (DoD), [Summary of the 2018 Department Of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity](#) (2019)
- U.S. Department of the Treasury, [Data Governance Board Charter](#) (January 2020)



Federal Financial Institutions Examination Council

FFIEC

Audit **AUD**

April 2012

IT EXAMINATION

HANDBOOK

Table of Contents

Introduction	1
IT Audit Roles and Responsibilities	2
Board of Directors and Senior Management	2
Audit Management	4
Internal IT Audit Staff	4
Operating Management	5
External Auditors	5
Independence and Staffing of Internal IT Audit	6
Independence	6
Staffing	7
Internal Audit Program	7
Risk Assessment and Risk-Based Auditing	10
Program Elements	10
Risk Scoring System	11
Audit Participation in Application Development, Acquisition, Conversions, and Testing	13
Outsourcing Internal IT Audit	14
Independence of the External Auditor Providing Internal Audit Services	15
Examples of Arrangements	15
Third-Party Reviews of Technology Service Providers	17
Appendix A: Examination Procedures	A-1
Appendix B: Glossary	B-1
Appendix C: Laws, Regulations, and Guidance	C-1

Introduction

This "Audit Booklet" is one of several booklets that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) and provides guidance to examiners and financial institutions on the characteristics of an effective information technology (IT) audit function. [1] This booklet replaces and rescinds Chapter 8 of the 1996 FFIEC Information Systems Examination Handbook. It should be used by examiners of the FFIEC member agencies [2] as a foundation from which they can assess the quality and effectiveness of an institution's IT audit program. It describes the roles and responsibilities of the board of directors, management, and internal or external auditors; identifies effective practices for IT audit programs; and details examination objectives and procedures. Agency examiners will use the examination procedures in Appendix A to assess the adequacy of IT audit programs at both financial institutions and technology service providers. The examination guidance and procedures in this booklet focus on IT audit and supplement other, more general, internal and external audit guidance provided by the FFIEC agencies. [3]

A well-planned, properly structured audit program is essential to evaluate risk management practices, internal control systems, and compliance with corporate policies concerning IT-related risks at institutions of every size and complexity. Effective audit programs are risk-focused, promote sound IT controls, ensure the timely resolution of audit deficiencies, and inform the board of directors of the effectiveness of risk management practices. An effective IT audit function may also reduce the time examiners spend reviewing areas of the institution during examinations. Ideally, the audit program would consist of a full-time, continuous program of internal audit coupled with a well-planned external auditing program.

The financial industry must plan, manage, and monitor rapidly changing technologies to enable it to deliver and support new products, services, and delivery channels. The rate of these changes and the resulting increased reliance on technology make the inclusion of IT audit coverage essential to an effective over all audit program. The audit program should address IT risk exposures throughout the institution, including the areas of IT management and strategic planning, data center operations, client/server architecture, local and wide-area networks, telecommunications, physical and information security, electronic banking, systems development, and business continuity planning. IT audit should also focus on how management determines the risk exposure from its operations and controls or mitigates that risk.

To determine what risks exist, management should prepare an independent assessment of the institution's risk exposure and the quality of the internal controls associated with the development, acquisition, implementation, and use of information technology. An institution's IT audit function can provide this independent assessment within the context of the overall audit function and can include work performed by both internal and external auditors and by other independent third parties as appropriate for the institution's complexity and level of internal expertise. The FFIEC member agencies believe that a strong internal auditing function combined with a well-planned external auditing function substantially increase the probability that an institution will detect potentially serious technology-related problems. An effective IT audit program should:

- Identify areas of greatest IT risk exposure to the institution in order to focus audit resources;
- Promote the confidentiality, integrity, and availability of information systems;
- Determine the effectiveness of management's planning and oversight of IT activities;
- Evaluate the adequacy of operating processes and internal controls;
- Determine the adequacy of enterprise-wide compliance efforts related to IT policies and internal control procedures; and
- Require appropriate corrective action to address deficient internal controls and follow up to ensure management promptly and effectively implements the required actions.

The examiner is responsible for evaluating the effectiveness of the IT audit function in meeting these objectives. The examiner should also consider the institution's ability to promptly detect and report significant risks to the board of directors and senior management. Examiners should take into account the institution's size, complexity, and overall risk profile when performing this and other evaluations. Examiners should consider the following issues when evaluating the IT audit function:

- Independence of the audit function and its reporting relationship to the board of directors or its audit committee;
- Expertise and size of the audit staff relative to the IT environment;
- Identification of the IT audit universe, risk assessment, scope, and frequency of IT audits;
- Processes in place to ensure timely tracking and resolution of reported weaknesses; and
- Documentation of IT audits, including work papers, audit reports, and follow-up.

IT Audit Roles and Responsibilities

Board of Directors and Senior Management

The board of directors and senior management are responsible for ensuring that the institution's system of internal controls operates effectively. One important element of an effective internal control system is an internal audit function that includes adequate IT coverage.

To meet its responsibility of providing an independent audit function with sufficient resources to ensure adequate IT coverage, the board of directors or its audit committee should:

- Provide an internal audit function capable of evaluating IT controls,
- Engage outside consultants or auditors to perform the internal audit function, or
- Use a combination of both methods to ensure that the institution has received adequate IT audit coverage.

An institution's board of directors may establish an "audit committee" to oversee audit functions and to report on audit matters periodically to the full board of directors. For purposes of this booklet, the term "audit committee" means the committee with audit oversight regardless of the type of financial institution. ^[4] Audit committee members should have a clear understanding of the importance and necessity of an independent audit function.

To comply with the Sarbanes-Oxley Act of 2002, ^[5] public stock-issuing institutions are required to appoint outside directors as audit committee members. All members of a stock-issuing institution's audit committee must be members of the board of directors and be independent (i.e., not otherwise compensated by, or affiliated with, the institution). Additionally, 12 CFR 363 (Federal Deposit Insurance Corporation Improvement Act, or FDICIA) requires all depository institutions with total assets greater than \$500 million to have independent audit committees. Although not all institutions are subject to these requirements due to their corporate structure (Sarbanes-Oxley) or their size (FDICIA), it is generally considered good practice that they use them as guidelines to ensure the independence of their audit committees.

The board of directors should ensure that written guidelines for conducting IT audits have been adopted. The board of directors or its audit committee should assign responsibility for the internal audit function to a member of management (hereafter referred to as the "internal audit manager") who has sufficient audit expertise and is independent of the operations of the business.

The board should give careful thought to the placement of the audit function in relation to the institution's management structure. The board should have confidence that the internal audit staff members will perform their duties with impartiality and not be unduly influenced by senior management and managers of day-to-day operations. Accordingly, the internal audit manager should report directly to the board of directors or its audit committee.

The board or its audit committee is responsible for reviewing and approving audit strategies (including policies and programs), and monitoring the effectiveness of the audit function. The board or its audit committee should be aware of, and understand, significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, information systems, and electronic banking. Control issues and risks associated with reliance on technology can include:

- Inappropriate user access to information systems,
- Unauthorized disclosure of confidential information,
- Unreliable or costly implementation of IT solutions,

- Inadequate alignment between IT systems and business objectives,
- Inadequate systems for monitoring information processing and transactions,
- Ineffective training programs for employees and system users,
- Insufficient due diligence in IT vendor selection,
- Inadequate segregation of duties,
- Incomplete or inadequate audit trails,
- Lack of standards and controls for end-user systems,
- Ineffective or inadequate business continuity plans, and
- Financial losses related to systems outages.

The board or its audit committee members should seek training to fill any gaps in their knowledge related to IT risks and controls. The board of directors or its audit committee should periodically meet with both internal and external auditors to discuss audit work performed and conclusions reached on IT systems and controls.

Audit Management

The internal audit manager is responsible for implementing board-approved audit directives. The manager oversees the audit function and provides leadership and direction in communicating and monitoring audit policies, practices, programs, and processes. The internal audit manager should establish clear lines of authority and reporting responsibility for all levels of audit personnel and activities. The internal audit manager also should ensure that members of the audit staff possess the necessary independence, experience, education, training, and skills to properly conduct assigned activities.

The internal audit manager should be responsible for internal control risk assessments, audit plans, audit programs, and audit reports associated with IT. Audit management should oversee the staff assigned to perform the internal audit work, should establish policies and procedures to guide the audit staff, and should ensure the staff has the expertise and resources to identify inherent risks and assess the effectiveness of internal controls in the institution's IT operations.

Internal IT Audit Staff

The primary role of the internal IT audit staff is to assess independently and objectively the controls, reliability, and integrity of the institution's IT environment. These assessments can help maintain or improve the efficiency and effectiveness of the institution's IT risk management, internal controls, and corporate governance.

Internal auditors should evaluate IT plans, strategies, policies, and procedures to ensure

adequate management oversight. Additionally, they should assess the day-to-day IT controls to ensure that transactions are recorded and processed in compliance with acceptable accounting methods and standards and are in compliance with policies set forth by the board of directors and senior management. Auditors also perform operational audits, including system development audits, to ensure that internal controls are in place, that policies and procedures are effective, and that employees operate in compliance with approved policies. Auditors should identify weaknesses, review management's plans for addressing those weaknesses, monitor their resolution, and report to the board as necessary on material weaknesses.

Auditors should make recommendations to management about procedures that affect IT controls. In this regard, the board and management should involve the audit department in the development process for major new IT applications. The board and management should develop criteria for determining those projects that need audit involvement. Audit's role generally entails reviewing the control aspects of new applications, products, conversions, or services throughout their development and implementation. Early IT audit involvement can help ensure that proper controls are in place from inception. However, the auditors should be careful not to compromise, or even appear to compromise, their independence when involved in these projects.

Operating Management

Operating management should formally and effectively respond to IT audit or examination findings and recommendations. The audit procedures should clearly identify the methods for following up on noted audit or control exceptions or weaknesses. Operating management is responsible for correcting the root causes of the audit or control exceptions, not just treating the exceptions themselves. Response times for correcting noted deficiencies should be reasonable and may vary depending on the complexity of the corrective action and the risk of inaction. Auditors should document, report, and track recommendations and outstanding deficiencies. Additionally, auditors should conduct timely follow-up audits to verify the effectiveness of management's corrective actions for significant deficiencies.

External Auditors

External auditors typically review IT control procedures as part of their overall evaluation of internal controls when providing an opinion on the adequacy of an institution's financial statements. As a rule, external auditors review the general and application controls affecting the recording and safeguarding of assets and the integrity of controls over financial statement preparation and reporting. General controls include the plan of organization and operation, documentation procedures, access to equipment and data files, and other controls affecting overall information systems operations. Application controls relate to specific information systems tasks and provide reasonable assurance that the recording, processing, and reporting of data are properly performed.

External auditors may also review the IT control procedures as part of an outsourcing arrangement in which they are engaged to perform all or part of the duties of the internal audit staff. Such arrangements are discussed in more detail in the "Outsourcing Internal IT Audit" section of this booklet.

The extent of external audit work, including work related to information systems, should be clearly defined in an engagement letter. Such letters should discuss the scope of the audit, the objectives, resource requirements, audit timeframe, and resulting reports. Examiners will typically review the engagement letter, reports, and audit work papers to determine the extent to which they can rely on external audit coverage and reduce their examination scope accordingly.

Independence and Staffing of Internal IT Audit

Independence

The ability of the internal audit function to achieve desired objectives depends largely on the independence of audit personnel. Generally, the position of the auditor within the organizational structure of the institution, the reporting authority for audit results, and the auditor's responsibilities indicate the degree of auditor independence. The board should ensure that the audit department does not participate in activities that may compromise, or appear to compromise, its independence. These activities may include preparing reports or records, developing procedures, or performing other operational duties normally reviewed by auditors.

The auditor's independence is also determined by analyzing the reporting process and verifying that management does not interfere with the candor of the findings and recommendations. For an effective program, the board should give the auditor the authority to:

- Access all records and staff necessary to conduct the audit, and
- Require management to respond formally, and in a timely manner, to significant adverse audit findings by taking appropriate corrective action.

Internal auditors should discuss their findings and recommendations periodically with the audit committee or board of directors.

Ideally, the internal audit manager should report directly to the board of directors or its audit committee regarding both audit issues and administrative matters.^[6] Alternatively, an institution may establish a dual reporting relationship where the internal audit manager reports to the audit committee or board for audit matters and to institution executive management for administrative matters. The objectivity and organizational stature of the internal audit function are best served under such a dual arrangement if the internal audit manager reports administratively to the chief executive office (CEO), and not to the chief financial officer (CFO) or a similar officer who has a direct responsibility for systems being audited. The board or its audit committee should determine the internal audit manager's performance evaluations and compensation.

The formality and extent of an institution's internal IT audit function depends on the institution's size, complexity, scope of activities, and risk profile. It is the responsibility of the audit committee and management to carefully consider the extent of auditing that will

effectively monitor the internal control system subject to consideration of the internal audit function's costs and benefits. For larger institutions or institutions with complex operations, the benefits derived from a full time manager of internal audit or an audit staff will likely outweigh the cost. For small institutions with few employees and/or simple operations, these costs may outweigh the benefits. Nevertheless, an institution without an internal auditor can ensure that it maintains an objective and independent internal function by implementing comprehensive internal reviews of significant internal controls. The key characteristic of such reviews is that the person(s) directing or performing the review is (are) not also responsible for managing or operating those controls.

Staffing

Personnel performing IT audits should have information systems knowledge commensurate with the scope and sophistication of the institution's IT environment and possess sufficient analytical skills to determine and report the root cause of deficiencies. If internal expertise is inadequate, the board should consider using qualified external sources such as management consultants, independent auditors, or other professionals to supplement or perform the institution's internal IT audit function. In some institutions, a person or group that has no other responsibilities outside the IT audit function performs IT audits. Generally, institutions using this approach centralize IT audit coverage and assign one or more IT audit specialists to perform end-user application control reviews as well as technical system audits. A centralized IT audit department can ensure sufficient technical expertise, but can also strain technical resources and require multiple audits in a user department. Additionally, IT auditors in this environment may need to have a greater understanding of financial and business line audit concerns.

Other institutions may use an integrated audit approach. Using this method, IT audit specialists perform the technology system and other technical reviews, while generalist auditors perform the end-user application control reviews. Institutions should use auditors with technical knowledge appropriate for the areas reviewed.

An institution's hiring and training practices should ensure that the institution has qualified IT auditors. The auditor's education and experience should be consistent with job responsibilities. Audit management should also provide an effective program of continuing education and development. As the information systems of an institution become more sophisticated or as more complex technologies evolve, the auditor may need additional training.

Internal Audit Program

Action Summary

Management should develop and follow a formal internal audit program consisting of policies and procedures that govern the internal audit function, including IT audit.

An institution's internal audit program consists of the policies and procedures that govern its internal audit functions, including risk-based auditing programs and outsourced internal audit work, if applicable. While smaller institutions' audit programs may not require the formality of those found in larger, more complex institutions, all audit programs should include

- A mission statement or audit charter outlining the purpose, objectives, organization, authorities, and responsibilities of the internal auditor, audit staff, audit management, and the audit committee.
- A risk assessment process to describe and analyze the risks inherent in a given line of business. Auditors should update the risk assessment at least annually, or more frequently if necessary, to reflect changes to internal control or work processes, and to incorporate new lines of business. The level of risk should be one of the most significant factors considered when determining the frequency of audits.
- An audit plan detailing internal audit's budgeting and planning processes. The plan should describe audit goals, schedules, staffing needs, and reporting. The audit plan should cover at least 12 months and should be defined by combining the results of the risk assessment and the resources required to yield the timing and frequency of planned internal audits. The audit committee should formally approve the audit plan annually, or review it annually in the case of multi-year audit plans. The internal auditors should report the status of planned versus actual audits, and any changes to the annual audit plan, to the audit committee for its approval on a periodic basis.
- An audit cycle that identifies the frequency of audits. Auditors usually determine the frequency by performing a risk assessment, as noted above, of areas to be audited. While staff and time availability may influence the audit cycle, they should not be overriding factors in reducing the frequency of audits for high-risk areas.
- Audit work programs that set out for each audit area the required scope and resources, including the selection of audit procedures, the extent of testing, and the basis for conclusions. Well-planned, properly structured audit programs are essential to strong risk management and to the development of comprehensive internal control systems.
- Written audit reports informing the board and management of individual department or division compliance with policies and procedures. These reports should state whether operating processes and internal controls are effective, and describe deficiencies as well as suggested corrective actions. The audit manager should consider implementing an audit rating system (for example, satisfactory, needs improvement, unsatisfactory) approved by the audit committee. The rating system facilitates conveying to the board a consistent and concise assessment of the net risk posed by the area or function audited. All written audit reports should reflect the assigned rating for the areas audited.
- Requirements for audit work paper documentation to ensure clear support for all audit findings and work performed, including work paper retention policies.
- Follow-up processes that require internal auditors to determine the disposition of any agreed-upon actions to correct significant deficiencies.

- Professional development programs to be in place for the institution's audit staff to maintain the necessary technical expertise.

All institutions are encouraged to implement risk-based IT audit procedures based on a formal risk assessment methodology to determine the appropriate frequency and extent of work. See the "Risk Assessment and Risk-Based Auditing" section of this booklet for more detail.

IT audit procedures will vary depending upon the philosophy and technical expertise of the audit department and the sophistication of the data center and end-user systems. However, to achieve effective coverage, the audit program and expertise of the staff must be consistent with the complexity of data processing activities reviewed. The audit procedures may include manual testing processes or computer-assisted audit programs (discussed later in this section).

The audit department should establish standards for audit work papers, related communications, and retention policies. Auditors should ensure that work papers are well organized, clearly written, and address all areas in the scope of the audit. They should contain sufficient evidence of the tasks performed and support the conclusions reached. Formal procedures should exist to ensure that management and the audit committee receive summarized audit findings that effectively communicate the results of the audit. Full audit reports should be available for review by the audit committee. Policies should establish appropriate work paper retention periods. Institutions should consider conducting their internal audit activities in accordance with professional standards, such as the Standards for the Professional Practice of Internal Auditing issued by the Institute for Internal Auditors (IIA), and those issued by the Standards Board of the Information Systems Audit and Control Association (ISACA). These standards address independence, professional proficiency, scope of work, performance of audit work, management of internal audit, and quality assurance reviews.

IT auditors frequently use computer-assisted audit techniques (CAATs) to improve audit coverage by reducing the cost of testing and sampling procedures that otherwise would be performed manually. CAATs include many types of tools and techniques, such as generalized audit software, utility software, test data, application software tracing and mapping, and audit expert systems. CAATs may be:

- Developed by internal programming staff or by outside programmers with audit department supervision;
- Purchased generalized audit software, e.g., audit packages offered by CPA firms or software vendors;
- Developed by IT auditors; or
- Acquired from equipment manufacturers and software houses to analyze machine, programmer, and operations efficiency.

Whatever the source, audit software programs should remain under the strict control of the audit department. For this reason, all documentation, test material, source listings,

source and object program modules, and all changes to such programs, should be strictly controlled. In installations using advanced software library control systems, audit object programs may be catalogued with password protection. This is acceptable if the auditors retain control over the documentation and the appropriate job control instructions necessary to retrieve and execute the object program from the libraries where it is stored. If internal control procedures within the computer system do not allow for strict audit control, audit programs should not be catalogued. Computer programs intended for audit use should be documented carefully to define their purpose and to ensure their continued usefulness and reliability.

CAATs may be used in performing various audit procedures, including the following:

- Tests of transactions and balances, such as recalculating interest;
- Analytical review procedures, such as identifying inconsistencies or significant fluctuations;
- Compliance tests of general controls, such as testing the set-up or configuration of the operating system or access procedures to the program libraries;
- Sampling programs to extract data for audit testing;
- Compliance tests of application controls such as testing the functioning of a programmed control;
- Recalculating entries performed by the entity's accounting systems; and
- Penetration testing.

These tools and techniques can also be used effectively to check data integrity by testing the logical processing of data "through" the system, rather than by relying only on validations of input and output controls.

Risk Assessment and Risk-Based Auditing

Action Summary

The board of directors should establish an effective risk-based audit function.

An effective risk-based auditing program will cover all of an institution's major activities. The frequency and depth of each area's audit will vary according to the risk assessment of that area. Examiners should determine whether the audit function is appropriate for the size and complexity of the institution.

Program Elements

Properly designed risk-based audit programs increase audit efficiency and effectiveness. The sophistication and formality of risk-based audits may vary depending on the institution's size and complexity. To determine the appropriate level of audit coverage for the organization's IT environment, management should define an effective risk assessment methodology. This assessment methodology should provide the auditor and the board with objective information to prioritize the allocation of audit resources properly. Risk-based IT audit programs should:

- Identify the institution's data, application and operating systems, technology, facilities, and personnel;
- Identify the business activities and processes within each of those categories;
- Include profiles of significant business units, departments, and product lines, or systems, and their associated business risks and control features, resulting in a document describing the structure of risk and controls throughout the institution;
- Use a measurement or scoring system that ranks and evaluates business and control risks for significant business units, departments, and products;
- Include board or audit committee approval of risk assessments and annual risk-based audit plans that establish audit schedules, audit cycles, work program scope, and resource allocation for each area audited;
- Implement the audit plan through planning, execution, reporting, and follow-up; and
- Include a process that regularly monitors the risk assessment and updates it at least annually for all significant business units, departments, and products or systems.

Risk Scoring System

A successful risk-based IT audit program can be based on an effective scoring system. ^[7] In establishing a scoring system, the board of directors and management should ensure the system is understandable, considers all relevant risk factors, and, to the extent possible, avoids subjectivity. Major risk factors commonly used in scoring systems include the following:

- The adequacy of internal controls;
- The nature of transactions (for example, the number and dollar volumes and the complexity);
- The age of the system or application;
- The nature of the operating environment (for example, changes in volume, degree of system and reporting centralization, sensitivity of resident or processed data, the

impact on critical business processes, potential financial impact, planned conversions, and economic and regulatory environment);

- The physical and logical security of information, equipment, and premises;
- The adequacy of operating management oversight and monitoring;
- Previous regulatory and audit results and management's responsiveness in addressing issues;
- Human resources, including the experience of management and staff, turnover, technical competence, management's succession plan, and the degree of delegation; and
- Senior management oversight.

Auditors should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the audit committee or the board of directors. The sophistication and formality of guidelines will vary for individual institutions depending on their size, complexity, scope of activities, geographic diversity, and various technologies used. The institution can rely on standard industry practice or on its own experiences to define risk scoring. Auditors should use the guidelines to grade or assess major risk areas and to define the range of scores or assessments (e.g., groupings such as low, medium, and high risk or a numerical sequence such as 1 through 5).

The written risk assessment guidelines should specify the following elements:

- A maximum length for audit cycles based on the risk scores. (For example, some institutions set audit cycles at 12 months or less for high-risk areas, 24 months or less for medium-risk areas, and up to 36 months for low-risk areas. Audit cycles should not be open-ended.);
- The timing of risk assessments for each department or activity. (Normally risks are assessed annually, but more frequent assessments may be needed if the institution experiences rapid growth or significant change in operation or activities.);
- Documentation requirements to support scoring decisions; and
- Guidelines for overriding risk assessments in special cases and the circumstances under which they can be overridden. (For example, the guidelines should define who can override assessments, and how the override is approved, reported and documented.)

Numerous industry groups offer resources where institutions can obtain matrices, models, or additional information on risk assessments. Among these groups are: ISACA, American Bankers Association (ABA), American Institute of Certified Public Accountants (AICPA), and IIA. Day-to-day management of the risk-based audit program rests with the internal audit manager, who monitors the audit scope and risk assessments to ensure that audit coverage remains adequate. The internal audit manager also prepares reports showing the risk rating, planned scope, and audit cycle for each area. The audit manager

should confirm the risk assessment system's reliability at least annually or whenever significant changes occur within a department or function. Operating department managers and auditors should work together in evaluating the risk in all departments and functions by reviewing risk assessments to determine their reasonableness.

Auditors should periodically review the results of internal control processes and analyze financial or operational data for any impact on a risk assessment or scoring. Accordingly, operating management should be required to keep auditors up to date on all major changes in departments or functions, such as the introduction of a new product, implementation of a new system, application conversions, or significant changes in organization or staff.

Audit Participation in Application Development, Acquisition, Conversions, and Testing

Action Summary

Senior management should involve IT audit in major application development, acquisition, conversion, and testing.

The development, acquisition, or conversion of an automated application is a lengthy and complex process requiring a significant degree of interaction among the programming staff, user departments, and internal audit. This process, known as the system development life cycle or system development methodology, requires detailed developmental stages to ensure that applications meet the needs of the institution. As each stage of the life cycle is reached, the auditor should review the internal controls, testing, and audit trails included in the application. The incorporation of internal controls within a completed application already in production is usually more difficult and expensive. Guidelines should be developed to facilitate the review of new applications during the design phase so that controls can be identified during independent audit review early in the development process.

The institution's audit policy, as approved by the board of directors, should include guidelines detailing what involvement internal audit will have in the development, acquisition, conversion, and testing of major applications. This includes describing the monitoring, reporting, and escalation processes (when internal controls are found to be insufficient or when testing is found to be inadequate). For acquisitions, this includes describing the phases of the system development life cycle in which IT audit will be involved. For acquisitions with significant IT impacts, participation of IT audit may be necessary early in the due diligence stage.

It is necessary that audit's participation in the development process be independent and objective. Auditors can determine and should recommend appropriate controls to project management. However, such recommendations do not necessarily "pre-approve" the controls, but instead guide the developers in considering appropriate control standards and structures throughout their project. The auditors are more than just "consultants" on internal controls. While they should not have any direct involvement in management decisions, they should raise objections if they believe the control environment to be

inadequate.

Once a new application system, conversion, or major revision to an existing system is accepted for production processing, the IT auditor should conduct a post-implementation review. This review should occur shortly after the implementation of the new or revised system and should include extensive testing of program logic, calculations, error conditions, edits, and controls. Such testing helps to validate that the software operates as expected. By performing the review soon after migration to the production environment, the auditors can quickly identify processing errors or other unsatisfactory conditions. A prompt post-implementation review should minimize potential losses from processing errors or ineffective software operation or controls.

In larger IT facilities, formal quality assurance or change management groups may have primary responsibility for post-implementation reviews. In such cases, the IT auditor may choose not to perform a separate review but instead to participate in establishing the test criteria and evaluating results of any other independent reviews.

Outsourcing Internal IT Audit

Action Summary

The board of directors of an institution that outsources its internal IT audit function should ensure that the structure, scope, and management of the outsourcing arrangement provides for an adequate evaluation of the system of internal controls.

In addressing quality and resource issues, many institutions engage independent public accounting firms and other outside professionals to perform work that has been traditionally carried out by internal auditors. These arrangements are often called "internal audit outsourcing," "internal audit assistance," "audit co-sourcing," or "extended audit services."

Outsourcing such audit services may be beneficial to an institution if it is properly structured, carefully conducted, and prudently managed. To do this, management should ensure that there are no conflicts of interest and that the use of these services does not compromise independence. Potential conflicts of interest may arise if the outsourced auditing firm performs IT audit functions in addition to other audit services, such as providing the independent financial statement, or serving in an IT or management consulting capacity. The board of directors of an institution remains responsible for ensuring that the outsourced internal audit function operates effectively and complies with all regulations governing such arrangements.

Examiners should assess whether the structure, scope, and management of an internal audit outsourcing arrangement adequately evaluate the institution's system of internal controls. They should also determine whether or not directors and senior managers have fulfilled their responsibilities for maintaining an effective system of internal controls and for overseeing the internal audit function in an outsourced internal audit environment.

Additional detailed guidance on the structure, independence, and sound practices

concerning the use of outsourcing audit providers is available in the "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing."

Independence of the External Auditor Providing Internal Audit Services

It is important that examiners ensure that management has designed any outsourcing arrangements in order to maintain the independence of the audit provider. An accounting firm hired to perform internal audit services for an institution risks compromising its independence when it also performs the external audit for the institution. Concerns arise because, rather than having an independent review, the responsibility of performing outsourced internal audits places the accounting firm in the position of auditing its own work. For example, in designing procedures to audit an institution's financial statements, the accounting firm considers the extent to which it may rely on the institution's internal control system, including the internal audit function.

The Sarbanes-Oxley Act of 2002 specifically prohibits a registered public accounting firm from performing certain non-audit services for a public company client for whom it performs financial statement audits. Among those prohibited non-audit services are internal audit outsourcing services and financial information system design and implementation. Under rules adopted by the Securities and Exchange Commission, this prohibition generally became effective on May 6, 2003, although a one-year transition period was provided for contractual arrangements in place as of that date. Under Section 36 of the Federal Deposit Insurance Act and its implementing regulation and guidelines, FDIC-insured depository institutions with total assets of \$500 million or more are required to be audited annually. The guidelines require these institutions, whether or not they are public companies, and their external auditors to comply with the SEC's auditor independence requirements. Other non-public institutions are encouraged to have their financial statements audited and to follow the Sarbanes-Oxley Act's prohibition on outsourcing internal audit to their external auditor. However, there are circumstances in which these institutions can use the same accounting firm for both external and internal audit work.

Examples of Arrangements

An outsourcing arrangement is a contract between the institution and an audit services firm to provide internal audit services. Outsourcing arrangements take many forms and are used by institutions of all sizes. The services under contract can be as limited as assisting internal audit staff with an assignment in which they lack expertise. This type of arrangement would typically fall under the control of the institution's internal audit manager, to whom the audit provider would typically report.

Other outsourcing arrangements may call for an audit provider to perform all or several parts of the internal audit work. Under these types of arrangements, the institution should maintain an internal audit manager and, as appropriate, internal audit staff sufficient to oversee vendor activities. The audit provider usually assists the internal audit function in determining the institution's areas of risk and the levels of risk to be reviewed, and recommends and performs audit procedures approved by the institution's internal audit manager. In addition, the outsourced audit provider should work jointly with the internal audit manager in reporting significant findings to the board or its audit committee.

Before entering into an outsourcing arrangement, the institution should perform due diligence to ensure that the audit provider has a sufficient number of qualified staff members to perform the contracted work. Because the outsourcing arrangement is a professional or personnel services contract, the institution's internal audit manager should have confidence in the competence of the staff assigned by the audit provider and receive timely notice from the vendor of any key staffing changes. Throughout the outsourcing arrangement, management should ensure that the audit provider maintains sufficient expertise to perform effectively and fulfill its contractual obligations.

When an institution enters into an outsourcing arrangement, or significantly changes the mix of internal and external resources used by internal audit, operational risk may increase. Because the arrangement could be terminated suddenly, the institution should have a contingency plan to mitigate any significant gap in audit coverage, particularly for high-risk areas. In its planning, an institution should consider possible alternatives and determine what it will do if an auditor with specialized knowledge or skills is unable to complete reviews of high risk areas, or if an outsourcing arrangement is terminated. For example, management could maintain information about the services offered and areas of expertise, as well as contact names and phone numbers, of other firms in their geographic area that could provide internal audit assistance in specific areas or a broader range of outsourcing services.

When negotiating the outsourcing arrangement with a vendor, an institution should carefully consider its current and anticipated business risks in setting each party's internal audit responsibilities. To clearly define the institution's duties and those of the outsourcing vendor, the institution should have a written contract, often referred to as an engagement letter.^[8] The contract should:

- Define the expectations and responsibilities for both parties;
- Set the scope, frequency, and cost of work to be performed by the vendor;
- Set responsibilities for providing and receiving information, such as the manner and frequency of reporting to senior management and the board about the status of contract work;
- Establish the protocol for changing the terms of the service contract, especially for expansion of audit work if significant issues are found, and stipulations for default and termination of the contract;
- State that any information pertaining to the institution must be kept confidential;
- Specify the locations of internal audit reports and the related work papers;
- Specify the period of time that vendors must maintain the work papers;^[9]
- State that outsourced internal audit services provided by the vendor are subject to regulatory review and that examiners will be granted full and timely access to the internal audit reports and related work papers prepared by the outsourcing vendor;^[10]
- State that internal audit reports are the property of the institution, that the institution will be provided with any copies of the related work papers it deems necessary, and that employees authorized by the institution will have reasonable and timely access

to the work papers prepared by the audit provider;

- Prescribe a process (arbitration, mediation, or other means) for resolving problems and for determining who bears the cost of consequential damages arising from errors, omissions, and negligence; and
- State that audit providers will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee or a member of management of the institution, and will comply with professional and regulatory independence guidance.

Directors and senior management should ensure that the outsourced internal audit function is competently managed. For example, larger institutions should employ sufficient competent staff members in the internal audit department to assist the internal audit manager in overseeing the outsourcing vendor. Smaller institutions that do not employ a full-time audit manager should appoint a competent institution employee to oversee the outsourcing vendor's performance under the contract. This person should report directly to the audit committee for purposes of communicating audit issues and ideally should have no managerial responsibility for the area being audited.

Communication among the internal audit function, the audit committee, and senior management should not diminish because the institution engages an outsourcing vendor. The institution's audit manager should be involved with the audit provider in defining the audit universe and setting a risk-based IT audit schedule. The audit provider should appropriately document all work and promptly report all control weaknesses found during the audit to the institution's internal audit manager.

The outsourcing vendor should work with the internal audit manager to mutually determine what audit findings are significant and should be emphasized when reported to the board and its audit committee. The concept of materiality as the term is used in financial statement audits is not necessarily a good indicator of which control weaknesses to report. For example, reportable weaknesses could affect the institution's compliance with laws and regulations without a direct impact on the financial statements.

Third-Party Reviews of Technology Service Providers

A technology service provider (TSP) that processes work for financial institutions often is subject to separate audits by internal auditors from each of the serviced institutions. These audits may duplicate each other, creating a hardship on the provider's management and resources. The TSP can reduce that burden by arranging for its own third-party audit to determine the status and reliability of internal controls and by sharing the results of that audit with its client financial institutions.

A third-party audit or review is performed by independent auditors who are not employees of either the TSP or the serviced institution(s). The TSP, its auditors, or its serviced institutions may engage the third-party auditor. The serviced institutions' auditors may use this third-party review to determine the scope of any additional audit coverage they require to evaluate the system and controls at the TSP. Examiners can

also use the third-party review to help scope their supervisory activities.

Financial institutions are required to effectively manage their relationships with key TSPs. Institution management meets this requirement related to audit controls by:

- Directly auditing the TSP's operations and controls
- Employing the services of external auditors to evaluate the TSP's operations and controls; or
- Receiving from, and reviewing sufficiently detailed independent audit reports on, the TSP.

Financial institutions using such audits to complement their own coverage should ensure that the independent auditor is qualified to perform the review, that the scope satisfies their own audit objectives, and that any significant deficiencies reported are corrected. It is critically important that the examiner and the institution understand the nature and scope of the engagement and the level of assurance accruing from the work product of the reviewing firm.

There are two common types of independent third-party reviews: attestation reviews and non-attestation reviews. Attestation reviews ^[11] are generally conducted by Certified Public Accountants (CPAs) and are based upon Attestation Standards issued by the American Institute of Certified Public Accounts (AICPA). Non-attestation reviews include those performed by IT consultants or others; they may be based upon external standards ^[12] or industry developed criteria. ^[13]

The type of independent third-party review chosen should be based upon the size and complexity of the servicer, the products and services it offers, and its risk profile because the level of assurance provided varies with each type of review.

Users of audit reports or reviews should not rely solely on the information contained in the report to verify the internal control environment of the TSP. They should use additional verification and monitoring procedures as discussed more fully in the Outsourcing Technology Services Booklet of the FFIEC IT Examination Handbook. Refer to that booklet for additional information on vendor management and to supplement the examination coverage in this booklet.

Endnotes

[1]	This booklet uses the terms "institution" and "financial institution" to describe insured banks, thrifts, and credit unions, as well as technology service providers that provide services to such entities.
[2]	Board of Governors of the Federal Reserve System (Federal Reserve Board), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS).
[3]	These include the "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing," March 17, 2003; "Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations," September 22, 1999; and "Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners," July 23, 1992.
[4]	A federal credit union board of directors is required to establish a "supervisory committee" with oversight responsibility for audit. A supervisory committee consists of not less than three members, nor more than five members, one of whom may be a director other than the compensated officer of the board.
[5]	Sarbanes-Oxley Act of 2002 (Public Law 107-204) puts into place significant new requirements that provide for auditor independence of registered companies that will apply, through FDIC guidelines, (1) to any financial institution that is required under banking laws to have an annual independent audit or (2) to its holding company if the bank satisfies this requirement at the holding company level. All insured depository institutions with \$500 million or more in total assets are required under banking laws to have an annual audit by an independent public accountant. If the institution is a subsidiary of a holding company, it can satisfy this requirement by an independent audit of the holding company. Further, the Federal Reserve Board may apply the auditor independence requirements in the Act to all bank holding companies that are required by the Federal Reserve Board to have an annual audit by an independent public accountant even if no subsidiary institution is subject to the requirements.
[6]	Administrative matters in this context include routine personnel matters such as leave and attendance reporting, expense account management, and other departmental matters such as furniture, equipment and supplies.
[7]	Scoring refers to any consistent means of quantifying and then comparing distinct items based on elements that they have in common. All risk-based systems require some means to rank greater or lesser risk, or risk factors. Consequently, many risk-based systems rely on some means of scoring in their implementation.
[8]	In general, the contract between the institution and the audit provider may or may not be the same as the engagement letter.
[9]	If work papers are in electronic format, contracts often call for the vendor to maintain the software that allows the institution and examiners access to electronic work papers during a specified period of time.

[10] FDICIA Section 112 (12 USC Section 1831m(g)(3)) provides that all auditors are required to make their work papers available to bank examiners. 12 CFR 715.9(c) requires credit unions to obtain a signed audit engagement letter that includes a certification of unconditional access to the complete set of original working papers by credit union examiners.

[11] For example, AICPA's SSAE-16 Type I and Type II, SOC 2 Type I and Type II, SOC 3 (Web Trust). See http://www.aicpa.org/_catalogs/masterpage/Search.aspx?S=soc+1

[12] ISACA, NIST, IAA, & etc.

[13] Shared Assessments Program; see <http://www.sharedassessments.org/>

Appendix A: Examination Procedures

Examination objectives allow the examiner to determine the quality and effectiveness of the audit function related to IT controls. These procedures will disclose the adequacy of audit coverage and to what extent, if any, the examiner may rely upon the procedures performed by the auditors in determining the scope of the IT examination.

- Tier I objectives and procedures relate to the institution's implementation of an effective audit function that may be relied upon to identify and manage risks.
- Tier II objectives and procedures provide additional validation as warranted by risk to verify the effectiveness of the institution's audit function. Tier II questions correspond to the Uniform Rating System for Information Technology (URSIT) rating areas and can be used to determine where the examiner may rely upon audit work in determining the scope of the IT examination for those areas.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Determine the scope and objectives of the examination of the IT audit function and coordinate with examiners reviewing other programs.

1. Review past reports for outstanding issues, previous problems, or high-risk areas with insufficient coverage related to IT. Consider:

- Regulatory reports of examination;
- Internal and external audit reports, including correspondence/communication between the institution and auditors;
- Regulatory, audit, and security reports from key service providers;
- Audit information and summary packages submitted to the board or its audit committee;
- Audit plans and scopes, including any external audit or internal audit outsourcing engagement letters; and
- Institution's overall risk assessment.

2. Review the most recent IT internal and external audit reports in order to determine:

- Management's role in IT audit activities;

- Any significant changes in business strategy, activities, or technology that could affect the audit function;
- Any material changes in the audit program, scope, schedule, or staffing related to internal and external audit activities; and
- Any other internal or external factors that could affect the audit function.

3. Review management's response to issues raised since the last examination. Consider:

- Adequacy and timing of corrective action;
- Resolution of root causes rather than just specific issues; and
- Existence of any outstanding issues.

4. Assess the quality of the IT audit function. Consider:

- Audit staff and IT qualifications, and
- IT audit policies, procedures, and processes.

Using the results from the preceding procedures and discussions with the EIC, select from the following examination procedures those necessary to meet the examination objectives. Note: examinations do not necessarily require all steps.

Objective 2: Determine the quality of the oversight and support of the IT audit function provided by the board of directors and senior management.

1. Review board resolutions and audit charter to determine the authority and mission of the IT audit function.
2. Review and summarize the minutes of the board or audit committee for member attendance and supervision of IT audit activities.
3. Determine if the board reviews and approves IT policies, procedures, and processes.
4. Determine if the board approves audit plans and schedules, reviews actual performance of plans and schedules, and approves major deviations to the plan.
5. Determine if the content and timeliness of audit reports and issues presented to and reviewed by the board of directors or audit committee are appropriate.

6. Determine whether the internal audit manager and the external auditor report directly to the board or to an appropriate audit committee and, if warranted, has the opportunity to escalate issues to the board both through the normal audit committee process and through the more direct communication with outside directors.

Objective 3: Determine the credentials of the board of directors or its audit committee related to their ability to oversee the IT audit function.

1. Review credentials of board members related to abilities to provide adequate oversight. Examiners should:

- Determine if directors responsible for audit oversight have appropriate level of experience and knowledge of IT and related risks; and
- If directors are not qualified in relation to IT risks, determine if they bring in outside independent consultants to support their oversight efforts through education and training.

2. Determine if the composition of the audit committee is appropriate considering entity type and complies with all applicable laws and regulations. Note - If the institution is a publicly traded company, this is a requirement of Sarbanes-Oxley. Additionally, this is a requirement of FDICIA for institutions with total assets greater than \$500 million.

Objective 4: Determine the qualifications of the IT audit staff and its continued development through training and continuing education.

1. Determine if the IT audit staff is adequate in number and is technically competent to accomplish its mission. Consider:

- IT audit personnel qualifications and compare them to the job descriptions;
- Whether staff competency is commensurate with the technology in use at the institution; and
- Trends in IT audit staffing to identify any negative trends in the adequacy of staffing.

Objective 5: Determine the level of audit independence.

1. Determine if the reporting process for the IT audit is independent in fact and in appearance by reviewing the degree of control persons outside of the audit function have on what is reported to the board or audit committee.

2. Review the internal audit organization structure for independence and clarity of the reporting process. Determine whether independence is compromised by:

- The internal audit manager reporting functionally to a senior management official (i.e., CFO, controller, or similar officer);
- The internal audit manager's compensation and performance appraisal being done by someone other than the board or audit committee; or
- Auditors responsible for operating a system of internal controls or actually performing operational duties or activities.

Note that it is recommended that the internal audit manager report directly to the audit committee functionally on audit issues and may also report to senior management for administrative matters.

Objective 6: Determine the existence of timely and formal follow-up and reporting on management's resolution of identified IT problems or weaknesses.

1. Determine whether management takes appropriate and timely action on IT audit findings and recommendations and whether audit or management reports the action to the board of directors or its audit committee. Also, determine if IT audit reviews or tests management's statements regarding the resolution of findings and recommendations.

2. Obtain a list of outstanding IT audit items and compare the list with audit reports to ascertain completeness.

3. Determine whether management sufficiently corrects the root causes of all significant deficiencies noted in the audit reports and, if not, determine why corrective action is not sufficient.

Objective 7: Determine the adequacy of the overall audit plan in providing appropriate coverage of IT risks.

1. Interview management and review examination information to identify changes to the institution's risk profile that would affect the scope of the audit function. Consider:

- Institution's risk assessment,

- Products or services delivered to either internal or external users,
- Loss or addition of key personnel, and
- Technology service providers and software vendor listings.

2. Review the institution's IT audit standards manual and/or IT-related sections of the institution's general audit manual. Assess the adequacy of policies, practices, and procedures covering the format and content of reports, distribution of reports, resolution of audit findings, format and contents of work papers, and security over audit materials.

Objective 8: Determine the adequacy of audit's risk analysis methodology in prioritizing the allocation of audit resources and formulating the IT audit schedule.

1. Evaluate audit planning and scheduling criteria, including risk analysis, for selection, scope, and frequency of audits. Determine if:

- The audit universe is well defined; and
- Audit schedules and audit cycles support the entire audit universe, are reasonable, and are being met.

2. Determine whether the institution has appropriate standards and processes for risk-based auditing and internal risk assessments that:

- Include risk profiles identifying and defining the risk and control factors to assess and the risk management and control structures for each IT product, service, or function; and
- Describe the process for assessing and documenting risk and control factors and its application in the formulation of audit plans, resource allocations, audit scopes, and audit cycle frequency

Objective 9: Determine the adequacy of the scope, frequency, accuracy, and timeliness of IT-related audit reports.

1. Review a sample of the institution's IT-related audit reports and work papers for specific audit ratings, completeness, and compliance with board and audit committee-approved standards.

2. Analyze the internal auditor's evaluation of IT controls and compare it with any evaluations done by examiners.

3. Evaluate the scope of the auditor's work as it relates to the institution's size, the nature and extent of its activities, and the institution's risk profile.

4. Determine if the work papers disclose that specific program steps, calculations, or other evidence support the procedures and conclusions set forth in the reports.

5. Determine through review of the audit reports and work papers if the auditors accurately identify and consistently report weaknesses and risks.

6. Determine if audit report content is:

- Timely
- Constructive
- Accurate
- Complete

Objective 10: Determine the extent of audit's participation in application development, acquisition, and testing, as part of the organization's process to ensure the effectiveness of internal controls.

1. Discuss with audit management and review audit policies related to audit participation in application development, acquisition, and testing.

2. Review the methodology management employs to notify the IT auditor of proposed new applications, major changes to existing applications, modifications/additions to the operating system, and other changes to the data processing environment.

3. Determine the adequacy and independence of audit in:

- Participating in the systems development life cycle;

- Reviewing major changes to applications or the operating system;
- Updating audit procedures, software, and documentation for changes in the systems or environment; and
- Recommending changes to new proposals or to existing applications and systems to address audit and control issues.

Objective 11: If the IT internal audit function, or any portion of it, is outsourced to external vendors, determine its effectiveness and whether the institution can appropriately rely on it.

1. Obtain copies of:

- Outsourcing contracts and engagement letters,
- Outsourced internal audit reports, and
- Policies on outsourced audit.

2. Review the outsourcing contracts/engagement letters and policies to determine whether they adequately:

- Define the expectations and responsibilities under the contract for both parties.
- Set the scope, frequency, and cost of work to be performed by the vendor.
- Set responsibilities for providing and receiving information, such as the manner and frequency of reporting to senior management and directors about the status of contract work.
- Establish the protocol for changing the terms of the service contract, especially for expansion of audit work if significant issues are found, and stipulations for default and termination of the contract.
- State that internal audit reports are the property of the institution, that the institution will be provided with any copies of the related work papers it deems necessary, and that employees authorized by the institution will have reasonable and timely access to the work papers prepared by the outsourcing vendor.
- State that any information pertaining to the institution must be kept confidential.
- Specify the locations of internal audit reports and the related work papers.
- Specify the period of time that vendors must maintain the work papers. If work papers are in electronic format, contracts often call for vendors to maintain

proprietary software that allows the institution and examiners access to electronic work papers during a specified period.

- State that outsourced internal audit services provided by the vendor are subject to regulatory review and that examiners will be granted full and timely access to the internal audit reports and related work papers and other materials prepared by the outsourcing vendor.
- Prescribe a process (arbitration, mediation, or other means) for resolving problems and for determining who bears the cost of consequential damages arising from errors, omissions and negligence.
- State that outsourcing vendors will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of a member of institution management or an employee and, if applicable, they are subject to professional or regulatory independence guidance.

3. Consider arranging a meeting with the IT audit vendor to discuss the vendor's outsourcing internal audit program and determine the auditor's qualifications.

4. Determine whether the outsourcing arrangement maintains or improves the quality of the internal audit function and the institution's internal controls. The examiner should:

- Review the performance and contractual criteria for the audit vendor and any internal evaluations of the audit vendor;
- Review outsourced internal audit reports and a sample of audit work papers. Determine whether they are adequate and prepared in accordance with the audit program and the outsourcing agreement;
- Determine whether work papers disclose that specific program steps, calculations, or other evidence support the procedures and conclusions set forth in the outsourced reports; and
- Determine whether the scope of the outsourced internal audit procedures is adequate.

5. Determine whether key employees of the institution and the audit vendor clearly understand the lines of communication and how any internal control problems or other matters noted by the audit vendor during internal audits are to be addressed.

6. Determine whether management or the audit vendor revises the scope of outsourced audit work appropriately when the institution's environment, activities, risk exposures, or systems change significantly.

7. Determine whether the directors ensure that the institution effectively manages any outsourced internal audit function.

8. Determine whether the directors perform sufficient due diligence to satisfy themselves of the audit vendor's competence and objectivity before entering the outsourcing arrangement.

9. If the audit vendor also performs the institution's external audit or other consulting services, determine whether the institution and the vendor have discussed, determined, and documented that applicable statutory and regulatory independence standards are being met. Note - If the institution is a publicly traded company, this is a requirement of Sarbanes-Oxley. Additionally, this is a requirement of FDICIA for institutions with total assets greater than \$500 million.

10. Determine whether an adequate contingency plan exists to reduce any lapse in audit coverage, particularly coverage of high-risk areas, in the event the outsourced audit relationship is terminated suddenly.

Objective 12: Determine the extent of external audit work related to IT controls.

1. Review engagement letters and discuss with senior management the external auditor's involvement in assessing IT controls.

2. If examiners rely on external audit work to limit examination procedures, they should ensure audit work is adequate through discussions with external auditors and reviewing work papers if necessary.

Objective 13: Determine whether management effectively oversees and monitors any significant data processing services provided by technology service providers:

1. Determine whether management directly audits the service provider's operations and controls, employs the services of external auditors to evaluate the servicer's controls, or receives sufficiently detailed copies of audit reports from the technology service provider.

2. Determine whether management requests applicable regulatory agency IT examination reports.

3. Determine whether management adequately reviews all reports to ensure the audit scope was sufficient and that all deficiencies are appropriately addressed.

CONCLUSIONS

Objective 14: Discuss corrective actions and communicate findings.

1. Determine the need to perform Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.

2. Using results from the above objectives and/or audit's internally assigned audit rating or audit coverage, determine the need for additional validation of specific audited areas and, if appropriate:

- Forward audit reports to examiners working on related work programs, and
- Suggest either the examiners or the institution perform additional verification procedures where warranted.

3. Using results from the review of the IT audit function, including any necessary Tier II procedures:

- Document conclusions on the quality and effectiveness of the audit function as related to IT controls; and
- Determine and document to what extent, if any, examiners may rely upon the internal and external auditors' findings in order to determine the scope of the IT examination.

4. Review preliminary examination conclusions with the examiner-in-charge (EIC) regarding:

- Violations of law, rulings, and regulations;
- Significant issues warranting inclusion as matters requiring board attention or recommendations in the report of examination; and
- Potential effect of your conclusions on URSIT composite and component ratings.

5. Discuss examination findings with management and obtain proposed corrective action for significant deficiencies.
6. Document examination conclusions, including a proposed audit component rating, in a memorandum to the EIC that provides report-ready comments for all relevant sections of the report of examination.
7. Document any guidance to future examiners of the IT audit area.
8. Organize examination work papers to ensure clear support for significant findings and conclusions.

TIER II OBJECTIVES AND PROCEDURES

The Tier II examination procedures for the IT audit process provide additional verification procedures to evaluate the effectiveness of the IT audit function. These procedures are designed to assist in achieving examination objectives and scope and may be used entirely or selectively.

Tier II questions correspond to URSIT rating areas and can be used to determine where the examiner may rely upon audit work in determining the scope of the IT examination for those areas.

Examiners should coordinate this coverage with other examiners to avoid duplication of effort with the examination procedures found in other IT Handbook booklets.

A. MANAGEMENT

1. Determine whether audit procedures for management adequately consider:
 - The ability of management to plan for and initiate new activities or products in response to information needs and to address risks that may arise from changing business conditions;
 - The ability of management to provide reports necessary for informed planning and decision making in an effective and efficient manner;
 - The adequacy of, and conformance with, internal policies and controls addressing the IT operations and risks of significant business activities;
 - The effectiveness of risk monitoring systems;

- The level of awareness of, and compliance with, laws and regulations;
- The level of planning for management succession;
- The ability of management to monitor the services delivered and to measure the institution's progress toward identified goals in an effective and efficient manner;
- The adequacy of contracts and management's ability to monitor relationships with technology service providers;
- The adequacy of strategic planning and risk management practices to identify, measure, monitor, and control risks, including management's ability to perform self-assessments; and
- The ability of management to identify, measure, monitor, and control risks and to address emerging IT needs and solutions.

B. SYSTEMS DEVELOPMENT AND ACQUISITION

1. Determine whether audit procedures for systems development and acquisition and related risk management adequately consider:

- The level and quality of oversight and support of systems development and acquisition activities by senior management and the board of directors;
- The adequacy of the institutional and management structures to establish accountability and responsibility for IT systems and technology initiatives;
- The volume, nature, and extent of risk exposure to the institution in the area of systems development and acquisition;
- The adequacy of the institution's systems development methodology and programming standards;
- The quality of project management programs and practices that are followed by developers, operators, executive management/owners, independent vendors or affiliated servicers, and end-users;
- The independence of the quality assurance function and the adequacy of controls over program changes including the:
 - parity of source and object programming code,
 - independent review of program changes,
 - comprehensive review of testing results,
 - management's approval before migration into production, and
 - timely and accurate update of documentation;

- The quality and thoroughness of system documentation;
- The integrity and security of the network, system, and application software used in the systems development process;
- The development of IT solutions that meet the needs of end-users; and
- The extent of end-user involvement in the systems development process.

C. OPERATIONS

1. Determine whether audit procedures for operations consider:

- The adequacy of security policies, procedures, and practices in all units and at all levels of the financial institution and service providers.
- The adequacy of data controls over preparation, input, processing, and output.
- The adequacy of corporate contingency planning and business resumption for data centers, networks, service providers, and business units. Consider the adequacy of offsite data and program backup and the adequacy of business resumption testing.
- The quality of processes or programs that monitor capacity and performance.
- The adequacy of contracts and the ability to monitor relationships with service providers.
- The quality of assistance provided to users, including the ability to handle problems.
- The adequacy of operating policies, procedures, and manuals.
- The quality of physical and logical security, including the privacy of data.
- The adequacy of firewall architectures and the security of connections with public networks.

D. INFORMATION SECURITY

1. Determine whether audit procedures for information security adequately consider the risks in information security and e-banking. Evaluate whether:

- A written and adequate data security policy is in effect covering all major operating systems, databases, and applications;
- Existing controls comply with the data security policy, best practices, or regulatory

guidance;

- Data security activities are independent from systems and programming, computer operations, data input/output, and audit;
- Some authentication process, such as user names and passwords, that restricts access to systems;
- Access codes used by the authentication process are protected properly and changed with reasonable frequency;
- Transaction files are maintained for all operating and application system messages, including commands entered by users and operators at terminals, or at PCs;
- Unauthorized attempts to gain access to the operating and application systems are recorded, monitored, and responded to by independent parties;
- User manuals and help files adequately describe processing requirements and program usage;
- Controls are maintained over telecommunication(s), including remote access by users, programmers and vendors; and over firewalls and routers to control and monitor access to platforms, systems and applications;
- Access to buildings, computer rooms, and sensitive equipment is controlled adequately;
- Written procedures govern the activities of personnel responsible for maintaining the network and systems;
- The network is fully documented, including remote and public access, with documentation available only to authorized persons;
- Logical controls limit access by authorized persons only to network software, including operating systems, firewalls, and routers;
- Adequate network updating and testing procedures are in place, including configuring, controlling, and monitoring routers and firewalls;
- Adequate approvals are required before deployment of remote, Internet, or VPN access for employees, vendors, and others;
- Alternate network communications procedures are incorporated into the disaster recovery plans;
- Access to networks is restricted using appropriate authentication controls; and
- Unauthorized attempts to gain access to the networks are monitored.

2. Determine whether audit procedures for information security adequately consider compliance with the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information," as mandated by Section 501(b) of the Gramm-Leach-Bliley Act of 1999. Consider evaluating whether management has:

- Identified and assessed risks to customer information;
- Designed and implemented a program to control risks;
- Tested key controls (at least annually);
- Trained personnel; and
- Adjusted the compliance plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal/external threats to information security.

E. PAYMENT SYSTEMS

1. Determine whether audit procedures for payment systems risk adequately consider the risks in wholesale electronic funds transfer (EFT). Evaluate whether:

Adequate operating policies and procedures govern all activities, both in the wire transfer department and in the originating department, including authorization, authentication, and notification requirements;

- Formal contracts with each wire servicer exist (i.e., Federal Reserve Bank (FRB), correspondent financial institutions, and others);
- Separation of duties is sufficient to prevent any one person from initiating, verifying, and executing a transfer of funds;
- Personnel policies and practices are in effect;
- Adequate security policies protect wire transfer equipment, software, communications lines, incoming and outgoing payment orders, test keys, etc.;
- Credit policies and appropriate management approvals have been established to cover overdrafts;
- Activity reporting, monitoring, and reconciliation are conducted daily, or more frequently based upon activity;
- Appropriate insurance riders cover activity;
- Contingency plans are appropriate for the size and complexity of the wire transfer function; and
- Funds transfer terminals are protected by adequate password security.

2. Determine whether audit procedures for payment systems risk adequately consider

the risks in retail EFT (automatic teller machines, point-of-sale, debit cards, home banking, and other card-based systems including VISA/Master Charge compliance). Evaluate whether:

- Written procedures are complete and address each EFT activity;
- All EFT functions are documented appropriately;
- Physical controls protect plastic cards, personal identification number (PIN) information, EFT equipment, and communication systems;
- Separation of duties and logical controls protect EFT-related software, customer account, and PIN information;
- All transactions are properly recorded, including exception items, and constitute an acceptable audit trail for each activity;
- Reconcilements and proofs are performed daily by persons with no conflicting duties;
- Contingency planning is adequate;
- Vendor and customer contracts are in effect and detail the responsibilities of all parties to the agreement;
- Insurance coverage is adequate; and
- All EFT activity conforms to applicable provisions of Regulation E.

3. Determine whether audit procedures for payment systems risk adequately consider the risks in automated clearing house (ACH). Evaluate whether:

- Policies and procedures govern all ACH activity;
- Incoming debit and credit totals are verified adequately and items counted prior to posting to customer accounts;
- Controls over rejects, charge backs, unposted and other suspense items are adequate;
- Controls prevent the altering of data between receipt of data and posting to accounts;
- Adequate controls exist over any origination functions, including separation of data preparation, input, transmission, and reconciliation;
- Security and control exist over ACH capture and transmission equipment; and
- Compliance with NACHA, local clearinghouse, and FRB rules and regulations.

F. OUTSOURCING

1. Determine whether audit procedures for outsourcing activities adequately cover the risks when IT service is provided to external users. Evaluate whether:

- Formal procedures are in effect and staff is assigned to provide interface with users/ customers to control data center-related issues (i.e., program change requests, record differences, service quality);
- There are contracts with all customers (affiliated and nonaffiliated) and whether the institution's legal staff has approved them;
- Controls exist over billing and income collection;
- Disaster recovery plans interface between the data center, customers, and users;
- Controls exist over on-line terminals employed by users and customers;
- Comprehensive user manuals exist and are distributed; and
- There are procedures for communicating incidents to clients.

2. Determine whether audit procedures for outsourced activities are adequate. Evaluate whether:

- There are contracts in place that have been approved by the institution's legal staff,
- Management monitors vendor performance of contracted services and the financial condition of the vendor,
- Applicable emergency and disaster recovery plans are in place,
- Controls exist over the terminal used by the financial institution to access files at an external servicer's location,
- Internal controls for each significant user application are consistent with those required for in-house systems,
- Management has assessed the impact of external and internal trends and other factors on the ability of the vendor to support continued servicing of client financial institutions,
- The vendor can provide and maintain service level performance that meets the requirements of the client, and
- Management monitors the quality of vendor software releases, documentation, and training provided to clients.

Appendix B: Glossary

Application controls - Controls related to transactions and data within application systems. Application controls ensure the completeness and accuracy of the records and the validity of the entries made resulting from both programmed processing and manual data entry. Examples of application controls include data input validation, agreement of batch totals and encryption of data transmitted.

Application system - An integrated set of computer programs designed to serve a well-defined function and having specific input, processing, and output activities (e.g., general ledger, manufacturing resource planning, human resource management).

Audit charter - A document approved by the board of directors that defines the IT audit function's responsibility, authority to review records, and accountability.

Audit plan - A description and schedule of audits to be performed in a certain period of time (ordinarily a year). It includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work and includes other items such as budget, resource allocation, schedule dates, and type of report issued.

Audit program - The audit policies, procedures, and strategies that govern the audit function, including IT audit.

Exposure - The potential loss to an area due to the occurrence of an adverse event.

General controls - Controls, other than application controls, that relate to the environment within which application systems are developed, maintained, and operated, and that are therefore applicable to all the applications at an institution. The objectives of general controls are to ensure the proper development and implementation of systems, and the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IT strategy and an IT security policy, the organization of IT staff to separate conflicting duties and planning for disaster prevention and recovery.

Independence - Self-governance, freedom from conflict of interest and undue influence. The IT auditor should be free to make his or her own decisions, not influenced by the organization being audited, or by its managers and employees.

Outsourcing - The practice of contracting with another entity to perform services that might otherwise be conducted in-house. Contracted relationship with a third party to provide services, systems, or support.

Risk - The potential that events, expected or unanticipated, may have an adverse effect on a financial institution's earnings or capital.

Risk assessment - A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.

Systems Development Life Cycle (SDLC) - An approach used to plan, design, develop, test, and implement an application system or a major modification to an application

system.

Work program - A series of specific, detailed steps to achieve an audit objective.

Appendix C: Laws, Regulations, and Guidance

Laws

- 12 USC 1761 & 1761d: Supervisory Committee (N/A)
- Public Law 107-204: Sarbanes-Oxley Act of 2002, Pub (N/A)

Federal Financial Institutions Examination Council

- Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (March 2003)
- Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations (September 1999)
- Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners (July 1992)

Federal Reserve Board

- 12 CFR Part 208, Appendix D-1: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
- SR Letter 03-8; Statement on Application of Recent Corporate Governance Initiatives to Non-Public Banking Organizations (May 5, 2003)
- SR Letter 03-5: Amended Interagency Guidance on the Internal Audit Function and its Outsourcing (April 22, 2003)
- SR Letter 02-20: The Sarbanes-Oxley Act of 2002 (October 29, 2002)

Federal Deposit Insurance Corporation

- 12 CFR Part 363: Annual Independent Audits and Reporting Requirements (N/A)
- FIL 21-2003: Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (March 7, 2003)
- FIL 96-99: Interagency Policy Statement On External Auditing Programs of Banks

and Savings Associations (October 25, 1999)

National Credit Union Administration

- 12 CFR Part 715: Supervisory Committee Audits and Verifications (N/A)
- NCUA Letter to Credit Unions 02-CU-17: E-Commerce Guide for Credit Unions (December 2002)
- NCUA Letter to Credit Unions 01-CU-11: Electronic Data Security Overview (August 2001)
- NCUA Letter to Credit Unions 97-CU-5: Interagency Statement on Retail On-Line PC Banking (April 1997)

Office of the Comptroller of the Currency

- 12 CFR Part 30: Safety and Soundness Standards (N/A)
- OCC Bulletin 2003-12: Interagency Policy Statement on Internet Audit and Internal Audit Outsourcing (March 17, 2003)
- OCC Bulletin 99-37: Interagency Policy Statement on External Auditing Programs (July 9, 2003)
- Comptroller's Handbook: Community Bank Supervision, Booklet (August 2001)
- Comptroller's Handbook: Community Bank Supervision, Appendix (August 2001)
- Comptroller's Handbook: Internal and External Audits, Introduction (April 2003)
- Comptroller's Handbook: Internal and External Audits, Appendixes (April 2003)
- Comptroller's Handbook: Large Bank Supervision (May 2001)
- Comptroller's Handbook: Internal and External Audits, Supplemental Examination Procedures (April 2003)
- The Director's Book: The Role of a National Bank Director (March 1997)

Office of Thrift Supervision

- 12 CFR Part 562.4: Audit of Savings Associations and Savings Association Holding Companies (N/A)

- 12 CFR Part 570, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
- Thrift Bulletin 81: Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (March 17, 2003)
- CEO LTR 113: Internal Controls (July 14, 1999)
- Thrift Activities Handbook Section 341: Technology Risk Controls (January 2002)
- Thrift Activities Handbook Section 350: External Audit (July 2002)
- Thrift Activities Handbook Section 355: Internal Audit (February 2002)



FFIEC Information Technology Examination Handbook

Business Continuity Management

NOVEMBER 2019

Contents

INTRODUCTION.....	1
I BUSINESS CONTINUITY MANAGEMENT	2
II BUSINESS CONTINUITY MANAGEMENT GOVERNANCE.....	3
II.A Board and Senior Management Responsibilities	4
II.B Audit	6
III RISK MANAGEMENT.....	7
III.A Business Impact Analysis	9
III.A.1 Identification of Critical Business Functions	10
III.A.2 Interdependency Analysis	10
III.A.3 Impact of Disruption	11
III.B Risk Assessment.....	12
III.B.1 Risk Identification	13
III.B.2 Likelihood and Impact	14
IV BUSINESS CONTINUITY STRATEGIES	16
IV.A Resilience	18
IV.A.1 Physical	19
IV.A.2 Cyber Resilience	19
IV.A.3 Data Backup and Replication	19
IV.A.4 Personnel	21
IV.A.5 Third-Party Service Providers.....	22
IV.A.6 Telecommunications	23
IV.A.7 Power	24
IV.A.8 Change Management.....	24
IV.B Communications	25
V BUSINESS CONTINUITY PLAN	26
V.A Event Management.....	27
V.B Continuity and Recovery	28
V.C Facilities and Infrastructure	29
V.C.1 Data Center Recovery Alternatives	29
V.C.2 Branch Relocation	30
V.D Payment Systems.....	31
V.E Liquidity Considerations	31
V.F Other Components.....	31
V.F.1 Incident Response.....	32

V.F.2	Disaster Recovery	33
V.F.3	Crisis or Emergency Management	34
VI	TRAINING	35
VII	EXERCISES AND TESTS	37
VII.A	Exercise and Test Program	38
VII.B	Exercise and Test Policy	39
VII.C	Exercise and Test Strategies.....	39
VII.D	Exercise and Test Objectives.....	40
VII.E	Exercise and Test Plans	40
VII.F	Exercise and Test Scenarios.....	41
VII.G	Exercise and Test Methods	42
VII.G.1	Full-Scale Exercise.....	42
VII.G.2	Limited-Scale Exercise	43
VII.G.3	Tabletop Exercise.....	43
VII.G.4	Tests	44
VII.H	Industry Exercises and Resilience	44
VII.I	Third-Party Service Provider Testing	45
VII.J	Testing for Core and Significant Firms	45
VII.K	Post-Exercise and Post-Test Actions	46
VIII	MAINTENANCE AND IMPROVEMENT	47
IX	BOARD REPORTING	49
APPENDIX A:	EXAMINATION PROCEDURES	50
APPENDIX B:	GLOSSARY	70
APPENDIX C:	ABBREVIATIONS.....	77
APPENDIX D:	REFERENCES.....	78

Introduction

The “Business Continuity Management” (BCM) booklet is one in a series of booklets that comprise the *Federal Financial Institutions Examination Council (FFIEC)*¹ *Information Technology Examination Handbook (IT Handbook)*. The *IT Handbook* is prepared for use by examiners.² With the publication of this booklet, the FFIEC member agencies replace the “Business Continuity Planning” booklet issued in February 2015. The change from business continuity planning to business continuity management reflects the changes in customer and industry expectations for the resilience of operations.

The BCM booklet describes principles and practices for IT and operations for safety and soundness, consumer financial protection, and compliance with applicable laws and regulations. The BCM booklet also outlines BCM principles to help examiners evaluate how management addresses risk related to the availability of critical financial products and services. This booklet discusses BCM governance and its related components, including resilience strategies and plan development; training and awareness; exercises and tests; maintenance and improvement; and reporting for all levels of management, including the board of directors.

The focus of this revised booklet is on enterprise-wide, process-oriented approaches that consider technology, business operations, testing, and communication strategies critical to the continuity of the entire entity. However, business continuity should not be focused only on the planning process to recover operations after an event, but rather it should include the continued maintenance of systems and controls for the resilience of operations. Business continuity should be incorporated into the risk management life cycle of all systems, processes, and operations of an entity.

For *IT Handbook* purposes, the term “entities” includes depository financial institutions,³ nonbank financial institutions,⁴ bank holding companies,⁵ and third-party service providers.⁶

¹ The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. 95-630. The FFIEC members include the Board of Governors of the Federal Reserve System (FRB), the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the State Liaison Committee (SLC).

² Each FFIEC member agency may use the principles outlined in this booklet, consistent with the member agency’s supervisory authority.

³ The term “depository financial institution” includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions.

⁴ The term “nonbank financial institution” includes non-depository financial institutions under CFPB’s jurisdiction and subject to CFPB supervision and examination.

⁵ The term “bank holding company” includes any company which has control over any bank or over any company that is or becomes a bank holding company as defined by the Bank Holding Company Act.

⁶ The term “third-party service providers” includes those entities that provide banking services subject to examination under the Bank Service Company Act, the Home Owners Loan Act of 1933, the Dodd-Frank Wall Street Reform and Consumer Protection Act, or other relevant law.

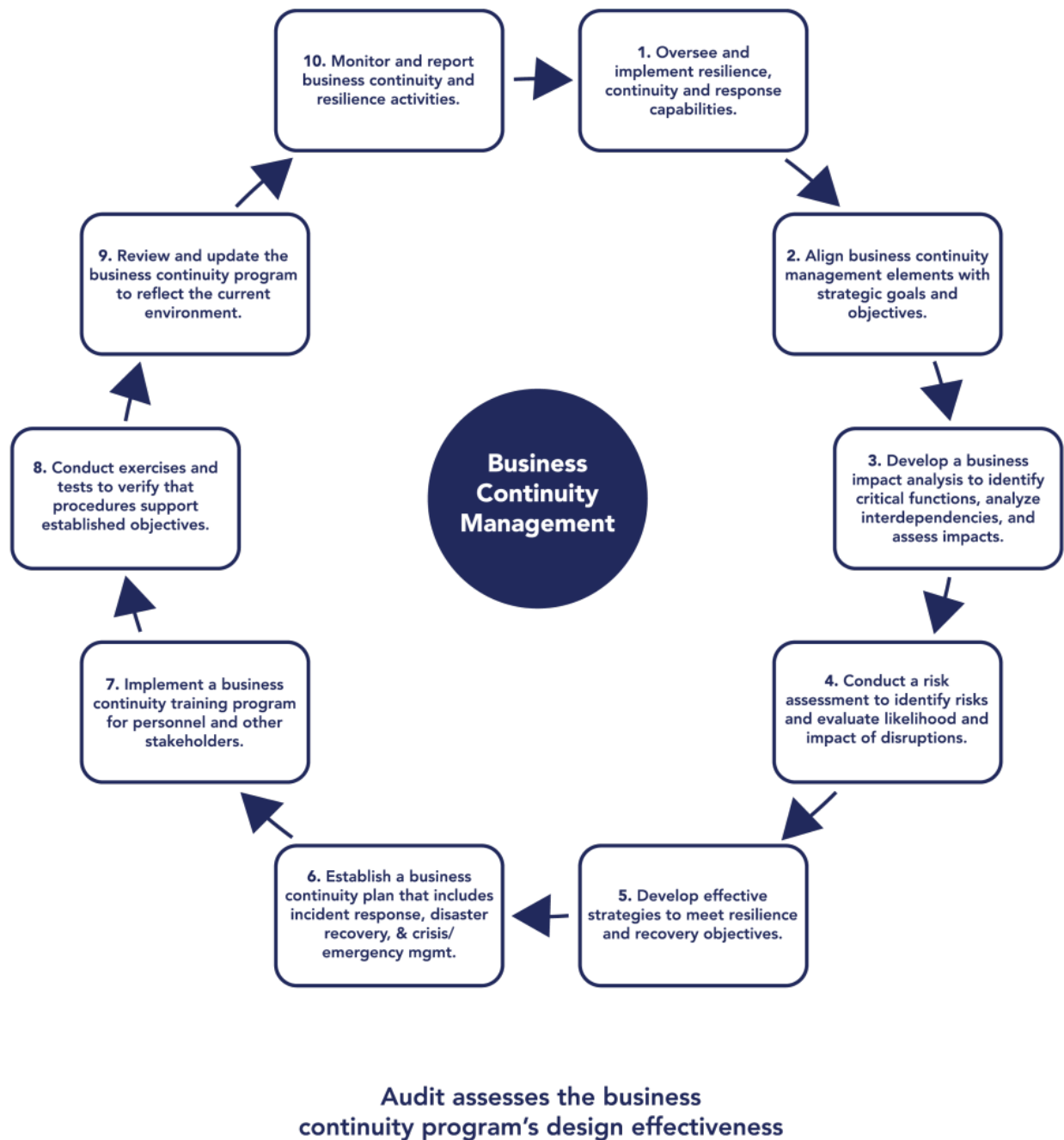
This booklet does not impose requirements on entities. Instead, this booklet describes practices that examiners may use to assess an entity's BCM function.

Appendix A of this booklet provides objectives-based examination procedures. The application of the principles and related examination procedures should vary according to an entity's complexity and risk profile. Examiners should evaluate entities in accordance with their agency's regulatory authority.

I Business Continuity Management

BCM is the process for management to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services. Disruptions such as cyber events, natural disasters, or man-made events can interrupt an entity's operations and can have a broader impact on the financial sector. Resilience incorporates proactive measures to mitigate disruptive events and evaluate an entity's recovery capabilities. An entity's BCM program should align with its strategic goals and objectives. Management should consider an entity's role within and impact on the overall financial services sector when it develops a BCM program.

Figure 1: Business Continuity Management Cycle



II Business Continuity Management Governance

This section provides specific information about BCM governance, including board and senior management responsibilities. General information about governance and risk management is contained in the *IT Handbook's* "Management" booklet and the FFIEC members' examination handbooks.

BCM governance should include:

- Aligning BCM practices with the risk appetite.
- Identifying the continuity level needed, consistent with the operation's criticality.
- Establishing business continuity policy and plans.
- Allocating resources to BCM activities.
- Providing competent management to implement the program.
- Monitoring and assessing business continuity performance relative to these goals.

Figure 1 depicts a typical BCM cycle that entities may follow to manage business continuity risks on an ongoing basis. To manage these risks, the entity may develop a single encompassing BCM policy or individual policies and plans for different functions, depending on the size and complexity of the entity's operations. An effective practice for business continuity-related policies is to address, at a minimum, the following areas: scope and responsibilities within BCM, accountability, authority, and guidance to develop and maintain effective BCM.

II.A Board and Senior Management Responsibilities

Action Summary

The board and senior management govern business continuity through defining responsibilities and accountability, and by allocating adequate resources to business continuity.

Examiners should review for the following:

- Alignment of BCM elements with the entity's strategic goals and objectives.
- Board oversight.
- Management assignment of BCM-related responsibilities.
- Development of BCM strategies.

The board⁷ and senior management should set the “tone at the top” and consider the entity's entire operations, including functions performed by affiliates and third-party service providers, when managing business continuity. Management should evaluate continuity risk, set short- and long-term continuity objectives, adopt policies and procedures to mitigate continuity risk, evaluate continuity performance, and adjust operations in response to test results and actual events.

Management can strengthen resilience by assessing risk, planning, testing the plans, and incorporating lessons learned from tests and events. Furthermore, management should consider resilience in business functions and the design of new products and services.

⁷ Most financial institutions have boards of directors; however, not all third-party service providers do. When an entity does not have a board, the senior leaders may have the responsibilities of the board described in this booklet.

Board oversight should include:

- Assigning BCM responsibility and accountability.
- Allocating resources to BCM.
- Aligning BCM with the entity's business strategy and risk appetite.
- Understanding business continuity risks and adopting policies and plans to manage events.
- Reviewing business continuity operating results and performance through management reporting, testing, and auditing.
- Providing a credible challenge⁸ to management responsible for the BCM process.

Management oversight should include:

- Defining BCM roles, responsibilities, and succession plans.
- Allocating knowledgeable personnel⁹ and sufficient financial resources.
- Validating that personnel understand their business continuity roles and responsibilities.
- Establishing measurable goals against which business continuity performance is assessed, such as levels of preparedness and resilience targets.
- Designing and implementing a business continuity exercise strategy.
- Confirming that exercises, tests, and training are comprehensive and consistent with the BCM strategy.
- Resolving weaknesses identified in exercises, tests, and training that exceed the entity's risk appetite.
- Meeting regularly with a designated coordinator or a business continuity committee to discuss policy changes, exercises, tests, and training plans.
- Assessing and updating business continuity strategies and plans to reflect the current business conditions and operating environment for continuous improvement.
- Coordinating plans and responses with external groups (as described in [IV.B, "Communications"](#)).

⁸ A credible challenge involves being actively engaged, asking thoughtful questions, and exercising independent judgment.

⁹ The term "personnel" includes both permanent and temporary staff.

II.B Audit

Action Summary

The board and senior management should engage internal audit or independent personnel to review and validate the design and operating effectiveness of the BCM program. Audit should report to the board and provide an assessment of management's ability to manage and control risks related to continuity and resilience.

Examiners should review the following:

- Scope of BCM-related audit activities.
- Audit reporting of BCM-related activities to the board.
- Board review of audit reports.
- Tracking and resolution of audit findings.
- Management's review of system and organization controls (SOC)¹⁰ and third-party service provider audit reports.

The board and senior management should engage internal audit (or an independent review) to assess the BCM design effectiveness, including policies and procedures, and the effectiveness of controls. Audit should report to the board and provide an assessment of management's ability to oversee and control risks related to continuity and resilience. Auditors should be qualified and independent of BCM processes. Audit scope and frequency depend on the entity's complexity, risk profile, and changes the entity may be experiencing. Large, complex entities may have multiple audits, covering various departments or aspects of the BCM program. Less complex entities may have their business continuity activities included within an IT general controls audit.

The internal audit of the BCM program should provide an independent assessment of management's ability to oversee the entity's continuity and resilience risk. Auditors should:

- Evaluate the business impact analysis (BIA) and risk assessment for reasonableness, identification of critical functions, and the likelihood of different events and the potential impact on operations.
- Evaluate controls for reliability, adequacy, and effectiveness regarding continuity and resilience.
- Leverage SOC reports and other external artifacts from third-party service providers, as appropriate.

¹⁰ "In 2017, the American Institute of Certified Public Accountants (AICPA) introduced the term "system and organization controls" (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization and system- or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the AICPA enables the introduction of new internal control examinations that may be performed (a) for other types of organizations, in addition to service organizations, and (b) on either system-level or entity-level controls of such organizations." (AICPA, [SOC 2 Examinations and SOC for Cybersecurity Examinations: Understanding the Key Distinctions.](#))

- Compare the entity's inherent risk level and the effectiveness of risk mitigation against the entity's risk appetite.
- Verify whether test plans achieve the stated objectives.
- Monitor BCM testing to verify that issues (e.g., deviation from test plans and failed objectives) are appropriately identified and escalated.
- Assess the BCM program's effectiveness.

Refer to the *IT Handbook's* "Audit" booklet for additional information.

III Risk Management

Business continuity risk management focuses on a subset of operational risk factors, against which capital and reserves alone may not protect an entity, and involves managing the possibility of an event that jeopardizes critical systems.¹¹ The BIA and risk assessment represent the foundation of BCM. As illustrated in figure 2, BCM should integrate with an entity's enterprise risk management (ERM),¹² which allows for the identification and management of risk across the entire entity. BCM allows management to set strategy to effectively mitigate risks posed by disruptive events. The level and formality of BCM and ERM integration should be commensurate with the entity's complexity and risk profile.

Figure 2: Business Continuity Management Elements (Relative to Enterprise Risk Management)



¹¹ Refer to the U.S. Department of the Treasury and the Department of Homeland Security's (DHS) [Financial Services Sector-Specific Plan 2015](#).

¹² ERM is "[a] process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." (Committee of Sponsoring Organizations of the Treadway Commission (COSO), [Enterprise Risk Management – Integrated Framework \(Executive Summary\)](#), September 2004)

Management should use the BIA and risk management processes to identify and monitor continuity risks for an entity. Once management determines the risk, there are four common strategies to address that risk: risk acceptance, risk mitigation, risk transference, and risk avoidance. Risk transference, such as obtaining insurance, may allow management to recover financial losses or expenses resulting from an event and can be an effective capital management tool; however, insurance should not be a substitute for effective controls or continuity and resilience planning. Management's continuity and resilience planning efforts should focus on risk mitigation and avoidance strategies, and where appropriate, risk acceptance strategies. These strategies are covered more in depth throughout this booklet. Refer to the *IT Handbook's* "Management" booklet for additional information.

Management at large and systemically important entities whose failure could trigger a broader financial disruption should assess the likelihood and impact of a disruption, both to the entity and the entire financial sector. These entities are a critical component of the broader financial system and should incorporate scenarios of disruptions impacting the financial sector into the entity's BCM processes.

The *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Sound Practices Paper)*¹³ outlines practices for financial industry participants that perform clearing and settlement activities for critical financial markets (core firms) and institutions that process a significant share of transactions in critical financial markets (significant firms). Regulators have notified all participants that meet the definition of a core or significant firm as set forth in the *Sound Practices Paper*. Because core and significant firms participate in one or more critical financial markets, and their failure to perform critical activities by the end of a business day could present systemic risk to financial systems, their role in financial markets should be addressed as part of the business continuity planning process.

¹³ Refer to the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* issued by the [SR Letter 03-9](#) (FRB), [Bulletin 2003-14](#) (OCC), and [Release No. 34-47638](#) (U.S. Securities and Exchange Commission (SEC)). Also refer to [68 Fed. Reg. 17809](#).

III.A Business Impact Analysis

Action Summary

Management should develop a BIA that identifies all business functions and prioritizes them in order of criticality, analyzes related interdependencies among business processes and systems, and assesses a disruption's impact through established metrics. The BIA should define recovery priorities and resource dependencies for critical processes.

Examiners should review the following as part of the BIA process:

- Identification of critical business functions.
- Identification of interdependencies across business units.
- Identification and analysis of disruptive events.
- Reasonableness of recovery objectives.
- Communication of BIA results throughout the entity.
- Comprehensiveness of management's BIA review.

A BIA is the process of identifying the potential impact of disruptive events to an entity's functions and processes. A BIA allows management to identify and analyze gaps in critical processes that would prevent the entity from meeting its business requirements. The BIA generally lists recovery priorities and resources on which critical processes depend (e.g., work flow analysis¹⁴). Through the BIA process, management should identify interdependencies among critical operations, departments, personnel, services, and the functions with the greatest exposure to interruption. Management should identify resources on which these functions and processes depend and exposures that would warrant further protective measures. Furthermore, the BIA should include financial and other resource costs (e.g., the loss of business, and exposure to legal and regulatory consequences) needed to recover and restore business functions and processes.

The time and resources to complete the BIA depends on the entity's size and complexity. Complex entities may have multiple BIAs for various business lines, subsidiaries, or other organizational separations. Information from the ERM, such as business processes and risk appetites, may facilitate the BIA development.

¹⁴ The work flow analysis can assist in documenting interdependencies among critical operations, departments, personnel, and services.

III.A.1 Identification of Critical Business Functions

Completing the BIA generally involves gathering information regarding business functions, impacts from disruptions, and business interdependencies; analyzing this information; and establishing recovery objectives. Critical business functions,¹⁵ including support activities (e.g., help desk, call center, human resources, and payroll), systems, and interrelationships may be analyzed in several ways. Work flows, interviews, organizational charts, network diagrams/topologies, data flow diagrams, succession plans, or delegations of authority for key personnel may help management identify business processes and hierarchies.

Management should inventory the entity's critical assets (e.g., people, hardware, software, data, information, and cash) and infrastructure (e.g., network connectivity, communication lines, facilities, and utilities), including those provided by third-party service providers. Furthermore, management should consider supporting activities (e.g., technology support, payroll, contracting) and software (e.g., email, office productivity suites), geographic locations, and unique aspects (e.g., proprietary hardware and software, documentation, or other specialized supplies). Management should also inventory third-party service providers, including specific services they provide. The methodology used should be repeatable, allowing management to reevaluate information after significant changes.

III.A.2 Interdependency Analysis

The BIA process allows management to identify, analyze, and prioritize interdependencies among business functions and systems for alignment with resilience and recovery objectives. The analysis allows management to evaluate interdependent business functions, systems, and shared resources.

During its analysis, management should identify single points of failure, which may include telecommunication lines, network connections between branches, backups that become corrupted, reliance on one power source, or data center locations in close geographic proximity. Personnel can be a single point of failure if there are no cross-trained personnel to back up their responsibilities. Important interdependencies that should be considered include the following:

- Internal systems and business functions, which could include customer services, production processes, hardware, software, application programming interfaces (i.e., code that allows two programs to communicate with each other), data, and documentation of vital records for legal/statutory or process documentation.
- Third-party service providers (e.g., core processing, online and mobile banking, settlement activities, and disaster recovery services), key suppliers (e.g., hardware, software, and utility providers), and business partners and their roles and responsibilities for resilience and recovery.

The BIA will assist management in forming contract and service-level agreement (SLA) requirements for availability and reliability of each service. For pre-existing contracts and SLAs,

¹⁵ The term "function" can consist of one or more processes.

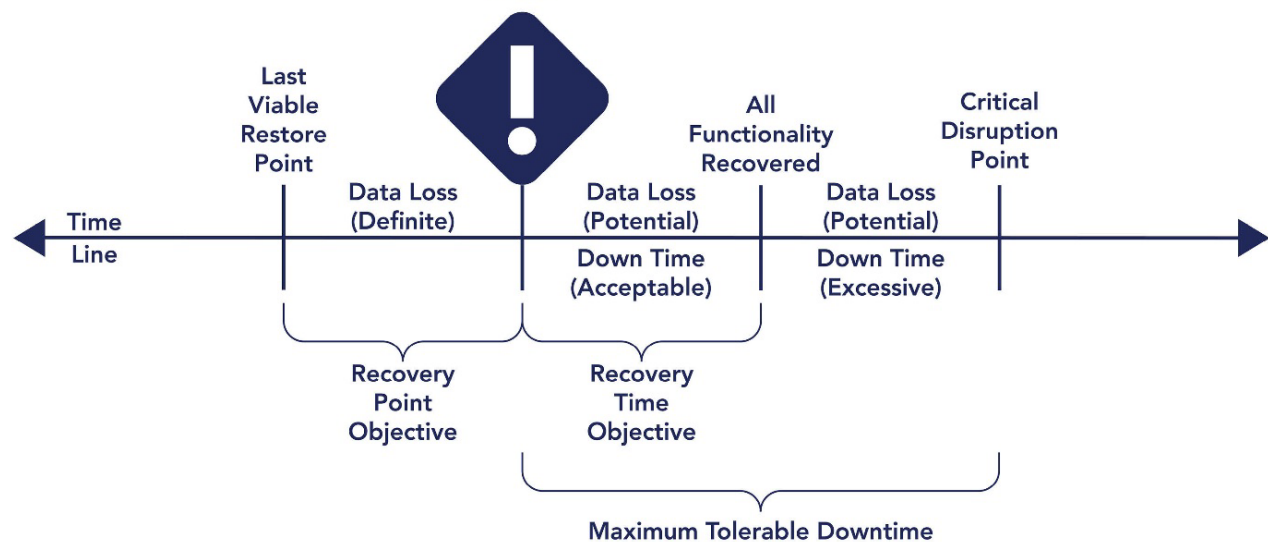
management should confirm that the contract and SLA requirements align with management's and the customer's continuity and resilience expectations.

III.A.3 Impact of Disruption

Through the BIA process, management should evaluate the potential impacts of disruptive events, including operational, financial, and other impacts. Management should establish recovery objectives after determining a disruption's impact. Common measurements include recovery point objective (RPO), recovery time objective (RTO), and maximum tolerable downtime (MTD).

Where applicable, these measurements should be evaluated for alignment with third-party service providers' contracted recovery expectations.

Figure 3: Recovery Objectives (Relative to an Event)



As illustrated in figure 3, the RPO represents the point in time, before a disruption, to which data can be recovered (given the most recent backup copy of the data) after an outage. Refer to section [IV.A.2, “Cyber Resilience,”](#) for additional information regarding backups.

As illustrated in figure 3, the RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and business processes. Determining the RTO is important for selecting appropriate technologies and strategies. When it is not feasible to meet an RTO, management should verify whether the RTO is realistic, initiate an action plan and milestone(s) to document the situation, and, when appropriate, plan for its mitigation. Management should consider interrelated RTOs for each business function to determine the total downtime caused by a disruption. Establishing realistic RTOs assists management in determining a critical path and hierarchy for recovery. For example, a process with a shorter RTO that is dependent upon on a process with a longer RTO may indicate a gap that should be analyzed further.

Whether driven by customer expectations or technological advancement, previously established RTOs that were a few hours in duration may now require near real-time recovery. Therefore, it may be appropriate for management to reevaluate currently acceptable RTOs.

As illustrated in figure 3, the MTD represents the total amount of time the system owner or authorizing official is willing to accept for a business process disruption and includes all impact considerations. The MTD is important for contingency planners when selecting an appropriate recovery method and developing the scope and depth of recovery procedures. Examiners may encounter other terminology to describe MTD (e.g., maximum allowable downtime).

Failure to meet established metrics, such as RPO, RTO, and MTD, may have operational impacts, including discontinued or reduced service levels, inability to meet security requirements, workflow disruptions, supply chain disruptions, and delays of business initiatives. The financial impact could include the loss of revenue, increased costs, or fines and penalties.

III.B Risk Assessment

Action Summary

Management should evaluate the likelihood and impact of potential disruptions and events. As part of this evaluation, management should consider the geographical area where the entity operates. Additionally, management should consider the risks and threats that could affect the entity's third-party service providers. Once management identifies scenarios; evaluates specific threats to the controls, strategies, and plans; and understands the entity's risk exposure, management should develop risk treatment strategies (including risk acceptance or risk transfer) based on the entity's risk appetite.

Examiners should review the risk assessment and determine whether it addresses the impact and likelihood of disruptions of the entity's information services, technology, personnel, facilities, and services provided by third parties. Specifically, examiners should review whether the following types of events are included in the risk assessment:

- Natural events such as fires, floods, severe weather, air contaminants, and hazardous spills.
- Technical events such as communication failure, power failure, equipment and software failure, transportation system disruptions, and water system disruptions.
- Malicious activity, including fraud, theft, blackmail, sabotage, cyber attacks, and terrorism.
- International events that may affect services (e.g., political instability and economic disruptions).
- Low likelihood and high impact events (e.g., terrorist attacks or pandemic events).

Risk assessment is the process of identifying risks to operations, organizational assets, individuals, and other organizations. Risk assessments incorporate threat and vulnerability

analyses and address the appropriate mitigations. As part of risk assessment processes, information from the ERM can be leveraged, such as business process documentation, critical risks, impacts, and tolerances. Management should use risk assessments to identify, measure, and mitigate risk exposures to critical functions and processes identified by the BIA. Furthermore, the risk assessment process may result in changes to the BIA. For example, management may prioritize business processes based on their importance to strategic goals and safe and sound practices; however, after developing threat models, results may necessitate prompt alteration of initial priorities or recovery plans.

III.B.1 Risk Identification

While management performs risk assessments, the focus of business continuity risk identification is on the resilience of the entity. While the causes of events can vary greatly, many of the effects do not. According to the Federal Emergency Management Agency (FEMA), threats and hazards can be categorized as natural, technological, and adversarial or human-caused.¹⁶ Each of these threats and hazards can be subcategorized, for example as internal (e.g., malicious insider or human error) or external, systemic or non-systemic, deliberate or inadvertent, and with or without warning. Although the characteristics of each hazard and threat (e.g., speed of onset, size of the affected area) may be different, the general tasks for recovering operations are the same. Management should address common operational functions in the business continuity plan (BCP) instead of having unique plans for every type of hazard or threat. Planning for all threats and hazards ensures that, when addressing emergency functions, planners identify common tasks and the personnel responsible for accomplishing the tasks.

Management should evaluate potential risks that are in the entity's geographic area. For example, entities could be located in flood-prone areas, earthquake zones, terrorist targets, or areas affected by tornados or hurricanes. In addition to geographic areas, management should also assess geopolitical risk and the potential for retaliatory cyber attacks. For example, U.S. sanctions against a nation-state could increase the risk of cyber attacks against critical infrastructure(s).

Management should coordinate business continuity risk identification efforts throughout the entity. Individual business units within larger entities should coordinate risk identification activities to identify systemic threats to the overall entity. Management should identify and inventory the entity's internal and external assets, types of threats and hazards, and existing controls as an important part of effective risk identification. Refer to the *IT Handbook's* "Management" booklet for additional information.

Furthermore, management should identify cyber security risks (refer to the *IT Handbook's* "Information Security" booklet for additional information), which should be gathered as part of the risk assessment process. Cyber security can pose risk to customer information as discussed in

¹⁶ Refer to FEMA's [Comprehensive Preparedness Guide \(CPG\) 101 Version 2.0](#). Non-FFIEC agency documents are included for illustrative purposes of common risks and are not supervisory expectations.

the *Interagency Guidelines Establishing Information Security Standards*¹⁷ that implement the Gramm-Leach-Bliley Act (GLBA).

Management should coordinate with external sources to obtain information about hazards and threats. External sources include industry information-sharing groups (e.g., Financial Services Information Sharing and Analysis Center (FS-ISAC)), and local, state, and federal authorities¹⁸ that provide timely and actionable information about hazards and threats. In addition, sharing information about events at an entity may help others identify, evaluate, and mitigate cybersecurity threats and vulnerabilities. Information about hazards and threats should be considered in the BIA, risk assessment, and other BCM processes. Refer to the *IT Handbook's* "Information Security" booklet for additional information.

One component in the risk identification process is the gathering and assessment of threat intelligence, which National Institute of Standards and Technology (NIST) defines as "information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes." Management should integrate its threat-intelligence process with the BCM function.

Threats are potentially magnified when entities and their third-party service providers are tightly interconnected. An incident affecting one entity or third-party service provider can result in cascading impacts that quickly affect other service providers, institutions, or sectors. The term "supply chain risk" in BCM may be used to represent the risk related to the interconnectivity among the entity and others. A critical failure at a third-party service provider could have large-scale consequences. Management should identify interconnectivity points between the entity and its third-party service providers, as well as between other entities and third-party service providers. Documenting the flow of transactions, such as developing formal process diagrams, may help management identify interdependencies and end-to-end processes.

III.B.2 Likelihood and Impact

Management should evaluate the likelihood and impact of disruptive events. Risks may range from those with a high likelihood of occurrence and low impact, such as brief power interruptions, to those with a low probability of occurrence and high impact, such as pandemics. The most difficult risks to address are those that may have a high impact on the entity but a low probability of occurrence. The Department of Homeland Security's (DHS) *National Infrastructure Protection Plan*¹⁹ provides examples of risk measurement processes and methodologies to help analyze risks.

¹⁷ Refer to the *Interagency Guidelines Establishing Information Security Standards* issued by [12 CFR 364, Appendix B](#) (FDIC); [12 CFR 208, Appendix D-2](#) and [12 CFR 225, Appendix F](#) (FRB); and [12 CFR 30, Appendix B](#) (OCC). Also refer to *Guidelines for Safeguarding Member Information*, [12 CFR 748, Appendix A](#) (NCUA).

¹⁸ Examples include ChicagoFIRST county and state government, the DHS's National Terrorism Advisory System, FEMA, and the World Health Organization.

¹⁹ Refer to DHS's [National Infrastructure Protection Plan](#).

As part of the assessment, management should quantify the impacts and define loss criteria as either quantitative (financial) or qualitative (e.g., impact to customers). The BCM risk assessment should be commensurate with the entity's risk and complexity and should include reasonably foreseeable events. Worst-case scenarios, such as destruction of the facilities and loss of life, should be addressed. State and local authorities may assist management with identifying specific risks or exposures for geographic locations, and special requirements for accessing emergency zones.

Management should also assess whether its third-party service providers consider the likelihood of a disruption based on the geographic location of facilities, their susceptibility to threats (e.g., location in a flood plain), and the proximity to critical infrastructure (e.g., power grids, telecommunications, nuclear power plants, airports, major highways, and railroads).

Management should determine the potential severity of threats and estimate the disruption's impact under various threat scenarios as it assesses the likelihood and impact of a disruption. The results may be scored quantitatively (e.g., based on a numerical ranking) or qualitatively (e.g., high, medium, and low) and then prioritized. Refer to the *IT Handbook's* "Management" booklet for additional information.

Once management identifies scenarios, it should evaluate specific threats to the entity's controls, strategies, and plans. The difference, or the gap, between the risks from likely foreseeable threats and the mitigation provided by current controls, represents the risk exposure. Management should develop strategies to manage risk, which could include risk mitigation, avoidance, acceptance, or risk transfer, based on the entity's risk appetite.

IV Business Continuity Strategies

Action Summary

The board and senior management should develop effective strategies to meet resilience and recovery objectives. Effective oversight generally includes guidelines to achieve defined business continuity objectives.

Examiners should review BCM strategies and determine whether the strategies:

- Address personnel, processes, technology, and facility issues.
- Address critical business risks in the operating environment (e.g., mitigate specific or unique threats, such as cyber threats or loss of critical third-party service providers).
- Outline a combination of backup, replication, and storage methods for data protection.
- Provide for high redundancy levels in the telecommunications infrastructure.
- Detail a consistent change management process throughout the entity.
- Include alternatives for any proprietary systems.
- Include provisions for appropriate international business activities, where applicable.

Business continuity strategies are developed after the BIA and risk assessment process. These strategies should be risk-based and address all foreseeable risks, including non-technology risks (e.g., transaction and liquidity). Strategies should include allocation of resources to meet resilience and recovery objectives. Strategies should be validated to confirm that they are viable and sufficient for peak work volumes. For example, the increased reliance on and interconnectivity of technology makes it less feasible for many entities to operate manually for an extended period, if at all.

Strategies should include the potential impact to personnel, processes, technology, facilities, and data. Personnel-related strategies may include logistical arrangements to transport or house staff at alternate facilities. In addition, management may establish alternate methods for communicating with employees, customers, and external parties. Process-related strategies may include redundant work sites for business-line operations or manual processes. Technology-related strategies may include fully equipped backup data centers or cloud providers. Backup strategies should include data files, operating systems, and applications and utilities. Facilities-related strategies may include geographic diversity or multiple power sources to reduce single point of failure risk.

Data protection strategies typically include a combination of backup, replication, and storage to achieve different levels of continuity and resilience. For example, it may be appropriate to deploy more automated, scalable solutions, such as data replication to a cloud. Management should develop comprehensive strategies to protect data, such as:

- Integrating operational, continuity, and resilience strategies to protect data based on recovery objectives.
- Designing a process to preserve the integrity and availability of data from threats.
- Monitoring the effectiveness and efficiency of data protection solutions.

Strategies should address critical business risks in the operating environment. Management should consider strategies to mitigate specific or unique threats, such as cyber threats or loss of critical third-party service providers. The specific strategy in response to an event may be different based on the entity's capabilities. Management should determine what alternatives exist for proprietary systems given the significant, unique risks to an entity's business activities. For example, some entities use internally developed assets (e.g., spreadsheets or other tools) that are critical for certain calculations within a business unit, which are often overlooked, including where and how they are stored, during the risk assessment and BIA processes. Furthermore, management should also consider access capabilities for voice and data, mapping technology infrastructure to employee needs, and internal and external capacity (including remote capacity) to determine whether telecommuting strategies are sufficient.

Strategies could include cloud architectures, virtualization, and other technologies. Cloud solutions may provide a cost-effective and high-availability environment. Independent of the strategies selected for architecture and data protection, management should still be responsible for data integrity and overall resilience. Cloud-based disaster recovery services²⁰ may be considered as part of resilience programs. Refer to section [V.C.1, "Data Center Recovery Alternatives,"](#) for additional information.

²⁰ Refer to the FFIEC's statement on [Outsourced Cloud Computing](#).

IV.A Resilience

Action Summary

Management should evaluate whether there are appropriate resources to ensure resilience, including an accessible, off-site repository of software, configuration settings, and related documentation, appropriate backups of data, and off-site infrastructure to operate recovery systems.

Furthermore, management should discuss potential disaster scenarios with the entity's third-party service providers to prepare for an event. Subsequently, management should assess the entity's immediate or short-term space requirements, systems, and personnel capacity to assume or transfer failed operations. Additionally, management should assess critical third-party service providers' susceptibility to simultaneous attacks and verify their resilience capabilities.

Examiners should review the following:

- Appropriateness of resilience practices, including the adequacy of recovery infrastructure and backup processes.
- Integration with disaster recovery services to protect against data destruction.
- Assessment of alternate data communications infrastructure between the entity and critical third-party service providers.
- Evaluation of the entity's susceptibility to multiple threat scenarios in resilience planning, testing, and recovery strategies.
- Designation of emergency personnel, including for critical business process-level employees.

Resilience is “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.”²¹ The business strategy, not technology solutions, should drive resilience. Resilience extends beyond recovery capabilities to incorporate proactive measures for mitigating the risk of a disruptive event in the overall design of operations and processes. Resilience strategies, including maintaining security standards, should extend across the entire business, including outsourced activities. Management should evaluate whether the entity has appropriate resources (e.g., human, financial, time) for resilience. When developing the entity's resilience strategies, management should consider lessons learned from previous events.

²¹ Refer to the Presidential Policy Directive/PPD-21, [Presidential Policy Directive -- Critical Infrastructure Security and Resilience](#) February 12, 2013.

IV.A.1 Physical

Physical resilience is the traditional approach to business continuity and includes IT architecture, infrastructure, facilities, and communications. To avoid the potential for failures after a disruption, management, when possible, should diversify telecommunication lines, establish redundant connections between branches and data centers, create backups, identify multiple power sources, and verify geographic diversity of key entity locations.

IV.A.2 Cyber Resilience

A challenge for cyber resilience is maintaining operations despite ever-changing risks (e.g., malware, data or system destruction and corruption, and communications infrastructure disruption). The sophistication and frequency of cyber attacks increase the potential for disruption and destruction of data and systems. Given the broad and increasing spectrum of cyber threats, resilience measures should be flexible enough to adapt to a diverse range of events. For example, a cyber attack could impact both production and backup facilities simultaneously, potentially rendering both inoperable, whether hosted internally or by a third-party service provider.

In addition, adversaries may initiate a secondary disruption (e.g., the original disruption could be the impact of a hurricane with the secondary disruption being false transactions or accessing sensitive data). Alternatively, adversaries can launch simultaneous attacks (e.g., a distributed denial of service (DDoS) attack combined with a wire transfer compromise). Therefore, management should adhere to established security and privacy policies and processes to comply with applicable regulations, even during disruptive events.

IV.A.3 Data Backup and Replication

Management should maintain data confidentiality, integrity, and availability for all iterations of data, including data backup and replication, not just focused on the production environment. Data backup and re-creation are important to recovering critical business functions in the event of disruptions. Backup files are commonly created electronically and can be mirrored at an off-site location, backed up on removable media, stored temporarily on network servers until rotated off-site, or backed up to a cloud environment. Backups should be readily accessible and adhere to the entity's information security policy.

Management should reassess backup and recovery strategies as the technology and threat environments evolve. For real-time or high-volume systems, it may be appropriate to have advanced duplication and backup methods. These advanced methods, including cloud and mirroring, provide high availability and are detailed in section V.E.1, "Data Center Recovery Alternatives."

Management should maintain an accessible, off-site repository of software, configuration settings, and related documentation. Even standard software configurations can vary from one location to another. Differences could include parameter settings and modifications, security profiles, reporting options, account information, customized software changes, or other options.

Failure to back up software configurations could result in inoperability or could delay recovery. Therefore, a comprehensive backup of critical software is important. Software backups generally consist of the following components:

- Operating systems.
- Applications.
- Utility programs.
- Databases.
- Other critical software identified in the BIA.

Management should establish effective procedures to recover critical networks and systems. Procedures may address the following:

- Backup types (physical or virtual).
- Backup levels (full, incremental, or differential).
- Updates and retention cycle frequencies.
- Software and hardware compatibility reviews.
- Data transmission controls.
- Data repository maintenance.

Refer to the *IT Handbook's* "Operations" booklet for additional information.

Data replication (also referred to as data synchronization or mirroring) is the process of copying data, usually with the objective of maintaining identical data sets in separate locations. Replication is important in any environment for resilience. Furthermore, management should consider integrity controls during replication so that data changes in production, development, and quality assurance environments are applied throughout the network.

Two common data replication processes used for information systems are synchronous and asynchronous. Synchronous replication represents the direct application of the data by applying changes at the same time. In practice, synchronous replication allows data to be transmitted in a continuous stream and minimizes data loss; however, it requires significant communication bandwidth and has limitations on the distance data can be transported due to latency issues. Synchronous replication is typically used for critical business functions where little or no data loss can be tolerated. Conversely, asynchronous replication is the indirect application of data through applying changes to a log before transit. In practice, asynchronous replication allows data to be transmitted in intermittent batches. While asynchronous replication increases the potential for data loss related to the fractions of a second required to transmit the data, this process requires less communication bandwidth and is useful for data transport over longer distances, due to reduced latency issues.

Management should determine the appropriate retention periods for each iteration of data backup. Entities should safeguard against replicating malware and data corruption. This risk is heightened with the use of near real-time data replication systems, as malware can be replicated undetected. Even with diagnostic tools, management could be unaware of an event that causes data integrity issues until well after it happens, as data could appear uncorrupted but later

determined to be inaccurate. Management may determine that the backup of critical data files should be subject to longer retention periods to ensure the ability to recover a backup prior to a corruption event.

Even in situations when the primary and backup facilities are inoperable or corrupted, customers of the entities expect to be able to access their accounts. Entities should develop appropriate cyber resilience processes (e.g., recovery of data and business operations, rebuilding network capabilities and restoring data) that enable restoration of critical services if the institution or its critical service providers fall victim to a destructive cyber attack or similar event. BCM should include the ability to protect offline data backups from destructive malware or other threats that may corrupt production and online backup versions of data. An example of an industry initiative to assist in addressing the resilience of customer account information is Sheltered Harbor.²²

IV.A.4 Personnel

Resilience is dependent upon personnel availability to maintain critical business processes. Personnel could be unavailable or distracted during such events as natural disasters, severe weather events, or pandemics.²³ While any one employee's role may not be designated as mission critical, management should plan for mass absenteeism during an event or disruption. Previous catastrophic events (e.g., Hurricane Katrina²⁴) demonstrate that personnel availability affects timely recovery.

Management should plan for events during which personnel may not be able to access facilities and critical personnel may not be available immediately after the disruption. Public infrastructure and transportation systems may not be operating, and telecommunication systems may be overburdened and unavailable. Therefore, management should consider:

- Staffing and skills needed to operate critical functions related to business continuity.
- Lodging arrangements for displaced employees and their families.
- Basic necessities and services for displaced employees, including water, food, clothing, childcare, transportation, and cash.
- On-site medical support and mobile command centers.
- Secure telecommunication options if employees work from an alternate location.
- Designated emergency personnel, including critical business process-level employees.

²² Sheltered Harbor is a voluntary industry initiative launched in 2015 following a series of cybersecurity simulation exercises between public and private sectors, known as the Hamilton Series. The purpose of the proposed Sheltered Harbor standard is to promote the stability and resiliency of the financial sector and to preserve public confidence in the financial system. The Sheltered Harbor standard proposes a combination of secure data vaulting of critical customer account information with a comprehensive resilience plan to provide customers timely access to their account information and underlying funds during a prolonged systems outage or destructive cyber attack. ([Sheltered Harbor](#)).

²³ Refer to the FFIEC's [FFIEC Highlights Pandemic Preparedness Guidance](#).

²⁴ Refer to the FFIEC's [Lessons Learned From Hurricane Katrina: Preparing Your Institution for a Catastrophic Event](#).

IV.A.5 Third-Party Service Providers

Many entities depend on third-party service providers to perform or support critical operations. A disruption in the delivery of those services can have a direct impact on entities' resilience. A critical failure at a widely used third-party service provider could have large-scale consequences. Management should assess critical third-party service providers' susceptibility to multiple event scenarios and verify such third parties' resilience capabilities. An entity's third-party service provider can be a single point of failure if management has not considered alternative providers or other contingency plans. If an alternative third-party service provider is not readily available, management should consider options to continue business operations and reevaluate resilience options periodically as conditions may change. Resilience planning should be closely coordinated with third-party service providers.

Establishing well-defined expectations with third-party service providers is important to business resilience. Contracts and SLAs with third-party service providers should detail roles and responsibilities of each party to promote resilience. Ongoing monitoring of the entity's third-party service providers helps management identify potential weaknesses in the third-party service provider's resilience that could affect the entity's operations.

Management's review of an entity's third-party service provider's BCM program may include independent audit reports or SOC reports. SOC reports can contain valuable information about the third-party service provider's products and processes. If management relies on SOC reports, it should verify whether business continuity activities are audited, including whether the scope and depth of review are sufficient to allow management to evaluate the third-party service provider's control environment.²⁵ Depending on the scope of the audit testing, additional inquiry and activities may be appropriate to understand the resilience of the third-party service provider.

Management should consider the same risks outlined in their entity's own internal BCP(s) in relation to third-party service providers, as well as:

- Capacity of third-party service provider to meet client recovery objectives in the agreements, relative to other clients' needs.
- Ability to participate in recovery testing with third-party service providers and access to testing results.
- Ability to move outsourced processes either in-house or to another third-party service provider.
- Alternative resource options (e.g., personnel and systems) for when primary services cannot be delivered.
- Data confidentiality, integrity, and availability (e.g., transportability and interoperability).

²⁵ SOC 1 reports cover controls at the third-party service provider that affect financial reporting. Business continuity activities are usually reported in unaudited sections of SOC 1 reports because they often do not have a direct correlation to the preparation of the financial statements, unless an event happened during the audit period. SOC 2 reports cover trust services criteria and include activities such as security, confidentiality, availability, privacy, and integrity. Audit firms typically do not opine on the quality of the business continuity activities, because it is difficult to predict what would happen during an actual event. Activities related to business continuity such as replication, plan development, and testing may be included in SOC 2 reports covering availability.

- Financial capacity to continue meeting contractual obligations.
- Services concentrated in a limited number of third-party service providers.

Business continuity-related provisions found in contracts and SLAs may include the following:

- Time parameter(s) for contracted service(s).
- Appropriate baseline metrics describing management's resilience and recovery expectations (e.g., an incident response metric to ensure timely response to events impacting business continuity and resilience).
- Periodic service reviews to ensure up-to-date agreements with all parties involved.

If operations at a third-party service provider cease, the length of time required to convert to an alternate system would, for most applications, exceed a reasonable RTO. To the extent possible, management should establish plans for the resilience of third-party service providers supporting critical operations.

IV.A.6 Telecommunications

Given the critical nature of telecommunications, management should ensure appropriate redundancy levels in the entity's telecommunications infrastructure. The entity's telecommunications infrastructure may contain single points of failure that are outside the control of a single entity. Management should understand the limitations of the entity's third-party telecommunications providers' infrastructure. For example, multiple carriers may rely on the same telecommunications backbone. Key aspects management should consider in establishing telecommunication redundancy include:

- Identifying and mitigating single points of failure across the entity's infrastructure.
- Developing and maintaining a plan to address an outage in the telecommunications lines with the entity's primary third-party service providers.
- Establishing redundant telecommunications links with each of the entity's third-party service providers through a contractual arrangement, which allows either party to switch its connection to an alternate communication path.
- Reviewing the entity's third-party service providers' plans and determining whether critical services can be restored within acceptable time frames.
- Developing guidelines, commensurate with the entity's size, complexity, and risk profile, to diversify connections to mitigate the risk of a telecommunications failure.
- Assessing the communications technology that bridges the transmission distance between the telecommunications service provider and the entity, sometimes referred to as the "last mile," for single points of failure.
- Monitoring relationships with telecommunications providers to manage risks.
- Inquiring about the physical paths used by telecommunications providers and verifying that system redundancies have been properly implemented.

Communication is critical to the financial services sector and other industries. Therefore, management should consider the following services provided by the federal government. These services give participants priority access to telecommunications during a wide-spread event.

- The Telecommunications Service Priority (TSP)²⁶ program.
- Government Emergency Telecommunications Service (GETS).²⁷
- Wireless Priority Service (WPS),²⁸ which is the wireless complement to GETS.

IV.A.7 Power

The financial industry is dependent on power to run its technology infrastructure and to supply basic necessities to personnel and customers. A long-term power outage can negatively impact an entity's resilience. Management should implement measures to provide electricity in the event of a short-term power disruption. Furthermore, management should develop plans to provide electricity in the event of a long-term power disruption. As part of its short-term and long-term plans, management should consider the following:

- Alternate energy sources (e.g., generators, multiple power grids).
- Fuel requirements, both for fuel on-hand and contracts with suppliers for deliveries during events, and any potential impediments to obtaining fuel.
- Load capacity of generators (e.g., length of time, useful life, level of power supplied).
- Continued maintenance of generators.
- Testing of generators.

IV.A.8 Change Management

Management should implement and align a consistent change management process throughout the entity, making sure to include BCM. As changes are made to production systems and business processes during the normal course of business, recovery systems and documentation at alternate locations should similarly be updated to reflect production and primary system changes.

The change management process should allow for expedient implementation of emergency changes during an event, such as changing an access control list to provide rapid access for

²⁶ Refer to the DHS's "[Telecommunications Service Priority](#)" (TSP) webpage. The TSP program provides service vendors a Federal Communications Commission mandate to prioritize requests by identifying those services critical to national security and emergency preparedness. TSP-designated circuits are recovered first in an emergency. Management may contact the entity's primary federal regulator for information on the TSP program and whether the entity qualifies for a TSP designation. If the entity qualifies, management should integrate the TSP program into the entity's BCP.

²⁷ Refer to the DHS's "[Government Emergency Telecommunications Service](#)" (GETS) webpage. GETS provides "priority access and prioritized processing in the local and long distance segments of the landline networks, greatly increasing the probability of call completion." It is intended to be used in an emergency or crisis situation when the landline network is congested and the probability of completing a normal call is reduced. Management may request GETS cards by submitting an application to the entity's primary federal regulator.

²⁸ Refer to the DHS's "[Wireless Priority Service](#)" webpage.

troubleshooting and analysis. Change tickets and corresponding activity should be reviewed for appropriateness once the event has been resolved. Even during events, changes should still be properly authorized, monitored, and documented. Poorly administered emergency changes can result in further disruption. Additionally, the interrelated nature of systems can compound disruptions to previously unaffected systems. After an emergency event, systems documentation should be updated for any changes made. Change management elements are addressed in more detail in the *IT Handbook's* “Development and Acquisition” and “Operations” booklets.

IV.B Communications

Management should consider, plan for, and prepare multiple mechanisms to communicate with others. For example, when traditional voice communications and telecommunications are impaired or inoperable, management may consider alternative communications systems such as text messaging through employer-provided and personal mobile phones, personal email, and instant messaging. Other common solutions include an inbound hotline number, an informational webpage, or a two-way polling phone system. Regardless of the communication device used, appropriate controls to safeguard customer and other sensitive information should be maintained.

BCM should include communication protocols and contact lists to notify stakeholders. Management should consider the content and process for developing such protocols and templates. Communication protocols should incorporate strategic communications and crisis management approaches in concert with public affairs or external communications (e.g., prepared public/press statements, media response plans, managing social media, etc.). Communication protocols provide customers, third-party service providers, and other external groups a means to communicate when normal channels are inoperable. External groups could include the following:

- Regulatory agencies (federal and states).
- Emergency responders.
- Law enforcement.
- Financial sector trade associations.
- Customers, third-party service providers, and other third parties (e.g., counterparties, clearing and settlement partners, payment system operators).
- Information-sharing entities (e.g., FS-ISAC).

V Business Continuity Plan

Action Summary

Management should develop business continuity plan(s) (BCP) with sufficient detail in relation to the entity's size and complexity. The BCP should address key business needs and incorporate inputs from all business units.

Examiners should review the plan for the following:

- Authorities, responsibilities, and relocation strategies.
- Communications protocols, event management, business continuity, and disaster recovery.
- Liquidity concerns before and during an adverse event.²⁹
- Alternatives for payment systems, facilities and infrastructure, data center(s), and branch relocation during a disaster.

As shown in figure 2, a BCP is an important component of BCM. The BCP documents the practices and procedures for continuing business operations during a disruption. The BCP focuses on critical business functions and varies according to the entity's size and complexity. The BCP includes specific elements, such as incident response, disaster recovery, and crisis management. Smaller entities may have a single BCP that includes these elements whereas large, complex entities may have multiple plans supported by subsidiary components for business functions, locations, or departments. Furthermore, the BCP should be a living document, regularly updated so that it remains current with system enhancements and organizational changes.³⁰

A comprehensive plan describes the authorities, responsibilities, procedures, and relocation strategies. Components of the plan should include:

- Roles, responsibilities, and required skills for entity personnel and third-party service providers.
- Solutions to various types of foreseeable disruptions, including those emanating from cyber threats.
- Escalation thresholds.
- Immediate steps to protect personnel and customers and minimize damage.
- Prioritization and procedures to recover functions, services, and processes.
- Critical information protection (e.g., physical, electronic, hybrid, and use of off-site storage).

²⁹ Refer to NIST SP 800-61, [Computer Security Incident Handling Guide](#).

³⁰ Refer to "BCP Strategy Concept," NIST SP 800-34 Rev. 1, [Contingency Planning Guide for Federal Information Systems](#). NOTE: While this document pertains to federal information systems, the principles are relevant for non-federal information systems.

- Logistical arrangements (e.g., housing, transportation, or food) for personnel at the recovery locations.
- Network equipment, connectivity, and communication needs, including entity-owned and personal mobile devices.
- Personnel at alternate sites, including arrangements for those permanently located at the alternate facility.
- Scope and frequency of testing.
- Resumption of a normalized state for business processes.

Representatives from all business units should contribute to BCP development and implementation. The BCP may be developed and maintained internally or outsourced. In either case, the entity's board and senior management should be responsible for the BCP. Management should verify the third-party service provider's qualifications and expertise when outsourcing BCP development. Management should work with the third-party service provider to design executable and viable strategies. Regardless of its development process, the BCP and supporting documentation should be stored so that it is readily accessible by personnel during adverse events.

V.A Event Management

The BCP may define various situations as events, disruptions, or triggers. An event is an occurrence or change in circumstances that may affect operations. An event can be physical, cyber, or a combination of both. A disruption is either an anticipated or unplanned event that causes operations to degrade or fail for an unacceptable length of time (e.g., a minor or extended power outage, an extended unavailable network, or equipment or facility damage or destruction). A trigger is an event that prompts management's response. Predefined threshold escalation triggers are a key element of a BCP, and responses should be designed to mitigate the impact from adverse events.

The BCP should include event management procedures that detail reasonably foreseeable event types and provide thresholds and responses. Procedures should describe how to report an event to management and the situations that warrant notification to those who address events. Management should consider establishing a team(s)³¹ to address events. Individuals managing the event may change depending on the nature of the event and team member availability. While the team should manage the event and communicate with stakeholders, event monitoring is an entity-wide responsibility (e.g., board, senior management, and other personnel).

Responses may include activities, programs, or systems that protect life and property, meet basic human needs, and preserve the entity's operational capability. Examples of event responses include:

- Switching operations to a backup facility after a software upgrade and subsequent rollback fail.

³¹ Depending on the entity's size and complexity, authority to respond to an event may fall to an individual, a team, or multiple teams. The term "team" is used for purposes of this booklet.

- Rerouting personnel to a safer location or authorizing telecommuting when the local area becomes unsafe.
- Authorizing telecommuting when an event causes disruptions to operations.
- Invoking disaster recovery procedures once management has identified a significant cyber attack.
- Activating emergency response procedures once a hurricane threatens the local region.

V.B Continuity and Recovery

Management should establish protocols for operations continuity and system recovery. The BCP may include:

- Addressing customer service requests during downtime.
- Tracking daily transactions.
- Reconciling general ledger accounts.
- Documenting operational tasks.
- Posting entries after system recovery.
- Maintaining backup records to provide customer account information (e.g., account numbers, customer names, addresses, account status, and account balances).
- Documenting steps for system hardware and software recovery and restart.

When appropriate, procedures should address manual steps for critical functions, such as back-office operations, loan operations, and customer support. Business continuity plans and procedures should be clear, concise, and easy to implement in an emergency,³² such as checklists and step-by-step procedures.

Displaced customers may not have access to their normal identification and personal records. The BCP should include alternate identity verification methods, and management should be alert for fraud or other suspicious activities. Procedures should address fraud identification³³ and suspicious activity reporting³⁴ according to protocols and legal requirements.³⁵

During the recovery phase, management should coordinate access and availability of power and telecommunications systems with various entities. Management should coordinate with the police and fire departments and local and state government agencies to facilitate timely, secure resilience strategies. Management may also coordinate with other federal agencies, such as the

³² Refer to NIST SP 800-34 Rev. 1, [Contingency Planning Guide for Federal Information Systems](#). NOTE: While this document pertains to federal information systems, the principles are relevant for non-federal information systems.

³³ Refer to the Financial Crimes Enforcement Network's (FinCEN) FIN-2006-A001, [Guidance to Financial Institutions Regarding Hurricane-Related Benefit Fraud](#).

³⁴ Refer to FinCEN's FIN-2013-G002, [Administrative Difficulties in Submitting Electronic Reports to FinCEN](#).

³⁵ Refer to 31 CFR 1020.220, [Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks](#).

Federal Emergency Management Agency, depending on the disaster severity. Refer to the *IT Handbook's* "Operations" booklet for additional information.

V.C Facilities and Infrastructure

The BCP should identify alternatives for core operations, facilities, infrastructure systems, suppliers, utilities, interdependent business partners, and key personnel. The backup site may mirror the operational functionality of the primary site. Management should consider site relocation for short-, medium-, and long-term scenarios. When selecting a facility, management should plan for scalability because an event may last for an extended period of time. In addition, management should consider the entity's proximity to police, fire, and medical facilities, and the expected response time frames should be factored into recovery strategies. Management should enlist the assistance of state and local agencies to expedite building permits and inspections for temporary facilities. Management should verify that recovery alternatives can accommodate the services and processing capabilities affecting critical operations, including:

- Core processing.
- Check processing and imaging.
- Commercial cash management.
- Payments.
- Mailing, faxing, and printing.
- Customer identification.

V.C.1 Data Center Recovery Alternatives

Data center recovery alternatives vary for infrastructure, configuration, operational state, and data migration. Management should document the reasons (e.g., cost and service level) for choosing an alternative and why it is appropriate based on the entity's risk profile and complexity. The level of intervention required to activate the alternate sites affects both the cost and duration to resume operations. Recovery alternatives may take several forms, such as fully redundant systems at alternate sites, cloud-based recovery solutions (either internally developed or outsourced), another data center, or a third-party service provider. Data center and alternate site development is complex, and management should consider constraints in the analysis and design process. The primary objectives are for data to be available and remotely accessible. Management should maintain appropriate controls, regardless of solution. Alternative recovery site examples may include:

- **Cold site:** A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The facility is ready to receive computer equipment when personnel move from their main computing location to the backup facility. This facility is usually not considered as the primary recovery option within the financial services industry because of the significant time necessary to install and activate the infrastructure. Comprehensive testing cannot occur until the infrastructure is established.
- **Warm site:** An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in

the event of a significant disruption. The systems are not loaded with the software or data required to resume operations and typically require manual intervention for failover and system reboots to resume critical processes. Therefore, end users may experience some disruption.

- **Hot site:** A fully operational off-site data center equipped with hardware and software used in the event of an information system disruption. Hot site development is complex, and management should consider constraints in the analysis and design process.
- **Mirrored data recovery sites:** Two or more separate, active sites that back up one another with each site independently supporting critical business functions. These sites provide almost immediate resumption capacity and are seamless for end users. Physical distance and its related latency present limitations for data centers that use real-time, data mirroring backup technologies. Similar to a hot site, these sites contain all of the equipment and connectivity capabilities; however, they also have a duplicate copy of the data. This method of high availability is commonly referred to as “Active-Active.”
- **Mobile site:** A site that possesses capabilities between what a warm and a cold site offer and has portable structures equipped with computing equipment available to customers or personnel. Completely activating a mobile site depends on how quickly it can be delivered and backups restored.
- **Colocation facility:** A facility that provides space, power, infrastructure, environmental controls, and telecommunications capabilities for multiple non-related tenants. If management relies on a colocation facility to deliver resources, there is a risk that the capacity at the colocation service provider may not be able to support the entity’s operations during a regional or large-scale event.
- **Reciprocal agreement:** An agreement that allows two entities to back up each other. While these agreements may be cost-effective, they are viable only if there is adequate excess capacity at the reciprocal financial institution and both operate on the same version and configuration of core software. Consideration should be given to security and privacy, as sensitive customer information could be exposed to the staff at the reciprocal financial institution. While these arrangements may be acceptable as a short-term solution, management should not rely on them as a long-term recovery solution.
- **Disaster recovery as a service (DRaaS):** A cloud-computing solution for replicating and hosting infrastructure, applications, and data that provides failover and recovery services.

V.C.2 Branch Relocation

An adverse event may lead management to temporarily limit or cease branch operations or temporarily transfer a branch’s operations to alternate locations. An important BCP component is establishing a physical location where personnel and customers can go to conduct business. For financial institutions, approval by the appropriate regulator may be required to close, relocate, or establish additional branch facilities.³⁶

³⁶ Refer to 12 U.S.C. 1831r-1, “[Notice of Branch Closure](#)”; 64 Fed. Reg. 34844, “[Policy Statement of the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision Concerning Branch Closing](#)”; 12 CFR 303, Subpart C, “[Establishment and Relocation of Domestic Branches and Offices](#)” (FDIC); 12 CFR 208.6, “[Establishment and Maintenance of Branches](#)” (FRB); 12 CFR 5.30, “[Establishment, Acquisition, and Relocation of a Branch of a National Bank](#)”

V.D Payment Systems

The BCP should address alternate arrangements if payment systems fail (e.g., automated teller machines (ATM), funds transfers, electronic banking, remote deposit capture, or mobile capabilities). Alternate solutions may include manual procedures for calling in or faxing wire or automated clearing house requests to correspondent financial institutions. In addition, web-based systems or third-party software may be used to perform transactions. Management should verify that redundant electronic payment systems and equipment (e.g., tokens and routers) are included at recovery sites for activation and that documentation is maintained for timely posting of entries when systems are recovered.

The BCP should also address increased cash demands and moving funds through electronic systems, including internet and mobile banking. Management may consider developing procedures for pre-established withdrawal limits based on the financial institution's relationships with customers. In addition, management should prepare for a potential increase in branch traffic when ATMs are unavailable. Pre-established agreements with various cash delivery services within and outside of the local area should also be considered so that ATMs can meet customer demand when service returns.

V.E Liquidity Considerations

The BCP should detail processes to address potential cash and liquidity needs during adverse events. During a disaster, power and communications systems may fail (e.g., inoperable ATMs or debit and credit card systems), requiring cash to fulfill customer and business needs. Arrangements to help meet liquidity needs may include:

- Emergency borrowing access.
- Alternative cash delivery.
- Procedures to secure, deliver, and distribute cash.
- Temporary purchase authority guidelines.
- Expense reimbursement options for personnel.
- Higher-limit credit cards or separate checking accounts, with designated individuals who can sign checks in emergency situations.

V.F Other Components

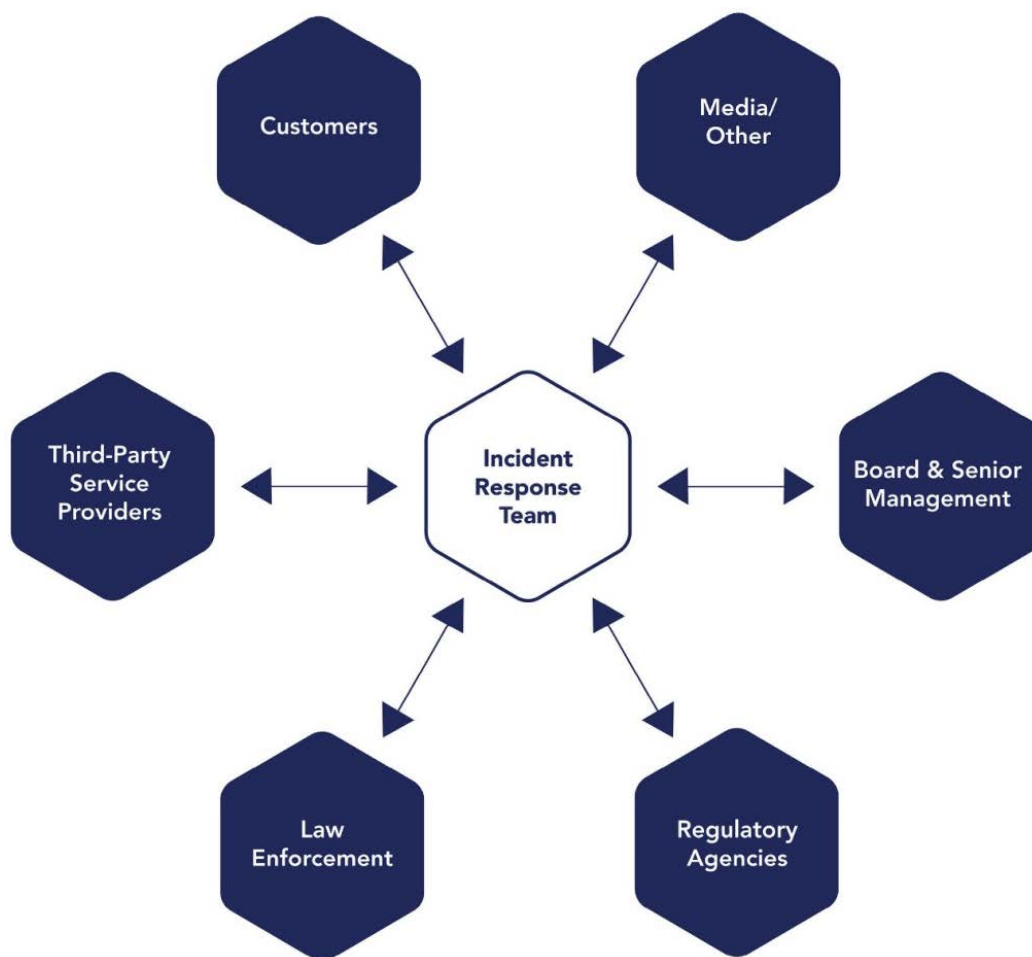
The BCP focuses on sustaining business processes during and after an event. The BCP may incorporate other plans and procedures to minimize a disruption's impact. Components may include incident response, disaster recovery, and crisis or emergency management.

(OCC); and 12 CFR 5.31, "[Establishment, Acquisition, and Relocation of a Branch and Establishment of an Agency Office of a Federal Savings Association](#)" (OCC).

V.F.1 Incident Response

Incident response helps management minimize the disruption of services or loss of information from an adverse event. Incident response priorities include preservation of life, preservation of property, incident stabilization, and communicating with stakeholders (e.g., impacted personnel, third-party service providers, customers, regulators, law enforcement). As shown in figure 4, the incident response team should coordinate communication with the noted stakeholders. Management should align incident response procedures with other related processes (e.g., cybersecurity, network operations, and physical security), outsourced services (e.g., contracted incident response obligations), and verify that the procedures are considered during planning and BCP development.

Figure 4: Incident Response Team (Adapted From NIST SP 800-61, Rev. 2)



Management should designate a spokesperson(s) to communicate with the news media. Management should consider various, pre-planned response scenarios approved by the board and senior management. Communication with the news media and via social media may be important for disseminating accurate information. Social media monitoring during an event can help management resolve conflicting messages and proactively respond to issues and concerns.

Management should train personnel to adhere to the plan when approached by the news media or communicating via social media.

Furthermore, management should leverage routine processes (e.g., vulnerability management and network monitoring) to anticipate potential incidents, including cyber incidents, and coordinate incident response planning with any third-party service provider plans. Furthermore, management should consider prearranging third-party forensic and incident response services. Management should periodically update and test the entity's incident response program to verify that it functions as intended, given rapidly changing threats. Refer to the *IT Handbook's* "Information Security" booklet for additional information.

V.F.2 Disaster Recovery

Disaster recovery is the restoring of IT infrastructure, data, and systems. Management should identify key business processes and activities to be maintained while IT systems and applications are unavailable and prioritize the order in which these systems are restored, which should be reflected in the BIA. In addition, management should develop a coordinated strategy for the recovery of data centers, networks, servers, storage, service monitoring, user support, and related software.

Recovery plans should address a broad range of adverse events (e.g., natural disasters, infrastructure failures, technology failures, unavailability of staff, or cyber attacks). Disaster recovery should address guidelines for returning operations back to a normalized state with minimum disruption.

Disaster recovery should also address the following:

- Security controls and protocols, including physical and logical, for implementation and operation of recovery systems.
- Procedures for restoring backlogged activity or lost transactions to identify how transaction records will be brought current within expected recovery time frames.
- Instructions to access critical information repositories and other resources when the primary facility is unavailable.

When developing disaster recovery plans, management should exercise caution when identifying critical and non-critical systems. For example, telephone banking, internet banking, or ATMs may not seem critical when systems are operating normally; however, these systems play a critical role in delivering services to customers during a disruption. Similarly, an email system may not appear critical but may be the primary system available for communication during an adverse event.

V.F.3 Crisis or Emergency Management

Crisis or emergency management³⁷ is the process that allows the recognition of a crisis, activation of a BCP, and management of emergencies. Crisis or emergency management includes the ability to recover from a major event through predefined leadership and communication. Not every event warrants a crisis or emergency management response. Management should consider the impact of a crisis or emergency on the entity and personnel. For example, management may invoke crisis or emergency response procedures during a natural disaster, cyber attack, or other high-profile event.

The crisis or emergency management portion of the BCP should address coordination with regulatory agencies, local and state officials, law enforcement, and first responders. Scenarios should detail disruptions, and not be confined to a single event, facility, or geographic area. Also, crisis or emergency management plans should address simultaneous disruptions of telecommunications and electronic messaging, including between the entity and third-party service providers.

Management should designate key personnel from applicable departments to act during a crisis or emergency situation, commensurate with the entity's size and complexity. Designated personnel should be authorized to make decisions in a timely manner. Key personnel may include:

- Senior management for leadership.
- Facilities management for safety and physical security.
- Human resources for personnel issues, travel, and relocation.
- Media relations for managing communications.
- Finance and accounting for funds disbursement and financial decisions, including unanticipated expenses.
- Legal and compliance for legal and regulatory concerns.
- IT, including information security, and operations for specific tactical responses.

Communication protocols for a crisis or emergency event should include contact lists and other viable methods to reach personnel and other stakeholders who may be called upon during a crisis. The contact list should be distributed and accessible to key personnel and should be verified and updated regularly. Management should be able to communicate with personnel located in isolated areas or dispersed across multiple locations. Procedures should enable employees to report their status in a centralized manner and obtain current information. Crisis or emergency management communication protocols should include provisions to contact the entity when normal communication channels are inoperable.

Notification systems can be manual or automated. In less complex environments, manual communication techniques, such as call trees, are often used; however, information gathering can

³⁷ The financial services industry uses the terms "crisis management" and "emergency management" interchangeably.

be time consuming, and responses can be unreliable in a crisis. Maintaining contact information can become unwieldy for large entities; therefore, automated solutions may be used.

VI Training

Action Summary

Management should implement a business continuity training program for all stakeholders.

Examiners should review for the following:

- Objectives of business continuity training.
- Alignment of business continuity training with strategies.
- Extent of targeted business continuity training provided to stakeholders, such as personnel, business continuity program staff, and the board.
- Format of the business continuity training program.
- Process for reviewing and updating the business continuity training program.

Management should include training as part of an effective business continuity program to educate stakeholders on resilience, business continuity goals, corporate-wide objectives, policies, and individual personnel roles and responsibilities. The board or senior management delegates a committee or individual to oversee the training program; however, the board should be responsible for the training program's effectiveness. Refer to the *IT Handbook's* "Management" booklet for additional information.

The training program should align with the entity's strategy and use a comprehensive, risk-based, multi-year approach, including interrelated programs (e.g., disaster recovery and third-party risk management). The frequency of exercises should depend on the size and complexity of the entity and the elements of the training program, risks, and testing program iteration, with all elements covered in a timely manner. Management should take inventory of the current skill sets for business continuity and identify and address any gaps. When appropriate, management should establish goals and objectives for supporting the entity's business continuity program as part of the performance management process. Some elements of the training program may include:

- Exercises.
- Current risks.
- Future risks.
- Recent failures.
- New programs/technologies.
- Organizational changes.
- Previous (exercise) lessons learned.

Training generally involves a conceptual understanding of business continuity, including testing methods, test results, and critical business functions. The training program should include conditions for activating the BCP and what to do when key personnel are unavailable. Training should selectively and purposely seek to validate plans and assumptions by testing the interactions of people, processes, and technology risks and vulnerabilities in a consequence-free exercise environment.

Training should be tailored to the target audience, addressing the needs of specific groups. Training participants should include the board, senior management, business process owners, and frontline personnel. For example, training for personnel who manage the business continuity program should be different than training for personnel not directly involved in recovery operations. Training should include significant business continuity concepts, interdependencies, disruption impacts, and operational resilience. When applicable, contractors involved with the business continuity program should also receive appropriate training.

The board should understand the business continuity program, testing initiatives, and key business continuity-related reports. Board training should occur regularly, or more frequently, based on significant changes to business processes, risks, BIA results, or lessons learned from incidents that have impacted the entity. Training methods may involve instructional classes, computer-based training, hands-on experience, lessons learned, and collaborating with other organizations. Role-based training includes cross-training personnel to compensate for significant absenteeism or operational disruptions, which may occur during an event. Training should reflect changes to the business continuity program as they occur.

VII Exercises and Tests

Action Summary

The board and senior management should provide for appropriate exercises and tests to verify that business continuity procedures support business continuity objectives. Exercises and tests should be used to validate one or more aspects of the entity's BCP.

Examiners should review for the following in exercise and testing plans:

- Provisions for exercises and tests occurring at appropriate intervals and when significant changes affect the entity's operating environment.
- Comprehensive program objectives and plans of exercises and tests to validate the ability to restore critical business functions in a timely manner.
- An exercise and test process that provides assurance for the continuity and resilience of critical business functions, without compromising production environments.
- Authorities and control over exercises and tests.
- Exercise and test policies, expectations, and strategies that demonstrate the entity's ability to utilize alternate facilities.
- Exercise and test objectives for resilience, system monitoring, and the recovery of business processes and critical system components.
- Exercise and test scenarios, including exercise and test assumptions, objectives, expectations, and assessment metrics.
- Types of exercises (e.g., full scale, limited scale, or tabletop) and tests.
- Exercises and tests related to interaction with third parties, industry-wide testing, and core and significant firms.
- Documentation of issues identified through exercises and tests, and action plans and target dates for resolution.
- Board expectations for overall business continuity capabilities, including guidelines to achieve defined business continuity objectives.

Exercises and tests³⁸ help ensure that business continuity procedures support business continuity objectives. An exercise is a task or activity involving people and processes that is designed to validate one or more aspects of the BCP or related procedures. There are many different types of exercises, depending on the intended goals and objectives. Exercises may include scenario-driven simulations of BCP elements. For example, exercises may include performing duties in a simulated environment (i.e., functional) or be discussion based (i.e., tabletop).

A test is a type of exercise intended to verify the quality, performance, or reliability of system resilience in an operational environment. Tests are evaluation tools that use quantifiable metrics to validate the operability of an IT system or system component in an operational environment

³⁸ For purposes of this booklet, the term "exercise" represents both exercises and tests, unless the term "test" is specifically mentioned.

(e.g., what happens as a result of removing power from a system or system component). Tests may focus on backup and recovery options of systems. The degree of testing can vary, from individual system components up to comprehensive tests of all system components that support business operations. Effectively, the distinction between the two is that exercises address people, processes, and systems whereas tests address specific aspects of a system.

VII.A Exercise and Test Program

Management should develop a comprehensive exercise and testing program including objectives, and plans to validate the entity's ability to restore critical business functions. The entity's risk profile should influence the frequency, objectives, and documentation of the overall exercise schedule. The entity's consolidated exercise and test schedule should be reflective of exercise and test objectives and the overall exercise and test universe.³⁹

Management should designate personnel with the authority to control the exercise or test and confirm milestones are met. Business line management should retain ownership and accountability for testing resilience of business operations, including applications and processes (both internal and external). While business line management should be responsible for testing its specific business processes and related interdependencies, managers should coordinate with personnel involved in the enterprise-wide business continuity process and support areas, such as IT and facilities management. Results should be reported to the board and senior management for inclusion in the enterprise-wide business continuity process.

Exercises and tests should occur either at appropriate intervals, when new risks are identified, or when significant changes affect the entity's operating environment. Significant changes can render existing test plans obsolete, so BCP(s) should be retested soon after the change. A comprehensive program allows management to evaluate business interdependencies and improve continuity and resilience.

A key objective for management should be to develop a testing process that validates the effectiveness of the entity's business continuity program, and identifies any deficiencies that may exist. Therefore, the exercise and test program should incorporate the following:

- A policy that includes strategies and expectations for exercise and test planning.
- Roles and responsibilities for implementation.
- Sufficient personnel to perform the exercise or test, provide oversight, and document the results.
- Precautions to safeguard production data, such as performing a backup before performing a test in a test environment, or testing during non-peak hours.
- Provisions for emergency stops (i.e., management's authority to stop an exercise if a real-life event occurs) and concluding exercises and tests.

³⁹ Similar to an audit universe, an entity's exercise and test universe is composed of an inventory of all business processes and system components that are compiled and maintained to identify areas for the exercise and test planning process.

- Verification of continuity and resilience process assumptions and the ability to process a sufficient volume of work during adverse operating conditions.
- Activities commensurate with the importance of the business process, as well as to critical financial markets.
- Result comparison against the BCP to identify gaps between the exercise or test process and recovery guidelines, with revisions incorporated where appropriate.
- Independent review of business continuity program and exercises and tests (internal and external).

VII.B Exercise and Test Policy

The entity's policies should define exercise and testing expectations and strategies. The policies should:

- Identify key roles and responsibilities.
- Establish minimum frequency, scope, and reporting requirements.
- Define documentation expectations that are consistent across business processes.
- Include a process for correcting deficiencies identified during exercises or tests.
- Address testing of communication and connectivity between the entity and third-party service providers.
- Detail participation with critical third-party service providers to confirm that entity personnel understand integration with recovery processes.

VII.C Exercise and Test Strategies

Management should develop exercise and testing strategies that demonstrate the entity's ability to support connectivity, functionality, volume, and capacity using alternate facilities. The strategies should include expectations for individual business lines and use of exercise and testing methodologies and scenarios. Testing strategies should encompass internal and external dependencies, including activities outsourced to domestic and foreign-based third-party service providers. Management should test all aspects of the entity's BCP. Strategies may include:

- A multi-year plan to execute the specific depth and breadth of exercises and tests to identify gaps in the program by using different methodologies and scenarios over time.
- Expectations for testing internal and external recovery dependencies.
- Assumptions, methodologies, and exercises used to develop the test strategies.

Lessons learned from natural disasters and other events show that for critical business functions, testing strategies should include transaction processing and functional testing to assess the recoverability of infrastructure, capacity, and data integrity. Regardless of the recovery strategy used, management should regularly test recovery provisions commensurate with the risk to the entity and, where applicable, the overall financial service sector.

VII.D Exercise and Test Objectives

The exercise and testing objectives should include resilience, system monitoring, and the recovery of business processes and critical system components. Tests can range from recovering a single file to a full-scale failover to another data center. Tests should include physical security, critical systems, multiple departments, and third-party relationships. Exercises should be sufficiently thorough to test dependencies and interrelationships among systems and third-party service providers. As the exercise and test process matures, it should become increasingly complex up to and including full-scale recovery exercises. Exercises and any associated tests should accomplish the following objectives:

- Build confidence that resilience and recovery strategies meet business requirements.
- Demonstrate that critical services can be recovered within agreed upon recovery objectives (RTOs and RPOs), including customer SLAs, and within MTDs.
- Establish that critical services can be restored in the event of an incident at the recovery location.
- Familiarize staff with recovery processes.
- Verify that personnel are adequately trained and knowledgeable of recovery plans and procedures.
- Confirm exercise and test plans remain compatible with the BCP and the entity's infrastructure.
- Identify gaps and deficiencies.

VII.E Exercise and Test Plans

Plans address the objectives and expectations of the exercise or test and outline the scenario and any assumptions or constraints that may exist. Exercises and test plans should include metrics to assess whether objectives are met. Plans should identify roles and responsibilities for participants, support personnel, and observers.⁴⁰ Exercise and test plans should be commensurate with the nature, scale, and complexity of the recovery objectives.

Management should receive and review third-party service provider exercise results, regardless of the entity's extent of participation. Management should consider the scope and results of these exercises in the entity's BCP. Management should evaluate third-party service providers' resilience and ability to recover critical services used by the entity if an event occurs. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for additional information.

Test plans generally include the following:

- Roles and responsibilities for all test participants, including support personnel.
- A consolidated exercise and test schedule that encompasses all objectives.
- A specific description of objectives and methods.
- Identification of decision makers and succession plans.

⁴⁰ For the purposes of this booklet, the term "observers" does not constitute an independent review or audit function.

- Exercise and test locations.
- Exercise and test escalation procedures and the ability to adjust for simulated scenarios.
- Contact information.
- Metrics to measure the success or failure of the exercise or test.

Management should review the exercise and test results, update the BCP where appropriate, and report the results to the board or board-designated committee. Suggestions for improving test scenarios, plans, or scripts provided by test participants should be incorporated into the testing cycle, where appropriate.

VII.F Exercise and Test Scenarios

Management should develop realistic exercise and test scenarios, based on risks, which simulate disruptions in business functions and help management determine the ability to meet both business requirements and customer expectations. The goal should not be to execute “perfect” exercises without issues; instead, it should be to continuously strengthen the business continuity program and validate the BCP(s). Management should identify and document assumptions used in developing each scenario. The scenarios should include threats that could affect third-party service providers and others, such as significant business partners. Exercises and tests should include communication processes with applicable stakeholders. Exercises demonstrate not only the ability to failover to an alternate site but also validate recovery objectives. Management should consider all reasonably foreseeable risks to connectivity and service-level agreements between the entity’s facility(ies), third-party service provider facilities, and with any applicable counterparties (i.e., entities on the other side of a financial transaction) with whom they transact significant or critical business.

Scenarios may include:

- Simultaneous attacks affecting both the entity and a third-party service provider.
- Cyber-related events (e.g., isolated malware attack, DDoS attack, data corruption, or a full-scale data center outage).
- Use of mirrored sites to demonstrate that alternate sites can effectively support customer-specific requirements, work volumes, and site-specific business processes.
- Processing a full day’s work at peak volumes.

To the extent possible, scenarios should include only resources that would be available during an event (e.g., backup files or equipment at the alternate site). Considering data and systems helps management verify the integrity of data backups (including access to encrypted data) and the adequacy of off-site systems and supplies, such as workstations and procedure manuals.

Management should develop exercise and test scripts to guide participants and meet objectives. Each script should document the procedures, which may include:

- Applications, business processes, systems, or facilities reviewed.
- Sequential steps for employees or external parties to perform.

- Procedures to guide manual work-around processes.
- A detailed schedule for completion.
- Methods for participants to record results, quantifiable metrics, and any issues.

VII.G Exercise and Test Methods

Exercises and tests help management validate continuity and resilience of technology components, including systems, networks, applications, and data, that support critical business functions. The type or combination of methods should be determined by the entity's size and complexity and the nature of its business. The DHS offers assistance and examples of testing methods,⁴¹ which are available to all entities and may be helpful when developing exercises and tests. Rigorous exercise methods and increased frequency help provide greater confidence in the continuity and resilience of business functions. While comprehensive exercises involve greater investments of time, resources, and coordination, the benefit is a more accurate assessment of recovery capabilities if a disaster occurs. This assists management in assessing the resilience of systems and responsiveness of the individuals involved in the recovery process. Comprehensive testing of all critical functions and applications allows management to identify potential problems; therefore, management should use one of the more thorough testing methods discussed in this section to verify the BCP's viability.

While names for exercises and tests may be different, or used interchangeably, this booklet lists the most commonly encountered elements in the following subsections.

VII.G.1 Full-Scale Exercise

Full-scale exercises (sometimes called a full interruption or comprehensive exercise) help management validate internal and external interdependencies between critical business functions, information systems, and networks (e.g., for critical functions, exercises should include transaction processing and functional testing). Integrated exercises move beyond comprehensive exercises to include testing with internal and external parties and the supporting systems, processes, and resources. Management should periodically reassess and update exercise and test plans to reflect changes in the business and operating environment.

A full-scale exercise simulates full use of available resources (personnel and systems) prompting a full recovery of business processes. The goal of a full-scale exercise is to determine whether all critical systems can be recovered at the alternate processing site and whether personnel can implement the procedures defined in the BCP. For example, a full-recovery exercise might simulate the complete loss of primary facilities. Features of a full-scale exercise may include the following:

⁴¹ As members of an established sector of critical infrastructure, financial institutions can leverage testing constructs implemented by the DHS. The Homeland Security Exercise and Evaluation Program is the DHS policy and guidance for designing, developing, conducting, and evaluating exercises. The program provides a threat- and performance-based exercise process that includes a mix and range of exercise activities through a series of four reference manuals to establish exercise programs and design, develop, conduct, and evaluate exercises.

- Engaging personnel from all business units to participate and interact with internal and external management response teams.
- Validating the crisis or emergency management process is operating as designed.
- Verifying personnel knowledge and skills.
- Validating management response and decision-making capability.
- Coordinating participants and decision makers.
- Validating communication protocols.
- Conducting activities at alternate locations or facilities.
- Processing data using backup media or alternative methods.
- Completing actual transactional volumes or an illustrative subset.
- Performing recovery exercises over a sufficient length of time to allow issues to unfold as they would in a crisis.

VII.G.2 Limited-Scale Exercise

A limited-scale exercise is a simulation involving applicable resources (personnel and systems) to recover targeted business processes. The goal of a limited-scale exercise is to determine whether targeted systems can be recovered and whether personnel understand their responsibilities as defined in the plan. Features of a limited-scale exercise may include the following:

- Implementing a plan appropriate to the scenario.
- Verifying personnel knowledge and skills.
- Validating management response and decision-making capability.
- Executing on-the-scene coordination and decision-making roles.
- Verifying whether participants can connect to alternate system(s).
- Conducting activities at alternate locations or facilities.
- Testing communication and remote access capability (e.g., switching to alternate equipment or telecommuting).

While limited-scope exercises are important, they often have limited participation (e.g., departmental personnel only) or scope and do not necessarily allow management to gauge interconnectivity and how systems and capacity would support daily activities and workloads.

VII.G.3 Tabletop Exercise

A tabletop exercise (sometimes referred to as a walk-through) is a discussion during which personnel review their BCP-defined roles and discuss their responses during an adverse event simulation. The goal of a tabletop exercise is to determine whether targeted plans and procedures are reasonable, personnel understand their responsibilities, and different departmental or business unit plans are compatible with each other. By themselves, tabletop exercises are likely insufficient to validate recovery capabilities, because they are limited to a discussion-based analysis of policies and procedures.

Features of a tabletop exercise may include the following:

- Engaging operational and support personnel who are responsible for implementing the BCP.
- Practicing and validating specific functional response capabilities.
- Demonstrating knowledge, skills, team interaction, and decision-making capabilities.
- Role playing with simulated responses, critical steps, recognizing difficulties, and resolving problems.
- Clarifying critical plan elements, as well as problems noted during exercises.
- Creating action plans to correct issues.

VII.G.4 Tests

Management uses tests to verify the quantifiable performance and reliability of system resilience. The goal of testing is to determine whether system resilience conforms to the BCP and stated recovery objectives. Test methodologies and frequencies should align with the risk associated with the business function as well as the entity's testing strategies and objectives. Management should clearly define the characteristics of a successful test, which may include the following:

- Validating RPOs, RTOs, and MTDs.
- Demonstrating recoverability at peak volumes.
- Confirming that systems can support critical business processes (e.g., transfer to alternate sites, increased workloads, manual workarounds, and communication).
- Integrating technologies that support critical business activities, including data replication, recovery, and off-site storage.
- Testing backup data to assess integrity and availability.
- Certifying facility controls (e.g., environmental, backup power, and physical security).
- Verifying workspace restoration (e.g., network connectivity and communications).

VII.H Industry Exercises and Resilience

Given the potential for and nature of widespread and systemic disruptive events, public and private sector groups⁴² conduct exercises with their members to verify resilience across the financial industry. These exercises simulate significant regional or industry-wide emergencies, and members are encouraged to use backup sites and test their recovery capabilities. In addition to financial institutions, these coordinated tests often include participation by third-party service providers and government agencies. There are several methods for entities of all sizes to participate, such as through third-party service provider user groups or industry initiatives. For example, industry initiatives include the U.S. Department of the Treasury's Hamilton Series (national and regional series) and the FS-ISAC's Cyber-Attack Against Payment Systems (CAPS). The results of these exercises are usually available to members of industry and regulatory groups, and summaries may be available to the public.

⁴² Public and private groups include the [FS-ISAC](#), [Financial Services Sector Coordinating Council \(FSSCC\)](#), [Financial Systemic Analysis & Resilience Center \(FSARC\)](#), [Financial and Banking Information Infrastructure Committee \(FBIIC\)](#), and some regional coalitions.

Examiners should understand that opportunities to participate in such exercises may be limited. The *Financial Sector Cyber Exercise Template*⁴³ is publicly available from the U.S. Department of the Treasury, and management can use it to help verify the entity's own response capabilities and evaluate how it would respond during similar situations. Additionally, the template and results may be used as resources to validate exercise and testing assumptions and scenarios.

VII.I Third-Party Service Provider Testing

Third-party service providers deliver critical services to many entities and should be included in the enterprise-wide exercise and testing program. The extent of inclusion in the entity's program should be based on the criticality of the third-party service provider and the business function. Management should obtain assurance that third-party service providers are resilient and have adequate infrastructure and personnel to restore critical services consistent with business and contractual requirements. The right to perform or participate in testing with third-party service providers should be included in the contract governing the entity's relationship with the third party.

Management should actively participate in the entity's third-party service providers' testing programs and should verify that testing strategies include likely significant disruptive events. Third-party service providers should be transparent about testing parameters and results because not all clients can participate in every testing activity (e.g., when there is a large client volume) and some exercises and tests may not be relevant to the services provided to a specific customer. Management should request and receive test results and reports, remediation action plans and status reports upon their completion, and related analysis or modeling. Management should track and resolve any issues identified during the exercise in a timely manner, according to the severity of the issues. Any test results that affect the entity should be presented to its board. In most instances, equating one entity's recovery experience with another's does not guarantee similar results; therefore, management should perform its own analysis. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for additional information.

VII.J Testing for Core and Significant Firms

Management at core and significant firms should develop verification strategies and execute exercise and testing activities to validate that the entity implemented sound recovery practices consistent with the entity's role in the industry. Additionally, management should consider the impact of an event at its entity on the entire financial sector. The elements discussed in the *Sound Practices Paper* supplement the agencies' respective policies and other guidance on business continuity planning. Entities not designated as core and significant firms may also consider guidance from the *Sound Practices Paper* as a model for enhancing their testing processes.

Identification of external interdependencies is important given the sector's reliance on core and significant firms. Internal testing activities should include systems that support critical market activities in which these firms are core or significant. Exercise and testing activities should confirm that such critical clearing and settlement activities could be recovered within RTOs.

⁴³ Refer to the U.S. Department of the Treasury's [Financial Sector Cyber Exercise Template](#).

Industry standard time frames are continually adjusted based on available technology, pertinent risks, and industry initiatives. Management should adjust its RTOs to be in line with industry standard time frames. Furthermore, management should design testing activities to demonstrate the ability to perform the following activities if a wide-scale disruption affects the accessibility of key personnel:

- Complete pending material payments and transactions.
- Access funding.
- Manage material open risk positions.
- Make related entries to books and records.
- Validate internal and external communication protocols.
- Ensure connectivity, functionality, and volume capacity.

Management should test with the relevant core firms from their alternate sites and meet testing standards the core firms establish specifically for significant firms and for participants more generally. Management at core and significant firms should perform testing to assess the effectiveness of their recovery strategies. Management is also encouraged, to the extent practical, to participate in pertinent market-wide and cross-market tests⁴⁴ that validate connectivity from alternate sites and include transaction, settlement, and payment processes.

Examination and supervisory activities may include evaluations of verification strategies and testing plans to assess whether core and significant firms, which are the focus of the *Sound Practices Paper*, have achieved the resilience to protect the financial system from a wide-scale disruption.

VII.K Post-Exercise and Post-Test Actions

Management should document issues identified during exercises and tests and create action plans with target dates for resolving issues. Exercise and test results should be analyzed and compared with the objectives and success criteria in the exercise and test plans, and reported to appropriate levels of management. For those items not remediated, management should document decisions to accept risks identified during the exercises.

Additionally, management should test corrective actions implemented as a result of a failed recovery objective or to address major issues encountered. Management may choose to retest during or before the next regularly scheduled exercise depending on an issue's severity. Business line management should update the BCP based on test results and adjust the BCM process, including the exercise and testing program. Finally, management should submit regular reports to the board on the exercise and testing activities and whether the BCP meets the entity's recovery and resilience objectives.

Exercise and test results may include the following documentation:

⁴⁴ Industry and cross-market tests are often conducted by associations such as the Securities Industry Association, Bond Market Association, and Futures Industry Association. These associations are mentioned for illustrative purposes only; this note is not an endorsement of any of these associations.

- Dates and locations.
- An executive summary comparing objectives and results.
- Material deviations from the plans, including whether intended participation was achieved.
- Problems identified and lessons learned.
- Assignment of responsibility for timely resolution of issues identified.

Management should periodically analyze results and issues to determine whether problems can be traced to a common source, such as inadequate change control procedures. Fixing the root cause of the problem may help resolve many underlying issues.

VIII Maintenance and Improvement

Because risks and technology often change, management should regularly review and update the business continuity program to reflect the current environment. Periodic reviews allow management to align the business continuity processes with business objectives. Management should use this information to prioritize and focus on system and process corrections and enhancements. Triggers that prompt maintenance and improvement of the business continuity program may include the following:

- Changes in enterprise strategies.
- New or reconfigured products, services, or infrastructure.
- Changes in products and services offered by third-party service providers.
- Deficiencies identified in third-party service provider business continuity processes.
- New legislation, regulatory requirements, or resilience practices.
- Results of operational metric analysis (e.g., key risk indications, key performance indicators).
- Early warning indicators that may identify potential continuity events, crises, or incidents (e.g., frequency and severity of storms, increased cyber attacks, or increases in customer service calls).
- Variances between budgeted and actual business continuity expenses.
- Results from exercises and tests, and lessons learned.
- Changes in the threat landscape (e.g., new capabilities, intent of threat actors).
- Recommendations (e.g., from audits, vulnerability assessments, and penetration tests).

To determine the extent of changes to the business continuity program, BCM program personnel should contact business unit managers regularly to assess the nature of any changes to the business, structure, systems, software, hardware, personnel, or facilities. Management at smaller, less complex entities may perform this function informally; however, the maintenance and improvement concepts remain valid for those entities.

The business continuity program should be reviewed for accuracy and completeness at periodic intervals. Likely areas⁴⁵ that should be adjusted within the BCP may include:

⁴⁵ The concept of business continuity program review elements aligns with NIST SP 800-34 Rev. 1, [Contingency Planning Guide for Federal Information Systems](#). While this document pertains to federal information systems, the principles are relevant for non-federal information systems.

- Operational requirements.
- Security requirements.
- Technical procedures.
- Hardware, software, and other equipment.
- Team member contact information.
- Vendor contact information.
- Alternate and off-site facility requirements.
- Vital records.

When updating the business continuity program, management should document, track, and resolve any changes. Management should document, analyze, and review lessons learned from adverse events. Understanding these lessons allows management to prepare for future adverse events. Documented procedures for incorporating lessons learned should include:

- Identifying the failure(s).
- Determining the cause(s).
- Evaluating potential solutions.
- Implementing timely corrective actions as appropriate.
- Recording and reviewing corrective actions taken.

As part of the maintenance and improvement process, management should maintain version control of key business continuity documents and ensure that the latest versions are readily available to appropriate personnel. The level of detail in documentation should be commensurate with the nature of the entity's operations. This information should be accessible during an event and can be maintained by BCM program management and personnel. The BCM documentation should include evidence substantiating periodic updates of the BIA, risk assessment, and BCP(s).

Business continuity document management processes may include the following:

- Roles and responsibilities.
- Document control.
- Version control.
- Storage and disposal.

Management should follow the entity's information security standards for confidential or sensitive information contained within business continuity documentation. Additionally, management should maintain backup copies of relevant business continuity documentation in the event that the primary repository becomes inaccessible.

IX Board Reporting

Action Summary

The board should establish expectations for management's business continuity reporting, regularly monitor business continuity and resilience activities, and provide credible challenges to management.

Examiners should review reports and meeting minutes and conduct discussions with management on the following:

- BIA.
- Risk assessment.
- BCP.
- Resilience.
- Exercise and test results.
- Identified issues.
- Strategy updates.
- Audit results.
- Metrics, including key risk indicators and key performance indicators for BCM and resilience.

As illustrated in figure 1, management should report on the status of business continuity to the board, completing the BCM cycle. Reports should include a written presentation providing the BIA, risk assessment, BCP, exercise and test results, and identified issues. Additionally, reports should include regular strategy updates based on changes in personnel, roles and responsibilities, and business operations. The board should monitor business continuity and resilience activities regularly to verify that they are implemented as envisioned and reviewed periodically or as changes dictate. The board should be updated in a timely manner based on lessons learned. Board minutes should reflect business continuity discussion (including credible challenges) and approvals.

Appendix A: Examination Procedures

Examination Objective

These examination procedures (also known as the work program) are intended to assist examiners in determining the quality and effectiveness of the business continuity process on an enterprise-wide basis or across a particular line of business. Additionally, these procedures assist examiners in evaluating whether business continuity testing demonstrates the entity's ability to meet its business continuity objectives including management's ability to recover, resume, and maintain operations after disruptions, ranging from minor outages to full-scale disasters. Examiners are not limited by the examination procedures presented here and may choose to use only certain components of the work program based on the size, complexity, and nature of the entity's business. Depending on the examination objectives, a line of business can be selected to sample how the entity's continuity planning or testing processes work individually or for a particular business function or process.

Objective 1: Determine the appropriate scope and objectives for the examination.

1. Review past reports for outstanding issues or previous problems. Consider the following:
 - a. Regulatory reports of examination.
 - b. Internal and external audit reports.
 - c. Reports by independent risk management.
 - d. Business continuity tests.
 - e. Regulatory, audit, and business continuity reports on third-party service providers.
2. Review management's response to issues identified during or subsequent to the last examination. Consider the following:
 - a. Adequacy and timing of corrective action.
 - b. Resolution of root causes rather than symptoms.
 - c. Status of uncorrected issues.
 - d. Retesting to validate corrective action.
3. Interview management and review responses to pre-examination information requests to identify changes to technology infrastructure or new products and services that could affect business resilience. Consider the following:
 - a. Products or services delivered to either internal or external users.
 - b. Network topology or diagram, including changes to configuration or components and all internal and external connections.
 - c. Hardware and software inventories.
 - d. Loss, addition, or change in duties of key personnel.
 - e. Third-party service providers and software vendor listings.
 - f. Changes to internal business processes.
 - g. Changes based on industry changes or threat intelligence.

4. Review newly identified threats and vulnerabilities to the continuity of operations. Consider the following:
 - a. Technology and security vulnerabilities.
 - b. Internally identified threats.
 - c. Externally identified threats (e.g., cybersecurity alerts, pandemic alerts, or emergency warnings published by information-sharing organizations and government agencies).

Objective 2: Determine whether the board and senior management promote effective governance of business continuity through defined responsibilities, accountability, and adequate resources to support the program. (II.A, “[Board and Senior Management Responsibilities](#)”)

1. Determine whether business continuity policies and critical business procedures are:
 - a. Up-to-date and reflective of the current business environment.
 - b. Communicated effectively throughout the entity.
 - c. Available during adverse events.
 - d. Securely maintained.
2. Determine whether the board and senior management provide leadership when overseeing business continuity, including:
 - a. Evaluating continuity risk.
 - b. Setting short- and long-term continuity objectives.
 - c. Adopting appropriate policies and procedures.
 - d. Evaluating continuity performance.
 - e. Adjusting programs and operations in response to test results and actual events.
3. Determine whether management strengthens resilience through the following:
 - a. Assessing continuity risk.
 - b. Resilience planning.
 - c. Testing business continuity plans.
 - d. Incorporating lessons learned from testing and events.
 - e. Considering resilience in business functions and the design of existing operations and new products and services.
4. Determine whether board oversight includes the following:
 - a. Assigning business continuity responsibility and accountability.
 - b. Allocating resources to business continuity (e.g., personnel, time, budget, and training).
 - c. Aligning BCM with business strategy and risk appetite.
 - d. Understanding business continuity risks and adopting appropriate policies and plans to manage events.
 - e. Understanding business continuity operating results and performance.

- f. Providing a credible challenge to management responsible for the business continuity process (e.g., the board minutes provide evidence of active discussions).
 - g. Establishing a provision for management intervention if timeliness for corrective action is not met.
5. Determine whether management oversight of business continuity includes the following:
- a. Defining business continuity roles, responsibilities, and succession plans.
 - b. Allocating knowledgeable personnel and sufficient financial resources.
 - c. Validating that personnel understand their business continuity roles.
 - d. Establishing measurable goals against which business continuity performance is assessed.
 - e. Designing and implementing a business continuity exercise strategy.
 - f. Confirming that exercises, tests, and training are comprehensive and consistent with the exercise strategy.
 - g. Resolving weaknesses identified in exercises, tests, and training.
 - h. Meeting regularly to discuss policy changes, testing plans, and training.
 - i. Assessing and updating business continuity strategies and plans to reflect the current business conditions and operating environment for continuous improvement.
 - j. Aligning plans between business units across the enterprise.
 - k. Coordinating plans and responses with external entities.

Objective 3: Determine whether the board and senior management engage audit or other independent review functions to review and validate the design and operating effectiveness of the BCM program. (II.B, “[Audit](#)”)

- 1. Determine whether the board and senior management have engaged audit (or an independent review) to validate the design effectiveness of the business continuity program and whether controls are operating effectively.
- 2. Determine whether audit reports to the board and provides an assessment of management’s ability to manage and control risks related to continuity and resilience.
- 3. Determine whether audit leverages SOC reports and other external artifacts from third-party service providers, as appropriate.
- 4. Determine whether the board or management validates that the auditor is qualified to carry out the review and is independent of the business continuity or related functions.
- 5. Evaluate the audit coverage of business continuity, whether through a general controls audit, during audits of business lines, or as a stand-alone business continuity audit. Audit coverage should include the following:
 - a. The reasonableness and comprehensiveness of the BIA and business continuity risk assessment(s).
 - b. The reliability, adequacy, and effectiveness of continuity and resilience controls.

- c. The effectiveness of risk mitigation efforts.
- d. Whether test plans achieve their stated objectives based on reasonable assumptions.
- e. Audit monitoring of exercises and tests, reviewing test plans and results, and verifying that any issues are identified and appropriately escalated.
- f. Assessment of the business continuity program effectiveness.

Objective 4: *Determine whether management developed an appropriate and repeatable BIA process that identifies all business functions and prioritizes them in order of criticality, analyzes related interdependencies, and assesses a disruption’s impact. (III.A, “[Business Impact Analysis](#)”)*

1. Determine the process through which management inventories business functions. Management may use the following artifacts to identify the functions:
 - a. Organizational charts.
 - b. Work flows (also called process maps).
 - c. Interview notes.
 - d. Network diagrams/topologies.
 - e. Data flow diagrams.
2. Determine whether management inventoried the critical assets and infrastructure upon which business functions depend, including the identification of single points of failure. Critical assets and infrastructure may include the following:
 - a. People.
 - b. Hardware.
 - c. Software.
 - d. Cash reserves.
 - e. Supporting activities (e.g., technology support, payroll, contracting).
 - f. Supporting software (e.g., email, office productivity suites).
 - g. Network connectivity.
 - h. Communication lines.
 - i. Facilities.
 - j. Utilities.
 - k. Infrastructure and services provided by third-party service providers.
3. Determine whether the interdependency analysis includes the following:
 - a. Internal systems and business functions, including services, production processes, hardware, software, and application programming interfaces, data, and vital records.
 - b. Third-party service providers, key suppliers, and business partners.
 - c. Telecommunications single points of failure.
 - d. Power single points of failure.
4. Review the BIA to determine whether the prioritization of business functions is reasonable. Consider management’s ability to do the following:

- a. Determine the operational and financial impacts of a disruption.
 - b. Aggregate loss impacts and determine a rating scale to indicate impact severity.
 - c. Reconcile BIA and risk assessment results with prioritization and document whether the reconciliation is adequate.
5. Determine whether the BIA produces sufficient information to estimate the following:
- a. Recovery point objectives (RPO).
 - b. Recovery time objectives (RTO).
 - c. Maximum tolerable downtime (MTD).

Objective 5: Determine whether management conducts a risk assessment sufficient to evaluate the likelihood and impact of potential disruptions and events. (III.B, “[Risk Assessment](#)”)

1. Review risk assessment(s) to determine whether management has identified all reasonably foreseeable hazards and threats to the continuity and resilience of the entity. Examples of risks can include:
 - a. Natural:
 - Flood, earthquake, hurricane, tornado, and other weather events.
 - b. Technological:
 - Technological: Malware, cyberattack, and hardware and software failure.
 - Operational: Critical infrastructure disruption (e.g., transportation and water systems).
 - c. Adversarial or human-caused:
 - Personnel: Strike, pandemic, and malicious insider.
 - Social: Terrorism, vandalism, looting, riots, and protests.
 - d. Combination:
 - Facility: Fire, power outage, and loss of access.
 - Geographic-related: Proximity to railroad or highways used for transport of hazardous materials, proximity to airports, traffic difficulties, and other issues.
 - Third-party: Services concentrated in a limited number of third-party service providers.
2. Determine whether management identifies BCM risks and coordinates risk identification efforts throughout the entity to identify systemic threats.
 - a. Determine whether management identifies and inventories the following:
 - Internal and external assets.
 - Types of threats and hazards.
 - Existing controls.
 - b. Verify that the risk assessment includes the identification of cybersecurity risks and results of information security risk assessments.
 - c. Assess whether management obtains information about hazards and threats from external sources.
 - d. Determine whether management considers threat intelligence in risk identification efforts.

3. Ascertain whether management identifies interconnectivity points between the entity and its third-party service providers, as well as interconnectivity between other entities and their third-party service providers (i.e., supply chain).
4. Determine whether the risk assessment includes the impact and likelihood of potential disruptive events, including worst-case scenarios.
5. Determine whether management identifies and analyzes gaps between the entity's risk exposure and the risk appetite, and documents any controls implemented to mitigate the residual risk.

Objective 6: Determine whether the entity's risk management strategies are designed to achieve resilience. (IV.A, "[Resilience](#)")

1. Verify that management has evaluated strategies and resource needs and allocates appropriate resources to achieve resilience:
 - a. Appropriate personnel and skillsets to carry out the functions.
 - b. Time to identify and implement solutions.
 - c. Budget to accomplish resilience goals and objectives.
2. Determine whether management has implemented physical resilience measures that:
 - a. Establish redundant communications between branches and data centers.
 - b. Identify multiple power sources.
 - c. Geographically diversify key entity locations.
3. Determine whether management has implemented data and cyber resilience measures that:
 - a. Maintain confidentiality, integrity, and availability for backup, replication, and production environments.
 - b. Implement appropriate backups and sufficient documentation and retention periods for each iteration of data backup.
 - c. Periodically reassess backup and recovery strategies as technology and threats change.
 - d. Maintain an accessible, off-site repository of software, configuration settings, and related documentation.
 - e. Establish procedures to recover critical networks and systems, including:
 - Backup types (physical or virtual).
 - Backup levels (full, incremental, or differential).
 - Update and retention cycle frequencies.
 - Software and hardware compatibility reviews.
 - Data transmission controls.
 - Data repository maintenance.
 - f. Protect offline data backups from destructive malware that may corrupt production and online backup versions of data.

4. Determine whether management documented and implemented, as appropriate, the following resilience measures for personnel:
 - a. Staffing and skills needed to operate critical functions related to business continuity.
 - b. Lodging arrangements for displaced employees and their families.
 - c. Basic necessities and services for displaced employees, including water, food, clothing, childcare, and transportation.
 - d. On-site medical support and mobile command centers.
 - e. Secure telecommunication options if employees work from an alternate location.
 - f. Designated emergency personnel, including critical business process-level employees (i.e., those necessary to ensure all critical business operations function appropriately).
5. Determine whether management documented and implemented, as appropriate, the following resilience measures for third-party service providers:
 - a. Considered disruptive events that threaten the operational resilience and viability of the entity's third-party service provider.
 - b. Assessed the entity's immediate or short-term space, systems, and personnel capacity to assume or transfer failed operations.
 - c. Assessed critical third-party service providers' susceptibility to multiple event scenarios.
 - d. Reviewed third-party service provider's resilience capabilities, including available test and SOC reports.
 - e. Verified that SLAs with third-party service providers align with the entity's recovery objectives.
 - f. Established plans for the resilience of third-party service providers supporting critical operations.
6. Determine whether management documented and implemented, as appropriate, the following resilience measures for telecommunications:
 - a. Identifying and mitigating single points of failure across the entity's infrastructure.
 - b. Developing and maintaining a plan to address an outage in the telecommunications lines with its primary third-party service providers.
 - c. Establishing redundant telecommunications links with each of the entity's third-party service providers through a contractual arrangement that allows either party to switch its connection to an alternate communication path.
 - d. Reviewing the entity's third-party service providers' plans and determining whether critical services can be restored within time frames acceptable to the entity.
 - e. Developing guidelines, commensurate with the entity's size, complexity, and risk profile, to diversify connections to mitigate the risk of a telecommunications failure.
 - f. Assessing the communications technology that bridges the transmission distance between the telecommunications service provider and the entity for single points of failure.
 - g. Monitoring relationships with telecommunications providers to manage risks.
 - h. Evaluating communications and resilience needs to ensure branch communications.

- i. Inquiring about the physical paths used by telecommunications providers and verifying that system redundancies have been properly implemented.
7. Determine whether management considers the following as part of the entity's power resilience strategies:
 - a. Alternate energy sources (e.g., generators and multiple power grids).
 - b. Fuel requirements, both for fuel on-hand and contracts with suppliers for deliveries during events.
 - c. Continued maintenance of generators.
 - d. Testing of generators.
8. Verify that BCM activities align with the entity's change management process.

Objective 7: Determine whether the entity's BCM includes communication protocols. (IV.B, "[Communications](#)")

1. Determine whether management considers, plans for, and prepares multiple mechanisms to communicate with personnel and other stakeholders while maintaining appropriate controls to safeguard customer information. Other stakeholders could include:
 - a. Regulatory agencies (federal and state).
 - b. Emergency responders.
 - c. Law enforcement.
 - d. Financial sector trade associations.
 - e. Information-sharing entities (e.g., FS-ISAC).

Objective 8: Assess the appropriateness of the entity's enterprise-wide BCP. (V, "[Business Continuity Plan](#)")

1. Verify that management implemented a comprehensive BCP that is reflective of the entity's risk environment. The BCP should outline the following:
 - a. Roles, responsibilities, and required skills for entity personnel and third-party service providers.
 - b. Solutions to various types of foreseeable disruptions, including those emanating from cyber threats.
 - c. Escalation thresholds.
 - d. Immediate steps to protect personnel and customers and minimize damage.
 - e. Prioritization and procedures to recover functions, services, and processes.
 - f. Critical information protection (e.g., physical, electronic, hybrid, and use of off-site storage).
 - g. Logistical arrangements (e.g., housing, transportation, or food) for personnel at the recovery locations.
 - h. Network equipment, connectivity, and communication needs, including entity-owned and personal mobile devices.

- i. Personnel at alternate sites, including arrangements for those permanently located at the alternate facility.
 - j. Scope and frequency of testing.
 - k. Resumption of a normalized state for business processes.
2. If management outsources the BCP's development, verify that management maintains oversight and ownership of the BCP.
 - a. Determine whether management verified the third-party service provider's qualifications and expertise.
 - b. Verify that entity management worked with the third-party service provider to design executable and viable strategies.
 - c. Verify that the plan reflects the entity's current products, business processes, and third-party service providers.
 - d. Determine whether roles and responsibilities reflect the entity's current organizational structure.
3. Determine whether the BCP includes event management procedures that detail reasonably foreseeable event types, and those procedures include threshold metrics and response methods.
 - a. Verify that procedures explain how to report an event to management and the situations that warrant notification.
 - b. Determine whether management (either an individual or team) has implemented procedures to communicate with both internal and external stakeholders.
 - c. Verify that event management processes include event response procedures that are appropriate to the event.
4. Assess management's protocols for operations continuity and system recovery. Verify that procedures are clear, concise, accessible, and can be implemented in an emergency. Verify the BCP includes procedures for the following:
 - a. Manual steps for critical functions, as applicable.
 - b. Alternate identity verification methods.
 - c. Fraud identification and suspicious activity reporting.
 - d. Other procedures as applicable. Examples may include:
 - Addressing customer service requests during downtime.
 - Tracking daily transactions.
 - Reconciling general ledger accounts.
 - Documenting operational tasks.
 - Posting entries after system recovery.
 - Maintaining backup records to provide customer account information (account numbers, customer names, addresses, account status, and account balances).
5. Verify that the BCP lists alternatives for core operations, facilities, infrastructure systems, suppliers, utilities, interdependent business partners, and key personnel.

- a. Verify that the BCP includes site relocation for short-, medium-, and long-term scenarios.
 - b. Determine whether management considers scalability.
 - c. Verify that recovery alternatives can accommodate the services and processing capabilities affecting critical operations, including:
 - Core processing.
 - Check processing and imaging.
 - Commercial cash management.
 - Mailing, faxing, and printing.
 - Customer identification.
 - Data center activities.
6. Verify that the BCP includes procedures for coordination with the first responders and local and state government agencies, when appropriate.
 7. Verify that the BCP includes procedures to establish an alternate physical location(s) where personnel and customers can go to conduct business, if appropriate.
 8. Determine whether the BCP addresses alternate arrangements in the event payment systems fail (e.g., ATMs, funds transfers, electronic banking, remote deposit capture, mobile capabilities).
 - a. Determine whether the BCP addresses processes for retrieving and transmitting transactions when payment systems are disrupted (e.g., manual procedures for calling in or faxing wire or automated clearing house requests to correspondent banks; mitigating strategies for web-based systems; or third-party software used to perform transactions).
 - b. Determine whether management verifies that redundant electronic payment systems and equipment (e.g., tokens and routers) are included at recovery sites for activation and that documentation is maintained for timely posting of entries when systems are recovered.
 - c. Determine whether instant issue cards are utilized and card company security procedures are implemented to limit potential fraud.
 9. Verify that the BCP addresses the entity's cash management requirements. Procedures may include:
 - a. Pre-established cash delivery arrangements.
 - b. Plans for increases in branch traffic when ATMs are unavailable.
 - c. Plans for the entity's operational cash needs.
 - d. Temporary purchase authority guidelines.
 - e. Expense reimbursement options for personnel.
 - f. Higher-limit credit cards or separate checking accounts with designated individuals who can sign checks in emergency situations.
 10. Determine whether management established an incident response process. As part of incident management planning, determine whether management does the following:

- a. Aligns incident response procedures with other related processes (e.g., cybersecurity, network operations, and physical security).
 - b. Considers incident response procedures during the development of the business continuity strategy.
 - c. Leverages routine processes (e.g., vulnerability management and network monitoring) to anticipate potential incidents, including cyber incidents.
11. Verify that management developed a coordinated disaster recovery strategy for data centers, networks, servers, storage, service monitoring, user support, and related software. Verify that procedures address the following:
 - a. Security controls and protocols, including physical and logical.
 - b. Procedures for restoring backlogged activity or lost transactions to identify how transaction records will be brought current within expected recovery time frames.
 - c. Instructions to access the repository of critical information when the primary facility is unavailable.
12. Verify whether management designates key personnel from applicable departments to act during a crisis or emergency situation. Key personnel may include:
 - a. Senior management for leadership.
 - b. Facilities management for safety and physical security.
 - c. Human resources for personnel issues and travel.
 - d. Media relations for managing communications.
 - e. Finance and accounting for funds disbursement and financial decisions, including unanticipated expenses.
 - f. Legal and compliance for legal and regulatory concerns.
 - g. IT, including information security, and operations for specific tactical responses.
13. Determine whether management established a crisis or emergency management process. Verify whether the BCP addresses the following:
 - a. Coordination with regulatory agencies, local and state officials, law enforcement, and first responders.
 - b. Disruptions not confined to a single event, facility, or geographic area.
 - c. Simultaneous disruptions of telecommunications and electronic messaging, including between the entity and third-party service providers.
 - d. Crisis or emergency management communication protocols, including the designation of a spokesperson(s) to communicate with the news media, as appropriate.

Objective 9: Determine whether the BCM program includes training and awareness to educate stakeholders about the entity’s continuity objectives and BCM goals. (VI, “[Training](#)”)

1. Verify that the training program aligns with the entity’s BCM strategy. Determine whether management does the following:
 - a. Inventories the current skillsets for BCM and identifies and addresses any training gaps.

- b. Establishes goals and objectives for supporting the BCM program as part of the entity's performance management process.
 - c. Implements a training program to educate stakeholders about the BCM goals and objectives. Elements may include:
 - Exercises.
 - Current risks.
 - Future risks.
 - Recent failures.
 - New programs/technologies.
 - Organizational changes.
 - Previous (exercise) lessons learned.
2. Assess whether management tailors training to the target audience, based on the audience's needs. The target audience could include:
 - a. Board members.
 - b. Senior management.
 - c. Business process owners.
 - d. Frontline personnel.
 - e. Contract personnel, as applicable.
3. Validate that management incorporates significant business continuity concepts, interdependencies, disruption impacts, and operations resilience into the training program.
4. Verify that the BCM training program, including board training, is updated as significant changes occur.

Objective 10: Determine whether the exercise and testing program is sufficient to allow management to assess the entity's ability to meet its continuity objectives. (VII, "[Exercises and Tests](#)")

1. Determine whether management implemented a comprehensive exercise and testing program, objectives, and plans to validate the entity's ability to restore critical business functions.
2. Verify that the program is appropriate for the entity's risk profile. Assess whether the entity's consolidated exercise and test schedule is reflective of exercise and test objectives and the overall exercise and test universe.
3. Determine whether management covers all of the functions in the exercise and test universe according to its established timeframes (e.g., all processes are covered annually or every three years).
4. Determine whether management has designated personnel with the authority to control the exercise or test and confirm exercise and test milestones are met.

5. Verify that business line management retains ownership for testing its specific business processes and coordinates with personnel involved in the enterprise-wide BCM process and support areas.
6. Verify that exercises and tests occur at appropriate intervals, or when significant changes affect the entity's operating environment.
7. Verify that management developed a process that is sufficiently robust to confirm the effectiveness of the entity's business continuity program. Therefore, the exercise program should incorporate the following:
 - a. A policy that includes strategies and expectations for exercise and test planning.
 - b. Roles and responsibilities for implementation.
 - c. Sufficient personnel to perform the exercise or test, provide oversight, and document the results.
 - d. Precautions to safeguard production data, such as performing a backup before performing a test in a test environment, or testing during non-peak hours.
 - e. Provisions for emergency stops and concluding exercises and tests.
 - f. Verification of continuity and resilience process assumptions and the ability to process a sufficient volume of work during adverse operating conditions.
 - g. Activities commensurate with the importance of the business process.
 - h. Entity's processes commensurate with their significance to critical financial markets.
 - i. Comparison of exercise and test results against the BCP to identify gaps between the exercise or test process and recovery guidelines, with revisions incorporated where appropriate.
 - j. Independent review of business continuity program and exercises and tests (internal and external).
8. Determine whether the exercise and test policy is appropriate and includes the following:
 - a. Key roles and responsibilities.
 - b. Minimum frequency, scope, and reporting.
 - c. Documentation expectations.
 - d. Processes for correcting deficiencies identified during exercises or tests.
 - e. Communication and connectivity between the entity and third-party service providers.
 - f. Participation with critical third-party service providers to confirm that entity personnel understand integration with all related recovery processes.
9. Determine whether the exercise and test strategies allow management to demonstrate the entity's ability to support connectivity, functionality, volume, and capacity using alternate facilities. Strategies may include the following:
 - a. Expectations for individual business lines and use of exercise and testing methodologies and scenarios.
 - b. Internal and external dependencies, including activities outsourced to domestic and foreign-based third-party service providers.

- c. Multi-year plan(s) to execute the specific depth and breadth of exercises and tests, which use different methodologies and scenarios over time.
 - d. Expectations for testing internal and external recovery dependencies.
 - e. Assumptions, methodologies, and exercises used to develop the test strategies.
 - f. Transaction processing and functional testing to assess the recoverability of infrastructure, capacity, and data integrity.
10. Verify that exercise and test objectives include resilience, system monitoring, and the recovery of business processes and critical system components.
11. Verify that exercises and associated tests accomplish the following objectives:
 - a. Build confidence that resilience and recovery strategies meet business requirements.
 - b. Demonstrate that critical services can be recovered within agreed upon recovery objectives (RTOs, RPOs, and MTDs) and customer SLAs.
 - c. Establish that critical services can be restored in the event of an incident at the recovery location.
 - d. Familiarize staff with recovery processes.
 - e. Verify that personnel are adequately trained and knowledgeable of recovery plans and procedures.
 - f. Confirm that exercise and test plans remain compatible with the BCP and the entity's infrastructure.
 - g. Identify any gaps between business continuity procedures and objectives.
12. Determine whether management established exercise and test plans, commensurate with the nature, scale, and complexity of the recovery objectives that address the objectives and expectations of the exercise or test and outline the scenario and any assumptions or constraints that may exist. Verify whether exercise and test plans include the following:
 - a. Identification of roles and responsibilities for participants, support personnel, and observers.
 - b. Metrics to assess whether objectives are met.
 - c. A consolidated exercise and test schedule that encompasses all objectives.
 - d. Specific descriptions of objectives and methods.
 - e. Roles and responsibilities for all test participants, including support personnel.
 - f. Identification of decision makers and succession plans.
 - g. Exercise and test locations to be utilized.
 - h. Escalation procedures and the ability to adjust for simulated scenarios.
 - i. Contact information.
13. Determine whether management developed reasonably foreseeable threat scenarios that simulate disruptions in business functions and the ability to meet both business requirements and customer expectations. Management should:
 - a. Identify and document assumptions used in developing each scenario.

- b. Develop scenarios that include threats that could affect third-party service providers, including communication processes with applicable stakeholders.
 - c. Develop exercises that demonstrate not only the ability to failover to an alternate site but also validate recovery objectives.
 - d. Create scenarios that include only the data and systems that would be available for recovery.
- 14. Verify that exercise and test scripts document the procedures for executing the exercise or test, which may include:
 - a. Applications, business processes, systems, or facilities reviewed.
 - b. Sequential steps for employees or external parties to perform.
 - c. Procedures to guide manual work-around processes.
 - d. A detailed schedule for completion.
 - e. Methods for participants to record results, quantifiable metrics, and any issues.
- 15. Assess whether exercise and test methods are commensurate with the size and complexity of the entity and the criticality of the function to the entity. Verify that exercises and tests are designed to do following:
 - a. Validate personnel knowledge and skills, including backup responsibilities.
 - b. Operate and perform duties (e.g., daily, quarterly, annually) from an alternate site.
 - c. Process transactions and assess system functionality.
 - d. Test the viability of both full and incremental backups.
 - e. Test network connectivity and interdependencies, including those with critical third-party service providers.
- 16. If management performs full-scale exercises, verify whether the exercise includes the following, where appropriate:
 - a. Engaging personnel from all business units to participate and interact with internal and external management response teams.
 - b. Validating that the crisis/emergency management process is operating as designed.
 - c. Verifying personnel knowledge and skills.
 - d. Validating management response and decision-making capability.
 - e. Demonstrating coordination among participants and decision makers.
 - f. Validating communication protocols.
 - g. Conducting activities at alternate locations or facilities.
 - h. Processing data using backup media or alternative methods.
 - i. Completing actual transactional volumes or an illustrative subset.
 - j. Performing recovery exercises over a sufficient length of time to allow issues to unfold as they would in a crisis.
- 17. If management performs limited-scale exercises, verify whether the exercise includes the following, where appropriate:

- a. Implementing a plan appropriate to the scenario.
 - b. Verifying personnel knowledge and skills.
 - c. Validating management response and decision-making capability.
 - d. Executing on-the-scene coordination and decision-making roles.
 - e. Verifying whether participants can connect to alternate system(s).
 - f. Conducting activities at alternate locations or facilities.
 - g. Testing communication and remote access capability (e.g., switching to alternate equipment or telecommuting).
18. If management performs tabletop exercises, determine whether targeted plans and procedures are reasonable, personnel understand their responsibilities, and different departmental or business unit plans are compatible with each other. (By themselves, tabletop exercises are likely insufficient to validate recovery capabilities because they are limited to a discussion-based analysis of policies and procedures.) Tabletop exercises may include the following:
 - a. Engaging operational and support personnel who are responsible for implementing the BCP.
 - b. Practicing and validating specific functional response capabilities.
 - c. Demonstrating knowledge and skills, as well as team interaction and decision-making capabilities.
 - d. Role playing with simulated responses, evaluating critical steps, recognizing difficulties, and resolving problems.
 - e. Clarifying critical plan elements, as well as problems noted during exercises.
 - f. Creating action plans to correct issues.
19. Verify that management clearly defines the characteristics of a successful test, which may include the following:
 - a. Validating RPOs, RTOs, and MTDs.
 - b. Demonstrating recoverability at peak volumes.
 - c. Confirming that systems can support critical business processes (e.g., transfer to alternate sites, increased workloads, manual workarounds, and communication).
 - d. Integrating technologies that support critical business activities, including data replication, recovery, and off-site storage.
 - e. Testing backup data to assess integrity and availability.
 - f. Certifying facility controls (e.g., environmental, backup power, and physical security).
 - g. Verifying workspace restoration (e.g., network connectivity and communications).
 - h. Ensuring that personnel are familiar with and are able to execute their responsibilities.
20. Determine whether the right to perform testing or participate in exercises and tests with third parties is described in the contract governing the entity's relationship with the third-party service provider.
21. Determine whether exercises and tests with third-party service providers are included in the entity's enterprise exercise and test program based on the risk prioritization of the third-party

service provider and the criticality of the services provided to the entity. Assess the following:

- a. The process to rank third-party service providers based on criticality, risk, and testing scope.
 - b. Coordinated exercises and tests that reasonably validate the abilities of both the entity and the third-party service provider to recover, restore, resume, and maintain operations after disruptions consistent with business and contractual requirements.
 - c. Evidence that exercises and tests of critical service providers include reasonably foreseeable significant disruptive events.
 - d. Documentation of the scope, execution, and results of exercises and tests in which the entity is unable to directly participate.
22. Determine whether the entity participates in its critical third-party service providers' exercise and test program(s) at reasonable intervals. Assess the execution of the exercises and tests and whether they included the following:
- a. End-to-end and, when appropriate, full-scale exercises.
 - b. Transaction processing and functional testing.
 - c. Network connectivity and interdependencies to include those with critical fourth parties.
 - d. Bidirectional operations between the entity's and its third-party service provider's primary and alternate locations and systems.
 - e. Supply chain considerations.
23. Determine whether testing scenarios with critical third-party service providers consider the following:
- a. An outage or disruption of the service provider.
 - b. An outage or disruption at the entity.
 - c. Incident response plans.
 - d. Crisis management plans.
 - e. Communication processes with third-party service providers and other stakeholders.
 - f. Cyber events.
 - g. Returning to normal operations.
24. Determine whether the tests validate the core or significant firm's backup arrangements to confirm the following:
- a. Backup sites are able to support typical payment and settlement volumes for an extended period.
 - b. Backup sites are fully independent of the critical infrastructure components that support the primary sites.
 - c. Trained employees are located at the backup sites at the time of disruption.
 - d. Backup site employees are independent of the staff located at the primary site at the time of disruption.

- e. Backup site employees are able to recover clearing and settlement of open transactions within the time frames addressed in the BCM processes and applicable industry standards.
25. Determine whether the exercise and test assumptions are appropriate for core and significant firms and consider the following:
 - a. Primary data centers and operations facilities that are completely inoperable without notice.
 - b. Whether personnel at primary sites, who are located at both data centers and operations facilities, are unavailable for an extended period.
 - c. Whether other organizations are also affected, causing effects that have the potential to cascade from one organization across to the entire financial services sector.
 - d. Infrastructure (e.g., power, telecommunications, transportation) that is disrupted.
 - e. Whether data recovery or reconstruction to restart payment and settlement functions can be completed within the time frames defined by the BCM process and applicable industry standards.
 - f. Whether continuity arrangements continue to operate until all pending transactions are closed.
26. Determine whether the core firm's testing strategy includes plans to test the ability of significant firms that clear or settle transactions to recover critical clearing and settlement activities from geographically dispersed backup sites within a reasonable time frame.
27. Determine whether the significant firm has an external exercise and test strategy that addresses key interdependencies, such as exercises and tests with third-party market providers and key customers, and determine the following:
 - a. Whether external exercise and test strategies include the significant firm's backup sites to the core firm's backup sites.
 - b. Whether the significant firm participates in industry (e.g., U.S. Department of the Treasury's Hamilton Series and FS-ISAC's CAPS exercises) or cross-market tests sponsored by core firms, markets, or trade associations. Tests should incorporate verifying the connectivity from alternate sites and include transaction, settlement, and payment processes, to the extent practical.
28. Determine whether the exercise and test program is sufficient to demonstrate the entity's ability to meet its continuity objectives and whether the results demonstrate the readiness of personnel to achieve the entity's recovery and resumption objectives. Determine whether management accomplishes the following:
 - a. Coordinate the execution of its exercise and test program to fully exercise its business continuity planning process.
 - b. Analyze and compare results against stated objectives.
 - c. Raise issues with appropriate personnel and assign responsibility for resolution.

- d. Escalate issues that cannot be resolved in a timely manner to the appropriate level of management.
 - e. Prioritize and track issues through final resolution.
 - f. Analyze results and issues to determine whether problems can be traced to a common source.
 - g. Document recommendations for future exercise and tests.
29. Verify that corrective actions have been implemented and that retesting occurs in a timely fashion to address deficiencies in meeting the entity's objectives.
30. Verify that test results are used to update the business continuity processes, enhance future testing, and evaluate whether risk mitigation strategies should be adjusted.

Objective 11: Determine whether management continuously measures the progress and assesses the effectiveness of BCM and uses the information to improve the BCM process. (VIII, "[Maintenance and Improvement](#)")

1. Determine whether management reviews and updates the business continuity program to reflect the current environment. Triggers that prompt maintenance and improvement of the BCM may include the following:
 - a. Changes in enterprise strategies.
 - b. New or reconfigured products, services, or infrastructure.
 - c. Changes in products and services offered by third-party service providers.
 - d. Deficiencies identified in third-party service provider BCM processes.
 - e. New legislation, regulatory requirements, or resilience practices.
 - f. Results of operational metric analysis (e.g., key risk indications, key performance indicators).
 - g. Early warning indicators that may identify potential continuity events, crises, or incidents (e.g., frequency and severity of storms, heightened cyber attack activity, or increases in customer service calls).
 - h. Variances between budgeted and actual BCM expenses.
 - i. Results from exercises and tests and lessons learned.
 - j. Changes in the threat landscape (e.g., new capabilities, intent of threat actors).
 - k. Recommendations (e.g., from audits, vulnerability assessments, and penetration tests, including those involving the use of advanced cybersecurity analysis and assessments).
2. Determine whether management has documented, analyzed, and reviewed lessons learned from adverse events. Documented procedures for incorporating lessons learned may include:
 - a. Identifying the failure(s).
 - b. Determining the cause(s).
 - c. Evaluating potential solutions.
 - d. Implementing corrective actions as appropriate.
 - e. Recording and reviewing corrective actions taken.

3. Verify that management documents, tracks, and resolves any changes when updating the BCP and the exercise and testing program(s). Furthermore, verify that management maintains appropriate version control of key BCM documents.
4. Determine whether management maintains backup copies of relevant BCM documentation in the event that the primary repository becomes inaccessible.

Objective 12: Determine whether the board has established expectations for BCM reporting. (IX, “[Board Reporting](#)”)

1. Review board minutes to determine whether management periodically reports to the board on the status of BCM.
 - a. Determine whether reports include a written BCM presentation, including the BIA, risk assessment, BCP, exercise and test results, and identified issues.
 - b. Determine whether management provides the board with regular strategy updates based on changes in personnel, roles and responsibilities, and business operations.
 - c. Verify that management documents the reasons (e.g., cost and service level) for choosing recovery alternatives and why they are appropriate based on the entity’s risk profile and complexity.
 - d. Assess whether the board provides a credible challenge to management, when appropriate.

Objective 13: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the examiner-in-charge regarding the following:
 - a. Apparent violations of laws and regulations.
 - b. Significant issues warranting inclusion in the report of examination.
 - c. Proposed Uniform Rating System for IT (URSIT) management component rating and the potential impact of the examiner’s conclusions on composite or other URSIT component ratings.
 - d. Potential impact of the examiner’s conclusions on the entity’s risk assessment(s).
2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.
3. Document conclusions in a memorandum to the examiner-in-charge that provides report-ready comments for all relevant sections of the report of examination and clarifying guidance to future examiners.
4. Organize work papers to show clear support for significant findings by examination objective.

Appendix B: Glossary

The purpose of the glossary is to define technical terms used in the *FFIEC IT Examination Handbook* booklets in the context of supervisory activities for the entities over which FFIEC members have supervisory authority. The FFIEC members strive to align terminology in the glossary with appropriate authoritative standards, including the *NIST Computer Security Resource Center Glossary* (NIST Glossary) as the primary source for cyber-related definitions, as appropriate. FFIEC members employed the following process to select, modify, or develop definitions.

When a NIST definition existed:

- If NIST had a defined term and modifications to the definition were unnecessary, the FFIEC members included the NIST definition in this glossary. When multiple NIST definitions were available for the same term, the FFIEC members selected a definition for supervisory purposes.
- If NIST had a defined term, but the definition needed additional clarity for supervisory purposes to assist with the identification of safety and soundness and enterprise risks related to IT, the FFIEC members included both the NIST definition and the FFIEC-adapted definition. Definitions of this nature are labeled “FFIEC Adapted for Supervisory Purposes” in this glossary’s source column.

When a NIST definition did not exist or the definition was not appropriate for supervisory purposes:

- If NIST did not have a defined term, but there was an appropriate authoritative third-party source (e.g., the International Organization for Standardization (ISO) Glossary), the FFIEC members included that authoritative definition.
- If NIST did not have a defined term and there was not an appropriate authoritative third-party source, the FFIEC members developed a definition for supervisory purposes. Definitions of this nature are labeled “FFIEC Developed for Supervisory Purposes” in this glossary’s source column.

Note: Due to the constantly evolving nature of IT and its associated risks, the FFIEC members may update definitions to maintain alignment with other government agencies and the financial services industry.

Term	Definition	Source
A		
Application programming interface (API)	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.	NIST Glossary
	Software code that allows two or more programs to communicate with each other.	FFIEC Adapted for Supervisory Purposes

Asynchronous replication	Data is first written to the primary storage area (store) and then copied to the secondary storage area (forward) at predefined intervals, which is useful over smaller bandwidth connections and longer distances where latency could occur.	FFIEC Developed for Supervisory Purposes
B		
Business continuity	The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruption.	ISO 22300:2018(en)
Business continuity management (BCM)	The process for management to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services.	FFIEC Developed for Supervisory Purposes
Business continuity plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.	NIST Glossary
	A comprehensive written plan(s) to maintain or resume business in the event of a disruption.	FFIEC Adapted for Supervisory Purposes
Business impact analysis (BIA)	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.	NIST Glossary
	Management's analysis of an entity's requirements, functions, and interdependencies used to characterize contingency needs and priorities in the event of a disruption.	FFIEC Adapted for Supervisory Purposes
C		
Cold site	A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.	NIST Glossary
Contingency plan	A plan that is maintained for disaster response, backup operations, and post-disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.	NIST Glossary
Crisis	Abnormal and unstable situation that threatens the organization's strategic objectives or viability.	Business Continuity Institute Disaster Recovery Journal Glossary
Crisis management	The process of managing an entity's preparedness, mitigation response, continuity, or recovery in the event of an unexpected significant disruption, incident, or emergency.	FFIEC Developed for Supervisory Purposes
Critical financial markets	Financial markets whose operations are critical to the economy. Critical financial markets provide the means for financial institutions to adjust their cash and securities positions and those of their customers in order to manage liquidity, market, and other risks to their organizations. Critical financial markets also provide support for the provision of a wide range of financial services to businesses and consumers in the United States and support the implementation of monetary policy. Examples of critical financial markets include federal funds, foreign	FFIEC Developed for Supervisory Purposes

	exchange, and commercial paper; U.S. government and agency securities; and corporate debt and equity securities.	
D		
Data	A representation of information as stored or transmitted.	NIST Glossary
	A physical or digital representation of information processed, stored (at rest), or transmitted (in transit).	FFIEC Adapted for Supervisory Purposes
Data center	A facility that houses virtual and/or physical information technology infrastructure(s) (e.g., computer, server, and networking systems and components) designed to store, process, and serve large amounts of data in support of an entity's strategic and business objectives. A data center may be a dedicated facility or an area or room, that contains computer, server and networking systems and components, and may be private or shared (e.g., a co-location facility).	FFIEC Developed for Supervisory Purposes
Data mirroring	The act of copying data from a database at a primary location to a database at a secondary location in or near real time.	FFIEC Developed for Supervisory Purposes
Data replication	The process of copying data, usually with the objective of maintaining identical sets of data in separate locations.	FFIEC Developed for Supervisory Purposes
Data synchronization	The simultaneous comparison and reconciliation of interdependent data files, to ensure that the files contain the same information.	FFIEC Developed for Supervisory Purposes
Database	A repository of information or data, which may or may not be a traditional relational database system.	NIST Glossary
	A repository of information or data organized to be accessed, managed, and updated.	FFIEC Adapted for Supervisory Purposes
Disaster	Situation where widespread human, material, economic, or environmental losses have occurred, which exceeded the ability of the affected organization, community, or society to respond and recover using its own resources.	ISO 22300:2018(en)
Disaster recovery	The process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure, systems, and applications, which are vital to an organization after a disaster or outage. Disaster recovery focuses on the information or technology systems that support business functions, as opposed to business continuity, which involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery is a subset of business continuity.	Business Continuity Institute Disaster Recovery Journal Glossary
Disruption	An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).	NIST Glossary
	An anticipated or unplanned event that causes operations to degrade or fail for an unacceptable length of time	FFIEC Adapted for Supervisory Purposes

E		
Emergency management	See crisis management.	
Emergency response	Actions taken in response to a disaster warning or alert to minimize or contain the eventual negative effects, and those taken to save and preserve lives and provide basic services in the immediate aftermath of a disaster impact, for as long as an emergency situation prevails.	Business Continuity Institute Disaster Recovery Journal Glossary
Event	Occurrence or change of a particular set of circumstances.	NIST Glossary
	An occurrence or change in circumstances that may affect operations. An event can be physical, cyber, or a combination of both	FFIEC Developed for Supervisory Purposes
Exercise	A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.	NIST Glossary
	A task or activity done to practice or test a procedure. There are many different types of exercises, depending on the intended goals and objectives. An exercise may involve performing duties in a simulated environment and can be discussion-based or simulation-based.	FFIEC Adapted for Supervisory Purposes
F		
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.	NIST Glossary
Full-scale exercise	A simulation involving a full use of available resources (e.g., hardware, software, personnel, communications, utilities, and processing from an alternate site) at the same time.	FFIEC Developed for Supervisory Purposes
Functional testing	Testing that verifies that an implementation of some function operates correctly.	NIST Glossary
H		
High availability	A failover feature to ensure availability during device or component interruptions.	NIST Glossary
	Ability of a system to be continuously operational for a desirably long length of time and to maintain a minimum amount of downtime during device or component interruptions. Availability can be measured relative to "100% uptime" or "never failing."	FFIEC Adapted for Supervisory Purposes
Hot site	A fully operational off-site data processing facility equipped with hardware and software, to be used in the event of an information system disruption.	NIST Glossary
I		
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	NIST Glossary

Incident management	The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible.	FFIEC Developed for Supervisory Purposes
Incident response	The response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.	Business Continuity Institute Disaster Recovery Journal Glossary
Infrastructure	System of facilities, equipment, and services needed for the operation of an organization.	ISO 22300:2018(en)
Integrated exercise	A simulation to test the effectiveness of the continuity plans for a business line or major function that incorporates more than one component or module, including external dependencies.	FFIEC Developed for Supervisory Purposes
Interdependencies	When two or more departments, processes, functions, or third-party providers interact to successfully complete a task, business function, or process.	FFIEC Developed for Supervisory Purposes
L		
Last mile	Communications technology that bridges the transmission distance between the telecommunication service provider and the entity.	FFIEC Developed for Supervisory Purposes
Latency	Time delay in processing voice packets.	NIST Glossary
	Time delay in processing voice and data packets.	FFIEC Adapted for Supervisory Purposes
Limited-scale exercise	A simulation involving applicable resources (personnel and systems) to recover targeted business processes.	FFIEC Developed for Supervisory Purposes
M		
Maximum tolerable downtime (MTD)	The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission.	NIST Glossary
	The total amount of time the system owner or authorizing official is willing to accept for a business process disruption, including all impact considerations.	FFIEC Adapted for Supervisory Purposes
N		
Network backbone	The main communication channel of a network that interconnects one or more network segments and provides a path for the exchange of data between devices. A backbone can span any geographic area.	FFIEC Developed for Supervisory Purposes
O		
Operational resilience	The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.	NIST Glossary
	The ability of an entity's personnel, systems, telecommunications networks, activities, or processes to resist, absorb, and recover from or	FFIEC Adapted for Supervisory Purposes

	adapt to an incident that may cause harm, destruction, or loss of ability to perform mission-related functions.	
Outage	The interruption of systems, infrastructure, support services, or essential business functions, which may result in the entity's inability to provide services for some period of time. The amount of time lost from an outage may result in downtime. Conversely, downtime may cause an outage.	FFIEC Developed for Supervisory Purposes
Outsourcing	The practice of contracting through a formal agreement with a third party(ies) to perform services, functions, or support that might otherwise be conducted in-house.	FFIEC Developed for Supervisory Purposes
R		
Reciprocal agreement	An agreement that allows two organizations to back up each other.	NIST Glossary
	An agreement that allows two entities (or two internal business groups) with compatible systems and functionality that allows each one to recover at the other's location.	FFIEC Adapted for Supervisory Purposes
Recovery point objective (RPO)	The point in time to which data must be recovered after an outage.	NIST Glossary
	The point in time to which data used by an activity is restored to enable the resumption of business functions. The RPO is expressed backward in time from the point of disruption and can be specified in increments of time (e.g., minutes, hours, or days).	FFIEC Adapted for Supervisory Purposes
Recovery time objective (RTO)	The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.	NIST Glossary
Remote access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).	NIST Glossary
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.	NIST Glossary
S		
Scenario	A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives.	NIST Glossary
Service level agreement	Defines the specific responsibilities of the service provider and sets the customer expectations.	NIST Glossary
	A formal agreement between two parties that records: a common understanding about products or services to be delivered, priorities, responsibilities, guarantees, and warranties between the parties. In addition, the agreement describes the nature, quality, security, availability, scope, and timeliness of delivery and response of the parties, the point(s) of contact for end-user problems, and the metrics by which the effectiveness of the process is monitored and approved, and may include other measurable objectives. The agreement should cover not only expected day-to-day situations, but also unexpected or adverse events, as the need for the service may vary.	FFIEC Adapted for Supervisory Purposes

Supply chain risk management	The implementation of processes, tools, or techniques to minimize the adverse impact of attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.	NIST Glossary
	The implementation of processes, tools, or techniques to minimize the adverse impact of attacks that allow the adversary to exploit vulnerabilities inserted prior to installation. This is done in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).	FFIEC Adapted for Supervisory Purposes
Synchronous replication	Data is written to both primary and secondary storage areas at the same time to ensure that multiple copies of the data are current and identical. This method is used for critical business functions where latency is unacceptable, and little or no data loss can be tolerated.	FFIEC Developed for Supervisory Purposes
T		
Tabletop exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.	NIST Glossary
	A discussion-based exercise where personnel meet in a classroom setting or in breakout groups to validate a component(s) of the business continuity plan(s) by discussing their roles and responsibilities. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.	FFIEC Adapted for Supervisory Purposes
Test	An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in an IT plan.	NIST Glossary
	A type of exercise intended to verify the quality, performance, or reliability of system resilience in an operational environment.	FFIEC Adapted for Supervisory Purposes
Threat intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.	NIST Glossary
Trigger	An event that causes the system to initiate a response. Note: Also known as a triggering event.	NIST Glossary
	An event that prompts a response from management or an automated system. Also known as a triggering event.	FFIEC Adapted for Supervisory Purposes
W		
Warm site	An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.	NIST Glossary

Appendix C: Abbreviations

ATM	automated teller machine
BCM	business continuity management
BCP	business continuity plan
BIA	business impact analysis
CA Letter	Consumer Affairs Letter
CAPS	Cyber-Attack Against Payment Systems
CDC	Centers for Disease Control and Prevention
CFPB	Consumer Financial Protection Bureau
CFR	Code of Federal Regulations
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DDoS	distributed denial of service
DHS	U.S. Department of Homeland Security
DRaaS	disaster recovery as a service
ERM	enterprise risk management
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FIL	Financial Institution Letter
FRB	Board of Governors of the Federal Reserve System
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSARC	Financial Systemic Analysis & Resilience Center
FSSCC	Financial Services Sector Coordinating Council
GETS	Government Emergency Telecommunications Service
IIA	Institute of Internal Auditors
ISO	International Organization for Standards
IT	information technology
<i>IT Handbook</i>	<i>FFIEC Information Technology Examination Handbook</i>
MTD	maximum tolerable downtime
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
ODNI	Office of the Director of National Intelligence
RPO	recovery point objective
RTO	recovery time objective
SLA	service-level agreement
SLC	State Liaison Committee
SOC	systems and organization control
SR Letter	Supervision and Regulation Letter
SSAE	Statement on Standards for Attestation Engagement
TSP	Telecommunications Service Priority
URSIT	Uniform Rating System for Information Technology
USC	United States Code
WPS	Wireless Priority Service Program

Appendix D: References

Laws

- 12 U.S.C. 95(b) / 1463(a) / 3102(b), “Comptroller Authority to Declare a Legal Holiday”
- 12 U.S.C. 1464, “Home Owners’ Loan Act”
- 12 U.S.C. 1831r-1, “Notice of Branch Closure”
- 12 U.S.C. 1861–1867, “Bank Service Company Act”
- 12 U.S.C. 1882, “Bank Protection Act”
- 12 U.S.C. 3352, “Emergency Exceptions for Disaster Areas”
- 15 U.S.C. 6801 and 6805(b), “Gramm–Leach–Bliley Act”
- 18 U.S.C. 1030, “Fraud and Related Activity in Connection With Computers”

Consumer Financial Protection Bureau

Guidance

- CFPB Statement on Supervisory Practices Regarding Financial Institutions and Consumers Affected by a Major Disaster or Emergency (September 2018)
- CFPB Compliance Bulletin and Policy Guidance; 2016-02, Service Providers (October 2016)

Federal Reserve

Regulations

- 12 CFR 208, Appendix D-1, “Interagency Guidelines Establishing Standards for Safety and Soundness”
- 12 CFR 208, Appendix D-2, “Interagency Guidelines Establishing Information Security Standards (State Member Banks)”
- 12 CFR 225, Appendix F, “Interagency Guidelines Establishing Information Security Standards”

Guidance

- SR Letter 20-3 / CA Letter 20-2, “Interagency Statement on Pandemic Planning” (March 2020)
- SR Letter 16-11, “Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than \$50 Billion” (June 2016)
- SR Letter 15-10 / CA Letter 15-8, “Expansion of the Federal Reserve’s Emergency Communications System” (October 2015)
- SR Letter 15-9, “FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors” (July 2, 2015)
- SR Letter 13-19 / CA Letter 13-21, “Guidance on Managing Outsourcing Risk” (December 2013)
- SR Letter 13-16, “End of Microsoft Support for Windows XP Operating System” (October 2013)

- SR Letter 13-6 / CA Letter 13-3, “Supervisory Practices Regarding Banking Organizations and Their Borrowers and Other Customers Affected by a Major Disaster or Emergency” (March 2013)
- SR Letter 12-14, “Revised Guidance on Supervision of Technology Service Providers” (October 2012)
- SR Letter 10-13, “Interagency Supervisory Guidance for Institutions Affected by the Deepwater Horizon Oil Spill” (October 2010)
- SR Letter 06-3, “Interagency Supervisory Guidance for Institutions Affected by Hurricane Katrina” (February 3, 2006)
- SR Letter 05-24, “Interagency Questions and Answers for Financial Institutions in Response to Hurricanes Katrina and Rita” (December 2, 2005)
- SR Letter 05-17, “Katrina Related Marketing Practices Invoking the Name of the Federal Reserve” (September 22, 2005)
- SR Letter 05-16, “Supervisory Practices Regarding Banking Organizations and Consumers Affected by Hurricane Katrina” (September 15, 2005)
- SR Letter 03-9, “Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System” (May 28, 2003)

Federal Deposit Insurance Corporation

Regulations

- 12 CFR 304.3(d), “Notification of Performance of Bank Services, Form FDIC 6120/06”
- 12 CFR 364, Appendix A “Interagency Guidelines Establishing Standards for Safety and Soundness”
- 12 CFR 364, Appendix B “Interagency Guidelines Establishing Information Security Standards”
- 12 CFR 364, Supplement A to Appendix B “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice”

Guidance

- FIL-25-2020 “Identification of Essential Critical Infrastructure Workers During the COVID-19 Response Efforts” (March 26, 2020)
- FIL-14-2020 “Interagency Statement on Pandemic Planning” (March 6, 2020)
- FIL-19-2019, “Technology Service Provider Contracts” (April 2, 2019)
- FIL-63-2018, “Cybersecurity Preparedness Resource” (October 19, 2018)
- FIL-62-2017, “Major Disaster Examiner Guidance” (December 15, 2017)
- FIL-68-2016, “FFIEC Cybersecurity Assessment Tool: Frequently Asked Questions” (October 18, 2016)
- FIL-43-2016, “Information Technology Risk Examination (InTREx) Program” (June 30, 2016)
- FIL-37-2016, “FFIEC Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks” (June 7, 2016)
- FIL-55-2015, “Cybersecurity Awareness Resources” (November 23, 2015)
- FIL-28-2015, “Cybersecurity Assessment Tool” (July 2, 2015)

- FIL-13-2015, “FFIEC Joint Statements on Destructive Malware and Compromised Credentials” (March 30, 2015)
- FIL-13-2014, “Technology Outsourcing: Informational Tools for Community Bankers” (April 7, 2014)
- FIL-11-2014, “Distributed Denial of Service (DDoS) Attacks” (April 2, 2014)
- FIL-44-2008, “Third-Party Risk: Guidance for Managing Third-Party Risk” (June 6, 2008)
- FIL-6-2008, “Interagency Statement on Pandemic Planning: Guidance for Minimizing a Pandemic’s Potential Adverse Effects” (February 6, 2008)
- FIL-49-2006, “Lessons Learned from Hurricane Katrina: Preparing Your Institution for a Catastrophic Event” (June 15, 2006)
- FIL-27-2005, “Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice” (April 1, 2005)
- FIL-84-2002, “Financial and Banking Information Infrastructure Committee’s Interim Policy on the Sponsorship of Private Sector Financial Institutions in the GETS Card Program” (August 6, 2002)
- FIL-50-2001, “Bank Technology Bulletin on Outsourcing” (June 4, 2001)

National Credit Union Administration

Regulations

- 12 CFR 748, "Security Program, Report of Suspected Crimes, Suspicious Transactions, Catastrophic Acts and Bank Secrecy Act Compliance"
- 12 CFR 748, Appendix A, “Guidelines for Safeguarding Member Information”
- 12 CFR 749, "Guidelines for Safeguarding Member Information", Records Preservation Program and Appendices – Record Retention Guidelines; Catastrophic Act Preparedness Guidelines"
- 12 CFR 749, Appendix A, “Record Preservation Program and Record Retention”
- 12 CFR 749, Appendix B, “Catastrophic Act Preparedness Guidelines”

Guidance

- NCUA Letter to Credit Unions 20-CU-03, "Identification of Essential Critical Infrastructure Workers" (March 2020)
- NCUA Letter to Credit Unions 20-CU-02, "NCUA Actions Related to COVID-19" (March 2020)
- NCUA Letter to Credit Unions 10-CU-10, "2010 Hurricane Season and Ongoing Disaster, Emergency, and Pandemic Preparedness and Planning" (June 2010)
- NCUA Letter to Credit Unions 09-CU-13, "Hurricane Preparedness and Pandemic Planning" (June 2009)
- NCUA Letter to Credit Unions 08-CU-01, “Guidance on Pandemic” (January 2008)
- NCUA Letter to Credit Unions 07-CU-13, “Evaluating Third-Party Relationships” (December 2007)
- NCUA Letters to Credit Unions (06-CU-11), "Interagency Guidance Lessons Learned by Institutions Affected by Hurricane Katrina" (June 2006)
- NCUA Risk Alert 06-Risk-01, “Disaster Planning and Response” (April 2006)

NCUA Letter to Credit Unions 06-CU-06, “Influenza Pandemic Preparedness” (March 2006)
 NCUA Letter to Credit Unions 02-CU-17, “e-Commerce Guide for Credit Unions”
 (December 2002)
 NCUA Letter to Credit Unions 01-CU-21, “Disaster Recovery and Business Resumption
 Contingency Plans” (December 2001)
 NCUA Letter to Credit Unions 01-CU-20, “Due Diligence Over Third-Party Service
 Providers” (November 2001)

Office of the Comptroller of the Currency

Regulations

12 CFR 5.30, “Establishment, Acquisition, and Relocation of a Branch of a National Bank”
 12 CFR 5.31, “Establishment, Acquisition, and Relocation of a Branch and Establishment of
 an Agency Office of a Federal Savings Association”
 12 CFR 30, Appendix A, “Interagency Guidelines Establishing Standards for Safety and
 Soundness”
 12 CFR 30, Appendix B, “Interagency Guidelines Establishing Information Security
 Standards”
 12 CFR 30, Appendix D, “OCC Guidelines Establishing Heightened Standards for Certain
 Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal
 Branches”
 12 CFR 30, Appendix E, “OCC Guidelines Establishing Standards for Recovery Planning by
 Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured
 Federal Branches”

Guidance

OCC Bulletin 2020-23, “Essential Critical Infrastructure Workers in the Financial Services
 Sector”
 OCC Bulletin 2020-13, “Pandemic Planning: Updated FFIEC Guidance”
 OCC Bulletin 2019-13, “Recovery Planning”
 OCC Bulletin 2019-8, “Loans in Areas Having Special Flood Hazards – Private Flood
 Insurance: Final Rule”
 OCC Bulletin 2018-47, “Recovery Planning Guideline: Final Revised Guidelines”
 OCC Bulletin 2018-14, “Installment Lending: Core Lending Principles for Short-Term,
 Small-Dollar Installment Lending”
 OCC Bulletin 2018-8, “Cyber Insurance: FFIEC Joint Statement on Cyber Insurance and Its
 Potential Role in Risk Management Programs”
 OCC Bulletin 2017-61, “Major Disasters: Interagency Examiner Guidance for Institutions
 Affected by Major Disasters”
 OCC Bulletin 2017-54, “Branches and Relocations: Revised Comptroller’s Licensing
 Manual Booklet”
 OCC Bulletin 2017-35, “Flood Disaster Protection Act: Revised Comptroller’s Handbook
 Booklet”

OCC Bulletin 2017-24, “Branch Closings: Revised Comptroller’s Licensing Manual Booklet”

OCC Bulletin 2017-21, “Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29”

OCC Bulletin 2017-7, “Third-Party Relationships: Supplemental Examination Procedures”

OCC Bulletin 2016-34, “Cybersecurity: Frequently Asked Questions on the FFIEC Cybersecurity Assessment Tool”

OCC Bulletin 2016-30, “Enforceable Guidelines for Recovery Planning: Final Guidelines”

OCC Bulletin 2015-31, “Cybersecurity: FFIEC Cybersecurity Assessment Tool”

OCC Bulletin 2013-29, “Third-Party Relationships: Risk Management Guidance”

OCC Bulletin 2012-28, “Supervisory Guidance on Natural Disasters and Other Emergency Conditions”

OCC Bulletin 2006-26, “Disaster Planning: Hurricane Katrina – Lessons Learned”

OCC Bulletin 2006-12, “Influenza Pandemic Preparedness: Interagency Advisory”

OCC Bulletin 2006-6, “Community Reinvestment Act: Hurricanes Katrina and Rita”

OCC Bulletin 2003-14, “Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System”

OCC Bulletin 2003-13, “Telecommunications Service Priority (TSP) Program: Policy on Sponsorship of TSP for Private Sector Entities”

OCC Bulletin 2002-33, “Government Emergency Telecommunications Service (GETS): FBIIC Policy on Sponsorship of GETS Cards for Private Sector Entities”

OCC Bulletin 2002-16, “Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance”

OCC Bulletin 1998-3, “Technology Risk Management: Guidance for Bankers and Examiners”

Other References

U.S. Department of Health & Human Services, Centers for Disease Control and Prevention, [*Pandemic Influenza*](#) (January 2019)

Communications, Security, Reliability, and Interoperability Council, [*Infrastructure Sharing During Emergencies*](#) (December 2014)

National Infrastructure Protection Plan, [*NIPP 2013: Partnering for Critical Infrastructure and Resilience*](#) (November 2013)

NIST SP 800-34 Rev. 1, [*Contingency Planning Guide for Information Technology Systems*](#) (May 2010)

BITS Financial Services Roundtable, [*BITS Framework for Managing Technology Risk for Service Provider Relationships*](#) (May 2008)

Basel Committee on Banking Supervision, [*The Joint Forum: High-level Principles for Business Continuity*](#) (August 2006)

U.S. Department of Homeland Security, [*Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources*](#) (September 2006)

Department of Health and Human Services, Centers for Disease Control and Prevention [*Business Pandemic Influenza Planning Checklist*](#) (December 2005)

Homeland Security Council [*National Strategy for Pandemic Influenza*](#) (November 2005)

Federal Reserve Bank of New York, [*Best Practices to Assure Telecommunications Continuity for Financial Institutions and the Payment and Settlement Utilities: Report by the Assuring Telecommunications Continuity Task Force*](#) (September 2004)

The President's National Security Telecommunications Advisory Committee, [*Financial Services Task Report*](#) (April 2004)



FFIEC Information Technology Examination Handbook

Development, Acquisition, and Maintenance

AUGUST 2024

INTRODUCTION.....	1
I..... OVERVIEW OF DEVELOPMENT, ACQUISITION, AND MAINTENANCE.....	3
II..... GOVERNANCE OF DEVELOPMENT, ACQUISITION, AND MAINTENANCE.....	5
II.A Policies, Standards, and Procedures.....	6
II.B Roles and Responsibilities	6
II.B.1 Board, Senior Management, and Other Common Roles	7
II.B.2 IT Project Management Roles	8
II.B.3 Development Roles	10
II.B.4 Acquisition Roles	12
II.B.5 Maintenance Roles	14
II.B.6 Other Common Development, Acquisition, and Maintenance Roles	14
II.B.7 Supply Chain Roles	15
II.B.8 Other Support Functions.....	15
II.B.9 Audit's Role	16
III..... RISK MANAGEMENT OF DEVELOPMENT, ACQUISITION, AND MAINTENANCE	18
III.A Risk Identification	19
III.B Risk Measurement	20
III.C Risk Monitoring and Reporting	20
III.D Controlling or Mitigating Risk.....	21
IV COMMON DEVELOPMENT, ACQUISITION, AND MAINTENANCE RISK TOPICS.....	22
IV.A Open-Source	23
IV.B Commercial-off-the-Shelf	25
IV.C Licenses, Agreements, and Copyright Protection.....	26
IV.C.1 Software Licenses.....	27
IV.C.1(a) Free and Open-Source Software Licenses.....	28
IV.C.1(b) Proprietary Software Licenses	28
IV.C.2 Hardware Licenses	29
IV.C.3 Copyright Protection.....	29
IV.D Secure Development	30

IV.E	Data	32
IV.F	Secure Operating Environments	32
IV.G	Microservices	33
IV.H	Containers	37
IV.I	Application Programming Interfaces	43
IV.I.1	API Gateway	44
IV.I.2	API Risk Mitigation	46
IV.J	Methodologies.....	48
IV.J.1	Waterfall.....	49
IV.J.2	Agile.....	49
IV.K	Quality Management.....	52
IV.L	Documentation Standards	53
IV.M	Post-Implementation Review	54
IV.N	IT Project Management.....	55
IV.N.1	IT Project Phases	56
IV.N.1(a)	<i>Initiation</i>	<i>57</i>
IV.N.1(b)	<i>Planning.....</i>	<i>58</i>
IV.N.1(c)	<i>Execution</i>	<i>59</i>
IV.N.1(d)	<i>Closeout.....</i>	<i>59</i>
IV.N.2	Monitoring and Controlling	60
IV.N.3	IT Project Documentation	61
IV.N.3(a)	<i>IT Project Request.....</i>	<i>61</i>
IV.N.3(b)	<i>Business Case.....</i>	<i>62</i>
IV.N.3(c)	<i>Feasibility Study.....</i>	<i>62</i>
IV.N.3(d)	<i>IT Project Plans.....</i>	<i>63</i>
IV.N.3(e)	<i>Closeout Documentation.....</i>	<i>63</i>
IV.O	System Development Life Cycle.....	64
IV.O.1	SDLC Phases	65
IV.O.1(a)	<i>Initiation</i>	<i>66</i>
IV.O.1(b)	<i>Development or Acquisition</i>	<i>68</i>
IV.O.1(c)	<i>Implementation and Assessment.....</i>	<i>69</i>
IV.O.1(d)	<i>Operations and Maintenance.....</i>	<i>71</i>
IV.O.1(e)	<i>Sunset and Disposal.....</i>	<i>72</i>
IV.P	Third-Party Relationship Risk Management.....	74
IV.P.1	Planning.....	74

IV.P.2	Due Diligence and Third-Party Selection	74
IV.P.3	Contract Negotiation	75
IV.Q	Supply Chain Considerations	75
IV.Q.1	Supply Chain Risk Management.....	77
IV.Q.2	Software Bill of Material	89
IV.Q.3	Enterprise Risk Management and Supply Chain Risks.....	90
V	DEVELOPMENT	91
V.A	Development Standards and Controls	93
V.B	Testing	96
V.C	DevOps and DevSecOps	99
V.C.1	DevOps.....	100
V.C.2	DevSecOps.....	100
V.D	Functional Development Types	105
V.D.1	Model Development.....	106
V.D.2	Database Development	107
VI	ACQUISITION	109
VI.A	Acquisition Policies, Standards, and Procedures	111
VI.B	Acquisition Projects	113
VI.C	Solicitation.....	113
VI.D	Evaluation.....	116
VI.E	Contracts and Other Agreements.....	117
VI.E.1	Statement of Work	117
VI.E.2	Master Services Agreement.....	119
VI.E.3	Service Level Agreement.....	120
VI.E.4	Contracts	120
VI.E.5	Escrowed Source Code Agreements and Documentation	124
VI.E.6	Exit Strategy	125
VII	MAINTENANCE	126
VII.A	Preventive Maintenance	127
VII.B	Change Management.....	127
VII.B.1	Implementing Changes	129
VII.B.2	Additional Control Considerations in Change Management.....	132
VII.B.2(a)	<i>Data Controls in the Testing Environment.....</i>	<i>132</i>
VII.B.2(b)	<i>Library Controls.....</i>	<i>132</i>

VII.B.2(c)	<i>Code Repository Controls</i>	133
VII.B.3	<i>Change Types</i>	135
VII.B.3(a)	<i>Routine Modifications</i>	135
VII.B.3(b)	<i>Major Modifications</i>	136
VII.B.3(c)	<i>Emergency Modifications</i>	137
VII.B.4	<i>Change Management Documentation</i>	139
VII.B.4(a)	<i>Change Request Form</i>	140
VII.B.4(b)	<i>Impact Analysis</i>	140
VII.B.4(c)	<i>Rollback or Back-Out Plan</i>	141
VII.C	End-of-Life	142
VII.D	Termination and Disposal	144
VII.E	Maintenance Documentation	145
APPENDIX A: EXAMINATION PROCEDURES		146
APPENDIX B: GLOSSARY		182
APPENDIX C: ABBREVIATIONS		202
APPENDIX D: REFERENCES		204

INTRODUCTION

The “Development, Acquisition, and Maintenance” booklet is one in a series of booklets that compose the *Federal Financial Institutions Examination Council (FFIEC)*¹ *Information Technology Examination Handbook (IT Handbook)*. The *FFIEC IT Handbook* is prepared for use by examiners.² With the publication of this booklet, the FFIEC members replace the “Development and Acquisition” booklet issued in April 2004. The revised title now reflects the importance of maintenance in the life of a system or component.³ This booklet

- Describes system and component development, acquisition, and maintenance.
- Highlights key risk management practices when developing, acquiring, or maintaining systems and components.
- Provides an overview of and discusses information technology (IT) project management, the system development life cycle (SDLC), and supply chain risk management (SCRM).
- Addresses the importance of system and software maintenance to an entity’s resilience.

For *FFIEC IT Handbook* purposes, the term “entity” includes depository financial institutions,⁴ nonbank financial institutions,⁵ bank holding companies,⁶ savings and loan holding companies,⁷ and third-party service providers.⁸

¹ The FFIEC was established on March 10, 1979, pursuant to [Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. 95-630](#). The FFIEC comprises the principals of the Board of Governors of the Federal Reserve System (FRB), the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the State Liaison Committee (SLC).

² Each FFIEC member uses the principles outlined in this booklet consistent with the member’s supervisory authority.

³ Examples of systems and components include hardware, firmware, software, peripherals, and network components.

⁴ The term “depository financial institution” includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions.

⁵ The term “nonbank financial institution” includes nondepository financial institutions under the jurisdiction of either state banking departments or the CFPB.

⁶ The term “bank holding company” includes any company that has control over any bank or over any company that is or becomes a bank holding company as defined by the [Bank Holding Company Act](#).

⁷ The term “savings and loan holding company” includes any company that directly or indirectly controls a savings association or controls any other company that is a savings and loan holding company as defined by the [Home Owners’ Loan Act](#).

⁸ The term “third-party service provider” means third parties that provide services, the provision of which is subject to examination under the [Bank Service Company Act](#), the [Home Owners’ Loan Act](#), the [Dodd–Frank Wall Street Reform and Consumer Protection Act](#), or other relevant law.

This booklet does not impose new requirements on entities. Instead, this booklet describes the principles and practices that examiners can use when assessing an entity's system development, acquisition, and maintenance activities.

[Appendix A](#) of this booklet provides objectives-based examination procedures. Application of principles and related examination procedures will vary consistent with the examined entity's complexity and risk profile (including the size of the entity or the nature of the systems and components).

I OVERVIEW OF DEVELOPMENT, ACQUISITION, AND MAINTENANCE

Development, acquisition, and maintenance activities are integral to an entity's operations. This booklet discusses how weaknesses in IT development, acquisition, and maintenance processes may lead to issues with confidentiality, integrity, availability, and resilience of the entity's systems, components, and data. Management determines the systems, products, and services that the entity will provide, whether to develop or acquire them, and how to maintain and service those systems, products, and services. Generally, whether developing or acquiring systems, products, and services, management performs some form of acquisition activity, including procurement. Management also oversees maintenance activities to prolong the life of systems and components (i.e., IT assets) and support continuity of operations. Management should plan for maintenance activities from the outset of acquisition or development to ensure secure continuity of operations. The following definitions and explanations provide an overview of IT development, acquisition, and maintenance.

Development: Systematic application of knowledge toward the production of useful materials, devices, and systems, or processes of defining, designing, testing, and implementing systems or components. Development includes validation and demonstration of a chosen technology, use of test and production environments, improvement of developed prototypes, integration into systems and subsystems, and inclusion of hardware builds. Development activities may be performed by the entity's personnel or third parties who develop systems and components on the entity's behalf. Management may choose to acquire systems and components from third parties and may customize them to meet the entity's needs.

Acquisition: All stages for acquiring products or services, beginning with determining the need for the product or service and ending with contract completion and closeout. Acquisition generally involves creating a relationship with a third party in the supply chain; therefore, effective SCRM is integral to the acquisition process. Acquisition activities include procurement processes that help ensure that management receives the contracted products or services. Acquisition activities, including procurement processes, help management achieve and maintain confidentiality, integrity, availability, as well as resilience, including supply chain resilience, throughout the life of systems and components.

Maintenance: Any act that either prevents the failure or malfunction of equipment or restores its operating capability. This includes incremental changes to improve performance. Maintenance activities include the processes to monitor systems and components and make changes (e.g., install patches and add new functions) to prevent their failure or malfunction and continue to meet user and customer needs. Management should perform preventive maintenance throughout the IT asset's useful life to prevent or minimize catastrophic failure and promote confidentiality, integrity, availability, and resilience. Maintenance may be performed by the entity's personnel or third parties. Maintenance activities should be performed regardless of the origin or location (e.g., geographic or virtual) of the systems or components.

The next section of this booklet addresses governance and risk management elements. Also addressed are common risk topics related to development, acquisition, and maintenance. The

booklet explains key topics, such as IT project management, SDLC, and supply chain risk management considerations, which are integral to development, acquisition, and maintenance activities to provide for ongoing operations. Appendices provide examination procedures, agency and industry references, and a glossary.

II GOVERNANCE OF DEVELOPMENT, ACQUISITION, AND MAINTENANCE

Action Summary

Management should establish, and the board of directors (board) should oversee, an effective governance framework for development, acquisition, and maintenance activities. Additionally, the board should oversee related IT project management processes to manage projects related to those activities.

Examiners should review the following:

- Enterprise-wide IT policies, procedures, and standards describing the entity's requirements throughout the development, acquisition, and maintenance life cycle.
- Charters (e.g., board, management, or committee), organizational charts, relevant documentation, and practices to determine whether appropriate roles and responsibilities are identified and assigned with suitable decision-making authority.
- Project plans and meeting minutes of the board and committees to ensure that activities and projects align with the entity's strategic objectives and the board's risk appetite.
- Project audit reports to determine whether the audit function provides independent, objective assurance of the effectiveness of an entity's development, acquisition, and maintenance activities.
- Documentation of controls for personnel with access to program code to limit placement into the production environment.
- Quality assurance (QA) reports to evaluate processes for the detection of potential coding errors.

The board⁹ should oversee and management should establish an effective governance structure that allows for the effective oversight and management of the development, acquisition, and maintenance of the entity's systems and components. Additionally, the board should oversee related IT project management processes and projects related to those activities. The board should oversee significant projects to ensure that they align with an entity's strategic plans. Projects that do not align may cause lost revenue or diminished economies of scale resulting in budget shortfalls. Misalignment may cause unexpected harm to the entity (e.g., noncompliance with laws and regulations and IT or operational performance issues). Ineffective communication or coordination by the board with appropriate stakeholders can lead to problems (e.g., scope creep on projects and cost overruns) and processes that do not facilitate appropriate communication across business departments. When IT activities are siloed away from business departments or other business line IT departments (i.e., when an entity has multiple lines of business that have their own IT departments), it may result in management establishing counterproductive objectives.

⁹ Most financial institutions have boards; however, not all third-party service providers do. When an entity does not have a board, senior leaders may have the responsibilities of a board as described in this booklet.

Management should consider the needs of internal and external stakeholders¹⁰ when making decisions regarding IT development, acquisition, and maintenance activities. Effective communication helps stakeholders carry out their roles and responsibilities and supports entity-wide alignment of these IT activities with an entity's strategic plans. Effective communication also helps stakeholders appropriately identify, assess, and mitigate risks and their potential impacts. Additionally, when contemplating IT projects and activities, management should consider business strategies and objectives, resilience needs, information security requirements, legal and regulatory requirements, and allocation of resources (e.g., personnel, budget, and time).

II.A Policies, Standards, and Procedures

Effective management develops and implements comprehensive, entity-wide IT policies, standards, and procedures covering the development, acquisition, and maintenance life cycle. Large or complex entities may have multiple policies for different business line functions and their underlying systems and components. The board and designated owners or committees should regularly review and approve IT policies. Policies should clearly delineate development, acquisition, and maintenance responsibilities and provide for communication to all personnel, stakeholders, and appropriate third parties. Standards, on the other hand, may be used to define the processes and rules to support IT policies. For example, software developers often use coding standards in their work. Procedures are often developed to provide instructions to perform a function or task to align with IT policies and standards and may be adjusted to meet changes in the entity's IT environment. Periodic adjustments to standards and procedures may be needed to continue to align with the board-defined risk appetite, threat environment, and risks to the entity and its customers. Management should review and approve deviations from policies, standards, and procedures related to development, acquisition, and maintenance. For example, if the entity's policy prohibits the use of open-source software, management should approve any exceptions when developers use open-source software.

II.B Roles and Responsibilities

The board should oversee and management should implement the entity's development, acquisition, and maintenance activities by identifying and assigning appropriate roles and responsibilities. Assigning roles and responsibilities helps management to assign decision-making authority to an appropriate individual or team. Designated roles and responsibilities allow management and stakeholders to identify relevant lines of communication. Additionally, management may specify qualifications, competence, skills, and expertise needed in various roles. Examples of common roles related to development, acquisition, and maintenance activities are described in the following sections of this booklet. In smaller or less complex entities, formal roles may not be established; however, management should identify and assign the responsibilities described in these sections. As appropriate for the needs of the entity, it is important to consider training needs to support development, acquisition, and maintenance

¹⁰ For purposes of this booklet, stakeholders may include management or designated individuals from all departments affected by the proposed project (e.g., information technology [IT], legal, compliance, independent risk management, business process owners, and audit), and board members. At times, stakeholders can also include external entities (e.g., clients, consumers, customers, or customers of financial institution clients of a third-party service provider).

responsibilities. For more information about IT roles and responsibilities in general, refer to the *FFIEC IT Handbook's* "[Management](#)" booklet.

II.B.1 Board, Senior Management, and Other Common Roles

Primary roles and responsibilities for the board and senior management for development, acquisition, and maintenance activities should include the following:

- **Board:** The board, or board-designated committee,¹¹ typically confirms that IT-related development, acquisition, and maintenance activities align with entity strategic objectives and the board's risk appetite. The audit committee of the board is involved with reviewing and validating the entity's audit-related activities, including development, acquisition, and maintenance.¹² Additionally, the board generally approves
 - Significant IT investments.
 - Policies and standards.
 - Significant IT projects that may affect the entity's strategic direction.¹³

Board members should have appropriate knowledge of risks to provide a credible challenge¹⁴ to management responsible for development, acquisition, and maintenance functions.

- **Senior management:** Senior management approves and champions development, acquisition, and maintenance projects within its authority, ensures that project execution is in alignment with entity objectives and risk appetite, and ensures that adequate resources, including qualified staff, are available to complete IT projects.
- **Chief information officer (CIO):** The CIO leads day-to-day IT system and component development, acquisition, and maintenance in accordance with the entity's policies and business strategy. Prudent practices include the CIO consulting with the entity's risk management function and legal counsel to ensure that development, acquisition, and maintenance decisions are consistent with sound risk management principles and applicable laws and regulations. Additionally, the CIO facilitates the integration of any new projects, systems, and components into the entity's operations to ensure that they align with strategic objectives and IT strategies. The CIO helps determine the feasibility of proposed projects or changes.

¹¹ For purposes of this booklet, when the role of the board is mentioned, it can be inferred that this role may be fulfilled by a board-designated committee, as appropriate, unless otherwise stated. An example of a board-designated committee is the architectural review board, which is common in larger or more complex entities.

¹² For more on the general role of audit and its responsibilities, refer to the *FFIEC IT Handbook's* "[Audit](#)" booklet.

¹³ Generally, the board approves critical operations and core business functions. For more information, refer to the following guidance: FDIC Financial Institution Letter (FIL) 103-2020, "[The FDIC Publishes Sound Practices to Strengthen Operational Resilience](#)"; FRB Supervision and Regulation (SR) Letter 20-24, "[Interagency Paper on Sound Practices to Strengthen Operational Resilience](#)"; and OCC Bulletin 2020-94, "[Operational Risk: Sound Practices to Strengthen Operational Risk](#)."

¹⁴ A credible challenge involves being actively engaged, asking thoughtful questions, and exercising independent judgment.

- **Chief information security officer (CISO):** The CISO typically develops enterprise-wide cybersecurity and information security policies and standards, including procedures promoting secure development, acquisition, and maintenance practices, and provides input for the consideration and inclusion of security and resilience in IT projects. The CISO is responsible for validating that security and resilience are maintained throughout the life of a project, system, or component.
- **IT steering committee:** An IT steering committee typically reviews and approves major development, acquisition, and maintenance proposals. Additionally, the committee provides a credible challenge to IT project managers and management responsible for development, acquisition, and maintenance activities. The credible challenge allows management to verify that projects adhere to entity policies, standards, and procedures; that project managers identify and appropriately mitigate risks; and that project costs stay within the allocated budget. The IT steering committee is responsible for reporting to the board and overseeing any issues (e.g., project issues or failure to meet standards) or additional project needs (e.g., additional funds and resources) by translating technical concepts in a way that is clear and understandable to relevant stakeholders.

II.B.2 IT Project Management Roles

There are multiple IT project management roles that, when performed effectively, can play a significant part in a project's success. A project can be part of larger programs, which may include multiple related projects. Roles may overlap in smaller or less complex entities or projects, which is acceptable if mitigating controls are in place. Segregation of duties and dual controls or other compensating controls are important for development, acquisition, and maintenance projects. For example, segregation of duties helps ensure that one person cannot use projects to misappropriate entity funds; purchase substandard software, hardware, or components; or initiate inappropriate contracts. Additionally, a key concern is that seemingly small problems in IT projects can quickly escalate in scale. Dual control may be used to mitigate this risk because it allows for problems to be identified and addressed earlier since no single person or group can make final decisions without agreement from others. For example, during development, code review involves a second individual to review code before it is released to test environments. Segregation of duties and dual control help foster security and resilience. For more information, refer to the "[IT Project Management](#)" section of this booklet. Common IT project management roles and responsibilities include the following:

- **Sponsor:** A project's sponsor is the most senior role in the project or program, which may contain multiple projects. Depending on the project's size and complexity, there may be more than one sponsor. Responsibilities include obtaining stakeholder endorsement for the project based on its objectives and business case,¹⁵ providing resources, and appointing the project owner. The sponsor represents the project in discussions with senior management, provides both formal and informal support to project teams, and promotes the positive aspects of the changes resulting from the project. The sponsor works with senior stakeholders

¹⁵ A business case provides justification to undertake a project, and the business case identifies the benefit, costs, and provides a rationale for the preferred solution. For more information, refer to the Project Management Institute (PMI), "[Is This Really Worth the Effort? The Need for a Business Case.](#)"

to resolve strategic issues across projects in a program or among projects. Additionally, the sponsor approves milestones and confirms the project's successful delivery.

- **Project owners:** A project owner typically helps determine a project's vision and guides progress toward the objectives to meet that vision throughout the project life cycle. The project owner manages key project risks to maintain alignment between the entity's objectives and those of the project. Additionally, the project owner obtains resources from the sponsor, serves as the primary communication link with management and other stakeholders, and is responsible for the successful completion of the project.
- **Product owner:** A product owner represents the business line stakeholders (e.g., team, department, or customer) for the team that undertakes the project. The product owner ensures that the project team delivers the most value by helping to prioritize deliverables. The product owner is responsible for communicating project status with the business line stakeholders.
- **Project or program managers:** Project or program managers are responsible for working with the business change manager to plan and monitor the project or program tasks. Additionally, they verify that tasks align with the objectives throughout the project's or program's life cycle. They are responsible for defining success and providing oversight for the completion of tasks and successful delivery of the project's or program's objectives. Project or program managers tend to have practical project management experience rather than specific business line expertise. They monitor and manage resources to stay within timelines and budget, including coordinating between projects and managing project interdependencies. Additionally, project or program managers manage issues and direct corrective action when necessary. They monitor, report, and communicate a project's or program's status to management and other stakeholders. Lastly, project or program managers maintain all project documentation.
- **Business change manager:** A business change manager represents the business line for projects or programs in discussions with others. The role includes highlighting and focusing on benefits and risks for the business line and identifying the appropriate timing (for example, during periods of lower volumes) of implementation and releases. The business change manager plans and manages the integration of the changes in business line systems or processes, including identifying new business processes, to meet strategic objectives. A project or program may have multiple business change managers representing their respective lines of business. The business change manager defines and monitors key performance indicators to objectively measure the project's or program's success. The business change manager translates the technical aspects and benefits of a project or program into a format that is understandable to and executable by business line management and staff. Business change managers plan and manage business continuity during and immediately after the change takes place.
- **Project or program management office or organization (PMO) personnel:** Traditional project management methodologies, such as waterfall, typically centralize project governance through the PMO. The entity's size, complexity, and project types determine the number and qualifications of PMO personnel. Larger or more complex entities often have numerous PMO personnel to coordinate the projects and programs undertaken by an entity. Smaller or less complex entities often do not have designated PMOs or dedicated project personnel. The IT project's size and complexity determine the PMO's extent of engagement. Beyond keeping projects on track and identifying and removing obstacles, PMO activities

generally involve analyzing the project's feasibility and risk; determining whether to develop, acquire, or outsource systems and components; ensuring quality of deliverables; and verifying that the project delivers value to the entity and affected business units.

- **Stakeholders:** Stakeholders should be involved early in the planning process to provide input before finalizing project requirements. In addition, regular communication between project managers and stakeholders helps to ensure that stakeholders agree with the project's proposed direction. The list of potential stakeholders can be internal or external and may include the following individuals:¹⁶

Internal stakeholders	External stakeholders
Board of directors	Customers, consumers of critical services, or financial institution clients of a third party
Senior management	Third parties (e.g., service providers, suppliers, or partners)
Heads of business lines, especially critical service owners	User groups
Relevant internal business unit personnel (e.g., IT, human resources, compliance, and legal)	Shareholders

II.B.3 Development Roles

Development personnel typically encompass the technology professionals charged with designing, building, and maintaining solutions to solve a business problem or fulfill technology needs identified by business strategy. Development personnel may create solutions to support new products offered to customers, expand existing system capacity to support growth, or integrate systems after a merger. Larger or more complex entities may have separate personnel or departments to fulfill development roles, or varying development roles may have more granular responsibilities (e.g., user interface developers, software engineers, or mobile application developers). In smaller or less complex entities, roles may overlap, which may be acceptable if appropriate mitigating controls are in place. Third parties may help the entity with or serve in development roles.

Segregation of duties and dual controls or other compensating controls are important for development, acquisition, and maintenance activities because they help foster security and resilience. For example, segregation of development and implementation duties helps ensure that developers cannot directly alter the production environment. Inappropriate developer access may adversely affect the production environment's confidentiality, integrity, availability, or resilience. Effective dual control allows management and other personnel to identify and address problems earlier since no single person or group can make changes or modifications without appropriate approval. Without dual control, seemingly small coding, building, and patching problems can quickly escalate in scale.

¹⁶ Refer to Cybersecurity and Infrastructure Security Agency (CISA), [CRR Supplemental Resource Guide, Vol. 3: Configuration and Change Management, Version 1.1](#). Also refer to CISA, [CRR Supplemental Resource Guide, Vol. 5: Incident Management, Version 1.1](#).

Typically, development deliverables are software applications or smaller modules of a larger application or system. Some larger or more complex entities, however, employ software engineering specialists to modify firmware, customize third-party-developed in-house applications, or adapt hardware products, such as automated teller machines (ATM), cash dispensers, and passbook or receipt printers to fit the entity's specific needs. Larger or more complex entities, especially those providing cloud, managed security, and payments services, often build proprietary hardware (e.g., servers or point-of-sale terminals) used in-house and by customers they service.

Staff roles that support development include the following:

- **Network architects:** Network architects generally design, select, and implement the appropriate system architecture to satisfy stakeholder requirements and achieve the desired results under given constraints. Network architects often have extensive knowledge of the entity's business plan to design a network to help the entity achieve its strategic objectives. They create plans and layouts for data communication networks and present those plans to management; explain risks; and justify recommended designs, changes, and consequences of inaction. They consider security when designing networks and systems. Once network architects define the appropriate architecture, they generally document and communicate it to the developers. Network architects upgrade hardware and software as needed to support solutions. After deployment, they may support those networks and troubleshoot any issues. When needed, network architects research new or emerging technologies to determine whether they are appropriate to implement for the entity. They evaluate network traffic to estimate growth and determine capacity management needs. Network architects may work with other IT personnel, such as network or system administrators and information systems managers, to ensure that networking needs are met. They work with third parties to manage upgrades and support the networks. Larger or more complex entities may define additional roles for enterprise architecture, including software and hardware architecture.
- **Developers:** Developers create software and the underlying systems and components to support an entity's business lines and strategic objectives, including security and resilience. They analyze users' needs and design and develop software to meet those needs, including how the systems or components will work together. Developers should have a clear understanding of user requirements and needs to ensure that deliverables meet user expectations. Developers document every aspect of a system or component as a reference for future maintenance and upgrades. They help ensure that a program continues to function normally through regular maintenance and, when necessary, recommend upgrades to keep pace with technology and security needs. They communicate with quality management personnel and testers to ensure that the system or component operates as envisioned. Developers may specialize in a particular language, platform, or business sector and may work individually in small or large teams.
- **Software engineers:** A software engineer is a type of developer who has a broad view of a project's system and software requirements and plans its scope and order of work. Software engineers may direct software developers, QA analysts, and testers.¹⁷
- **Hardware engineers:** Hardware engineers typically design new hardware. As part of the

¹⁷ Refer to the U.S. Bureau of Labor Statistics' [Occupational Outlook Handbook, "Software Developers, Quality Assurance Analysts, and Testers."](#)

design process, hardware engineers create schematics of equipment to be built and test the hardware. They analyze test results and modify the design as needed. Hardware engineers often work with developers to ensure that hardware components work together with the latest software. Additionally, hardware engineers oversee the manufacturing process for hardware. Many hardware engineers design devices used in manufactured products that incorporate processors and other computer components and that connect to the internet (e.g., point-of-sale terminals, card readers, and ATMs).

- **Information security analysts:** Information security analysts plan and carry out security measures to protect an entity's networks and systems. They work with developers to build security into systems and components and maintain the security aspects once developed. The role specializes in building and performing security assessments, identifying threats to systems, and ensuring that the software complies with the entity's security standards and policies. Information security analysts should have an enterprise-wide understanding of the entity's security architecture and interoperability of systems and components.
- **Systems analysts:** Systems analysts can also be referred to as systems architects. Systems analysts use their knowledge of the entity's systems, procedures, and technology needs to help IT personnel design systems that operate more efficiently and support the enterprise-wide business and strategic objectives. Systems analysts work with other IT personnel to help an entity's business leaders understand how systems and components support the entity's strategic and business line goals and objectives. Systems analysts devise ways to add functionality to systems by researching different technologies and analyzing costs and benefits of changing, upgrading, or implementing new IT systems to help managers decide which, if any, to install. Systems analysts validate the communication and interface between systems to ensure that they continue to function. They work with other IT personnel to evaluate system capacity needs. They work with business personnel to write instruction manuals and train the systems' end users. Additionally, systems analysts may work with other IT personnel to solve problems that arise after the initial system setup.

II.B.4 Acquisition Roles

Acquisition personnel typically procure systems or components. Larger or more complex entities may have separate individuals, teams, or departments responsible for acquisition. Acquisition personnel are often assisted by representatives from several departments, such as project management, IT, contracting, finance, information security, legal, and third-party risk management. Acquisition-related roles may be broken down further into the product or service type purchased (e.g., technology component). At smaller or less complex entities, the acquisition role often is one of multiple duties assigned to an individual (e.g., IT manager or president), which is acceptable if mitigating controls are in place. Additionally, third parties may perform the entity's acquisition activities (e.g., cloud access security broker). Segregation of duties, dual controls, and other compensating controls are important in acquisition activities to avoid conflicts of interest (e.g., choosing third parties based on relationships versus whether the third party provides the appropriate product, best service, or most advantageous price). Depending on whether the entity chooses to develop IT solutions or procure them from third parties, acquisition roles may vary.

General responsibilities include specifying what is required, requesting proposals, receiving bids from third parties, evaluating bids and bidders, initiating contracts, and managing contractual relationships. Responsibilities also include evaluating supply chain risks related to third parties (e.g., geopolitical risk for third parties outside the United States). These responsibilities may require specialized knowledge to evaluate pricing and other aspects (e.g., contract terms or support services) of the relationship. Responsibilities are carried out throughout the entire life cycle of the third-party relationship.¹⁸ For more information, refer to the “[Acquisition](#)” section of this booklet.

Roles that support acquisitions include the following:

- **Procurement manager:** A procurement manager can also be referred to as a third-party risk manager or business relationship manager. The procurement manager is responsible for the procurement strategy being consistent with the entity’s overall strategy and risk appetite. Procurement managers are responsible for developing the entity’s procurement policies, standards, and procedures to help ensure that procurement personnel avoid potential conflicts of interest or inappropriate third-party relationships. Procurement managers evaluate third parties based on the price, quality, functionality, and delivery speed of products and services. They verify that vendor processes align with the entity’s requirements (e.g., security and resilience) by interviewing vendors and visiting third-party facilities. They analyze proposals, financial reports, and other information to determine reasonable costs, negotiate contracts on the entity’s behalf, and arrange agreements with third parties (e.g., service-level agreements [SLA] or product delivery time frames). Procurement managers evaluate and monitor contracts to ensure that third-party management complies with the contract’s terms and conditions (including compliance with applicable laws and regulations) and determine the need for changes. When necessary, procurement managers meet with entity and third-party management to discuss defective or unacceptable products or services and determine corrective action. Procurement managers maintain and review records of items bought, costs, deliveries, product performance, and inventories. They may attend meetings, trade shows, and conferences to learn about new industry trends and make contacts with potential third-party partners. Procurement managers may work with other personnel, including those in program management, IT, information security, or business lines involved in the project.
- **Third-party risk manager:** This role can also be referred to as third-party relationship manager and may also be the same person as the procurement manager. This role involves performing due diligence on third parties before procuring systems, components, or contracting for services (e.g., development or information security activities). When appropriate, the third-party risk manager performs ongoing oversight over third parties throughout the relationship’s life cycle.

¹⁸ The term “business arrangement” may also be used and is meant to be interpreted broadly; it is synonymous with the term “third-party relationship.” A third-party relationship may exist despite a lack of a contract or remuneration. Third-party relationships can include outsourced services, use of independent consultants, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures.

II.B.5 Maintenance Roles

Appropriate personnel should perform maintenance throughout the life cycle of systems and components. Some responsibilities assigned as part of maintenance include asset management (including end-of-life [EOL] and end-of-support [EOS] management), patch management, vulnerability management, and performance and capacity management. Management should understand maintenance roles and related responsibilities. Maintenance personnel should have knowledge and understanding of all relevant systems and components they are expected to operate and maintain. Both maintenance personnel and management should analyze, document, and understand the costs of maintenance (e.g., budget, time, or personnel) versus the costs of not performing maintenance (e.g., system failures, data breaches, and customer dissatisfaction). Larger or more complex entities may have separate individuals, teams, or departments charged with maintenance. At smaller or less complex entities, maintenance roles may be part of other roles or duties that an individual may have, which is acceptable if mitigating controls are in place (e.g., segregation of duties and dual controls). Additionally, third parties may perform responsibilities related to maintenance for the entity, according to contractual agreements.

IT staff are generally responsible for maintaining an entity's systems and components to ensure that they continue to operate as expected. Maintenance generally includes performing updates and applying patches, monitoring the systems' or components' status, and monitoring the servers and infrastructure that support the entity's systems and components. Maintenance roles may have more granular responsibilities (e.g., network support) depending on the complexity of the entity's IT environment. Maintenance roles should be independent from development roles to prevent developers from accessing production environments. For more information, refer to the "[Maintenance](#)" section of this booklet.

II.B.6 Other Common Development, Acquisition, and Maintenance Roles

Depending on the entity's size and complexity, the following roles are common to development, acquisition, and maintenance activities:

- **Configuration or change control board (CCB):** The CCB is "a group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system."¹⁹ The CCB typically is part of an entity's change management process, and it reviews and prioritizes change requests related to a project or production environment.
- **Testers and quality assurance analysts:** During development, acquisition, and maintenance, testers and quality assurance analysts create test plans, scenarios, and procedures for new or changed systems and components to confirm that they function as intended. Testers are responsible for testing systems, components, and controls regardless of whether they are developed internally or procured from a third party. Testers design and conduct tests to check systems and components for problems. They identify, document, and

¹⁹ Refer to [NIST Glossary](#).

report risks from test results and recommend steps to minimize or resolve risks or defects. They assess the usability and functionality of systems and components to identify issues, including difficulties a user might have. They can use manual or automated processes, with additional testing as necessary, and evaluate results. Testers document the results of testing and report defects or problems to developers, project teams, and other stakeholders. Once the system or component is released to production, testers run additional tests to look for errors and usability problems. They perform tests after any upgrades, maintenance, or implementation of patches and fixes on a system or component to validate the changes made. Depending on the types of tests performed (e.g., unit, security, regression, and integration), other testers may be involved at various SDLC phases, based on the testers' roles and knowledge of the system or component and its use. For more information, see the "[Testing](#)" section in this booklet.

II.B.7 Supply Chain Roles

Typically, supply chain personnel are responsible for implementing and managing systems and components throughout the entity's supply chain. Larger or more complex entities may have separate individuals, teams, or departments charged with supply chain roles and responsibilities. These personnel may include representatives from several key departments, such as development, procurement (including logistics and product delivery), maintenance, project management, IT, contracting, finance, information security, and third-party risk management.

Common internal roles may be the chief risk officer, CIO, CISO, program executive, program manager, system engineers or system security engineers, and other personnel. Common external supply chain roles may be suppliers, developers, system integrators, third-party system service providers, and other external personnel responsible for supply chain activities as noted in agreements (e.g., contracts) between the entity, third parties, and their subcontractors.²⁰

II.B.8 Other Support Functions

Several lines of business and other support functions should be involved in overseeing or validating development, acquisition, and maintenance activities early in the process. One of those functions may be end-user and customer support, often referred to as the IT help desk. The end-user and customer support role works with development, acquisition, and maintenance personnel to respond to user or customer concerns. This role may also assist with resolving problems that cannot be corrected quickly. Moreover, this role provides feedback to development, acquisition, and maintenance personnel about the functionality of products and services. This role records the details of customer or user interactions and the resolution of problems. End-user and customer support staff should understand the escalation process and the personnel who can address more complex problems.

²⁰ For more information on common external supply chain roles, refer to NIST Special Publication (SP) 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

II.B.9 Audit's Role

An effective audit function provides independent, objective validation of controls and statements of assurance on the effectiveness of an entity's development, acquisition, and maintenance activities. Although auditors should not have any direct involvement in management decisions, they should raise objections if they believe the control environment is inadequate. Auditors may plan for their advisory capacity in development, acquisition, and maintenance activities by developing an understanding of the proposed system or changes. Auditors may require specialized knowledge of IT to advise on or review these activities. They should validate schedule adherence and management. Auditors should determine the effectiveness of controls in the entity's development, acquisition, and maintenance activities and recommend appropriate mitigation. They may communicate with developers regarding appropriate control standards and frameworks throughout IT projects.

Auditors do more than consult when reviewing controls in new or modified systems or components. In smaller or less complex entities, auditors typically assess an entity's development, acquisition, and maintenance activities during an "IT general controls"²¹ audit. Larger or more complex entities may have a dedicated IT audit function, which generally follows a risk-based approach to prioritize the review of numerous IT processes and controls. These entities may have separate audits to assess general processes, such as development, acquisition, or maintenance, or may review these activities as part of business line, project, or other technology audits. During each SDLC phase, auditors review the internal controls, testing, and audit trails included in systems and components.

Auditors may participate in an advisory capacity in IT projects and may perform pre- and post-implementation reviews. Post-implementation reviews should occur shortly after implementing the new or revised system or components. These reviews help validate that the system or component operates as expected and provide financial statement users with relevant information in ways that justify the cost of providing it.

In larger or more complex entities with numerous IT systems and components, formal quality management or change management groups may have primary responsibility for post-implementation reviews. In such cases, auditors may choose not to perform a separate review; however, they may participate in validating minimum test criteria and evaluating the results of reviews.

Auditors' validation activities regarding IT projects or change management may include reviews for the following:

- Project or changes were authorized.
- Project or changes were subjected to a risk-impact assessment.
- Project or changes were handled effectively and formally documented, especially when it was an emergency change.

²¹ While "IT general controls" is a typical name for all-encompassing IT audits, entities may use various names for these reviews.

- Project or changes were prioritized among all other IT projects or changes in a manner that is effective for the entity.
- Project or changes were tracked by a formal process.

For more information, refer to the *FFIEC IT Handbook's* “[Audit](#)” booklet.

III RISK MANAGEMENT OF DEVELOPMENT, ACQUISITION, AND MAINTENANCE

Action Summary

Management should implement continual risk management processes within the entity's development, acquisition, and maintenance activities to identify, measure, monitor, and control reasonably foreseeable internal and external risks and threats, including those that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

Examiners should review the following:

- Policies, standards, and procedures for identifying, measuring, mitigating, monitoring, and reporting risks related to development, acquisition, and maintenance activities.
- Documented processes and metrics used to measure the level of risk.
- Detailed documentation of processes used to review, accept, and document risks that management cannot mitigate or transfer.
- Documentation of risk assessment processes to identify key risks at the onset of IT projects and throughout their life cycles.
- Risk assessments that highlight internal and external risks related to development, acquisition, and maintenance activities.
- Documentation of ongoing processes and reports to monitor and communicate risk, including emerging risks related to development, acquisition, and maintenance activities.
- Reports to stakeholders that are timely, accurate, and include clear, relevant metrics.

Management should identify, measure, monitor, and control reasonably foreseeable internal and external risks and threats, including those that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.²² While the requirement is relative to risks to sensitive customer information, it is a prudent practice relative to any sensitive information type. Additionally, management should consider risks that could result in a severe disruption or material compromise to critical service delivery. It is also important to consider known risks related to developed or acquired products and systems,²³ and

²² Refer to 15 USC 6801 and 6805(b), "[Financial Services Modernization Act of 1999](#)" ([Gramm–Leach–Bliley Act or GLBA](#)), further implemented by FFIEC members as follows: FDIC: 12 CFR 364, appendix B, "[Interagency Guidelines Establishing Information Security Standards](#)"; FRB: Regulation H, 12 CFR 208, appendix D-2, "[Interagency Guidelines Establishing Information Security Standards](#)"; and Regulation Y, 12 CFR 225, appendix F, "[Interagency Guidelines Establishing Information Security Standards](#)"; NCUA: 12 CFR 748, appendix A, "[Guidelines for Safeguarding Member Information](#)"; and OCC: 12 CFR 30, appendix B, "[Interagency Guidelines Establishing Information Security Standards](#)." Additionally, refer to Federal Trade Commission (FTC) 16 CFR 314, "[Standards for Safeguarding Customer Information](#)."

²³ Developed or acquired products and services may include hardware (e.g., servers, laptops), software (e.g., application programming interfaces), or services (e.g., banking-as-a-service).

any known potential misuses. IT risk management activities should include policies, standards, and procedures for identifying, measuring, mitigating, monitoring, and reporting risks related to development, acquisition, and maintenance activities. Additionally, management should consider using threat models to assess security policies, standards, and procedures. While there are many widely used threat modeling methodologies, it is important for entity personnel to consider implementing a model commensurate with the threats in the entity's overall environment.

Risk management activities include identification of risks associated with development, acquisition, maintenance, and associated IT projects, including the risks associated with not initiating a project.²⁴ Examples of risk management activities to consider include the following:

- Measuring each activity's level of risk.
- Mitigating risks to an acceptable, board-approved level of residual risk.
- Monitoring risks related to development, acquisition, and maintenance activities.
- Reporting updates to senior management and the board, as necessary.

At times, management may choose to transfer some of the risk, such as by purchasing insurance (e.g., errors and omissions or cyber) to address the potential for unknown errors in source code. When management cannot mitigate or transfer risk, there should be a process to review, accept, and document the risk and its acceptance by the board. For an acquisition, management and the board may decline to move forward if the risk level exceeds the board's risk appetite (e.g., purchase of a product that uses an amount of open-source code above approved levels). Management and the board should regularly review and approve risk acceptance decisions consistent with the entity's governance structure. For more information about risk management, refer to the *FFIEC IT Handbook's* "[Management](#)" booklet.

III.A Risk Identification

Risk identification involves identifying and documenting risks that may affect development, acquisition, and maintenance activities. Effective risk identification is a continuous process that includes iterative reassessment of risks. Identifying key risks related to development, acquisition, and maintenance activities gives management opportunities to implement appropriate controls and mitigate risks. Identifying key risks at the onset of an IT project allows for early assessment of risks, risk effects, and risk mitigation options. For example, a code review helps developers find errors before migrating code between the test and the production environments. Ideally, risk identification and assessments involve stakeholders with business process knowledge who may be affected by the development, acquisition, or maintenance activities or the related IT projects. As always, information security concerns should also be considered.

Risk identification highlights internal and external risks related to development, acquisition, and maintenance activities. Examples of internal risks include insider threats (e.g., trusted employees who use authorized access in an unauthorized manner for personal gain, entity harm, or errors and omissions) and scheduling difficulties (e.g., loss of knowledgeable personnel or

²⁴ There is a strong relationship between the phases in the SDLC, the SCRUM life cycle (both discussed in this booklet), and the third-party risk management life cycle, referenced in the [Interagency Guidance on Third-Party Relationships: Risk Management](#).

unavailability of skilled personnel). Examples of external risks include those arising from third-party relationships, industry threats and changes (e.g., new products or services, regulatory changes, or new cyber threats), and natural disasters. Additionally, financial technology (fintech)²⁵ firms and other third-party relationships may not be subject to the same regulatory requirements as the entity. Management is responsible for holding the third party accountable to the entity's standards (e.g., compliance with regulations and adherence to security and resilience standards) and the board's risk appetite.

III.B Risk Measurement

Management should implement effective standards to measure risk in the entity's development, acquisition, and maintenance activities. Risk measurement should be an ongoing process and commensurate with the size and complexity of an entity's activities. As the complexity of an entity's activities and processes increases, management may benefit from using automated tools to help measure risk. Effective risk measurement processes include management setting and monitoring objective standards for performance. Examples of risk measurement related to development, acquisition, and maintenance include the following:

- Comparisons of estimated versus actual completion dates for IT project deliverables.
- Number of open issues related to projects and the length of time issues remain open.
- Percentage of occasions when management needed to back code out of production.
- Cost overruns greater than the entity's established limits.
- Service levels below those defined in contracts and agreements.
- Number of unapplied patches or patches applied beyond the policy time frames.
- Policy exceptions.

III.C Risk Monitoring and Reporting

Effective management monitors and reports risks related to development, acquisition, and maintenance activities. Examples of risks monitored by management include project management (e.g., milestone date shifts, negative test results, and major requirements changes), cybersecurity, supply chain, and emerging technology. Reports of these risks should be timely and accurate; include clear, relevant metrics (e.g., trends related to the number of open issues or code back-outs); and note deviations from policies, standards, and procedures. Reports should be distributed to appropriate stakeholders, including the board when necessary. Management should communicate technical aspects that are easily understood (e.g., explaining acronyms or technical jargon) when reporting to the entity's board and relate the IT issues to the entity's business concerns. Effective monitoring and reporting inform management about problems and performance issues in a timely manner, so that management can minimize the potential for an increase in the levels of risk associated with identified issues. Monitoring and reporting should enable all stakeholders to understand the risks and agree with the proposed courses of action.

²⁵ For purposes of this booklet, "fintech" refers to using technology in novel ways to provide financial services.

III.D Controlling or Mitigating Risk

Risk mitigation relies on identification and monitoring of risk in conjunction with the board's risk appetite. These limits should assist in limiting exposure to the various risks associated with the entity's IT-related activities. Implementation of effective operational controls to address these risks are described throughout this booklet. One example of risk mitigation is implementing code reviews during development to detect and correct errors earlier in the development process that might cause the system or component to fail. Effective management adopts repeatable control processes to ensure that risks are consistently addressed across the entity over time.

IV COMMON DEVELOPMENT, ACQUISITION, AND MAINTENANCE RISK TOPICS

Action Summary

Management should implement effective risk mitigation throughout development, acquisition, and maintenance activities regardless of the phase of the project in the life cycle and agnostic as to the type of technology. Specific risks and controls should be considered depending on management's chosen solution.

Examiners should review the following:

- Systems, components, and services, including related contracts and licenses, throughout the supply chain for appropriate risk identification and mitigation.
- Security controls (e.g., secure coding requirements and baseline configuration use) used to harden systems and components.
- Inventory of all systems and components (e.g., open-source, proprietary, application programming interfaces [API], and container images and registries), including related licenses, and data as part of IT asset management (ITAM).
- Access, authentication, and authorization controls for systems, components, data, and related documentation throughout the supply chain to ensure appropriate security.
- Segregation of duties in development, acquisition, and maintenance activities.
- Process of selecting and implementing methodologies to enable effective management and control of development, acquisition, or maintenance projects and alignment with entity objectives.
- Operating parameters (e.g., timing, speed, throughput, and data validation) for systems and components to determine performance.
- Activity logs related to systems, components, and data to identify operating risks.
- Monitoring processes of development and maintenance activity for identification of anomalies and unauthorized access or modification to systems, components, and data.
- Reporting processes for decision-making and measuring the level of project success.
- Training on development, acquisition, and maintenance concepts (e.g., methodologies); effectiveness of training; and capability of personnel to implement concepts learned.
- Documentation of internally developed systems and components and externally procured products and services to effectively operate and maintain the systems and components.
- Evaluation process (e.g., post-implementation review, stakeholder interview, problem documentation and resolution, cost-benefit analysis, and reports to senior management) for development, acquisition, and maintenance projects.

IT systems are designed, built, and implemented to achieve strategic goals and business objectives. While there are risks specific to each of the development, acquisition, and maintenance activities, certain risk considerations are common to all three. Common

development, acquisition, and maintenance risk topics are discussed in the following subsections of this booklet:

- “Open-Source”
- “Commercial-off-the-Shelf”
- “Licenses, Agreements, and Copyright Protection”
- “Secure Development”
- “Data”
- “Secure Operating Environments”
- “Microservices”
- “Containers”
- “Application Programming Interfaces”
- “Quality Management”
- “Documentation Standards”
- “Post-Implementation Review”
- “IT Project Management”
- “System Development Life Cycle”
- “Supply Chain Considerations”

IV.A Open-Source

Open-source software is software released under a license that allows the software and its source code to be accessed, used, modified, and shared by anyone.²⁶ Effective management identifies and mitigates risks related to the use of open-source components (e.g., open-source software components and hardware components). For example, components may be based on poorly written code, or the developer may not have properly addressed security concerns. Open-source vulnerabilities may be more common depending on the underlying code’s quality because the overall review process for open-source is less transparent and more difficult to validate. If the original developer makes updates, they may not be pushed to the entity. In that case, effective management would request updates from the original open-source developer to address vulnerabilities and manually deploy updates. Alternatively, when the original developer does not make updates to open-source systems and components, effective management may engage in-house or third-party software development personnel to update the software.

The Open Worldwide Application Security Project (OWASP) recommends the following component analysis²⁷ strategies to reduce risks associated with the use of open-source components:²⁸

²⁶ For more information, refer to NIST Directive S 6106.01, “[Open Source Code](#).”

²⁷ OWASP defines “component analysis” as “the process of identifying potential areas of risk from the use of third-party and open-source software and hardware components.”

²⁸ For more information, refer to OWASP, [Component Analysis](#).

- Evaluating the type of framework and libraries to reduce architectural changes, regressions (or defects), and code rewrites.
- Identifying and analyzing the purpose of each component to reveal the existence of components with duplicate or similar functionality.
- Evaluating the number of third-party and open-source components in a project because the higher the number, the more difficult it is for development teams to maintain large sets of components over time.
- Using private central repositories²⁹ or public repositories' code-signing and verification tools to minimize risk of threats³⁰ related to public repositories.
- Identifying a component's provenance³¹ to help ensure knowledge of authorship of software components, manufacturers, suppliers, software repositories, and country of origin.
- Maintaining accurate formulation³² and pedigree³³ information for source code that is readily available, modifiable, and redistributable.
- Identifying the license for a given component and whether it allows certain types of usage, contains distribution requirements or limitations, or requires specific actions if the component is modified.
- Aggregating the risk of all direct, transitive, runtime, and environmental dependencies providing a holistic view of inherited risk.³⁴

²⁹ A “[repository](#)” is defined as “a place, room, or container where something is deposited or stored.” For purposes of IT, repositories may store requirements, policies, processes, data, software libraries, projects, configurations, performance goals, and applications, with the potential of supporting both software development and operations management.

³⁰ Some of the threats against public repositories include typosquatting (i.e., naming a component to take advantage of common misspelling); organization/group abuse (i.e., pretending to be a public person or entity and abusing the perceived trust); malware through transfer (i.e., leveraging weak or absent code-signing requirements to spread malware through the transfer of an open-source project from one maintainer to another); and cross-build injection (i.e., abusing dependency resolution schemes and weak infrastructure controls to inject malicious components in place of safe ones).

³¹ For purposes of this discussion, the identification of a component's provenance refers to the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It can include personnel and processes used to interact with or make modifications to the system, component, or associated data.

³² OWASP describes “[formulation](#)” as “how components were built...and a comprehensive list of parallel and sequential steps that were taken to build, test, and deliver a component.”

³³ NIST Glossary defines “[pedigree](#)” as “the validation of the composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software this includes the composition of open source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid.”

³⁴ Inherited risks are derived from an application's transitive dependency (i.e., when an application or component has a direct dependency on another component and that component then has a dependency on another component) or direct dependency on every component. Transitive dependencies have their own risk that is inherited by every component and application that relies on them. Refer to OWASP, [Component Analysis](#).

- Evaluating the health of an open-source project through quality controls and metrics (e.g., frequency of code changes and patches), community engagement (e.g., user base and involvement), and vulnerability analysis.
- Including external services (such as those relied on for functionality) in the overall inventory of components.

During software evaluation, a review of the open-source developer's formal documentation helps management determine potential software maintenance risks after software selection. Open-source documentation may be less comprehensive when compared with documentation for proprietary systems and components. Effective management proactively maintains updated application and user documentation, especially when code changes are made.

For more information, refer to the *FFIEC IT Handbook's* "[Information Security](#)" and "[Architecture, Infrastructure, and Operations](#)" booklets.

IV.B Commercial-off-the-Shelf

Commercial off-the-shelf (COTS) systems are systems, components, or solutions that are ready-made and available for sale, lease, or license to the general public. COTS is also referred to as off-the-shelf. Entities typically use COTS for operating systems (OS), applications, network infrastructure, servers, desktops, laptops, and mobile devices. Entities often choose to use COTS because it generally is less costly than developing systems and components in-house and requires fewer resources to maintain. COTS solutions generally provide a default set functionality. For example, a default installation of a server OS may include mail, web, and file-sharing services whether or not the solution requires those functions. This is because COTS providers may be developing their products to serve a wide variety of customers, not just those in the financial industry. Therefore, unnecessary services may be present in COTS and represent potential security weaknesses (e.g., unnecessary services creating a wider attack surface), which should be mitigated (e.g., turned off or patched). Protection against those risks begins when the systems or components are constructed and installed through a process referred to as "hardening." Management should consult third-party providers and vendors regarding recommended security controls to harden the COTS solution. Hardening can involve employing recommendations in a documented installation procedure and generally includes the following:

- Changing default passwords.
- Installing the most secure, up-to-date versions of applications.
- Configuring security settings as appropriate.
- Enabling logging.
- Configuring backups to increase resilience.

A COTS solution may be integrated with existing systems and components to provide additional or enhanced business services to internal and external customers. Management should mitigate any risks related to integration (e.g., lack of interoperability or integration between systems and components). If modifications are made, the process to develop and implement them may be time-consuming and challenging. These modifications may result in additional configuration changes for COTS, or interface changes between COTS and other systems and components (e.g.,

APIs, middleware, and cloud). These changes may then require additional resources and personnel to perform. For more information, refer to the *FFIEC IT Handbook*'s "[Information Security](#)" and "[Outsourcing Technology Services](#)" booklets.

IV.C Licenses, Agreements, and Copyright Protection

Systems and components are often licensed, not purchased. Typically, licenses do not give a client (sometimes referred to as a licensee) ownership rights over the licensed product. The licensor³⁵ provides licenses to clients that grant certain rights to use the system or components. The licensor typically grants rights to a client for a specific duration and may charge annual and other fees for system or component use. An effective license and agreement review process at the entity is important to ensure that terms are clearly defined and understood prior to engagement. Before negotiating licenses, management should accurately assess current and future needs and ensure that licenses will continue to meet the entity's needs.

The defined scope of a license is a key issue in evaluating and, when feasible, negotiating the terms of a licensing agreement. When reviewing a license, management should confirm that it clearly states whether system or component usage is exclusive, the number of user licenses, and whether there are any time, place, manner, or other types of limitations with the system or component's use. Effective management reviews licenses to determine whether they allow backup copies related to mission-critical systems or components on which the entity may need to rely for disaster recovery or business continuity purposes. The entity may need to negotiate with licensors to ensure the ability to backup hardware and software if backups are not provided for in the license. In difficult license agreement negotiations, including when an entity has limited negotiating power, management should understand any resulting limitations and consequent risks. Possible actions that an entity might take in such circumstances include determining whether the product or service can still meet the entity's needs, whether the product or service would result in increased risk to the entity, and whether residual risks are acceptable. If the license agreement is unacceptable for the entity, management may consider other approaches, such as employing other third parties or conducting the activity in-house. In certain circumstances, entities may gain an advantage by negotiating license agreements as a group with other entities (e.g., user groups and banking associations).³⁶

If the entity plans to provide the systems or components to other related entities (e.g., subsidiaries or contractors), management should include those entities as users in the licenses. If management is responsible for developing systems and components and providing them to other entities or its subsidiaries, management should implement appropriate licenses for the systems or components developed.

Knowledge of license expiration dates is crucial for the planning and management of license renewal. If there is no license expiration or the license renews automatically (i.e., a perpetual

³⁵ A "[licensor](#)" is defined as "the person who gives or grants a license."

³⁶ For more information, refer to [Interagency Guidance on Third-Party Relationships: Risk Management](#). Specific agency references to this document include ([FDIC](#)) [FIL 29-2023](#), ([FRB](#)) [SR Letter 23-4](#), and ([OCC](#)) [Bulletin 2023-17](#).

license), the license agreement should explicitly outline those terms. Failure to specify a fixed term or termination date does not automatically provide the entity with a perpetual license. Management should specify in its agreement the appropriate time periods for all licenses and the minimum amount of notice required for license termination. Effective licensing and ITAM processes include tracking license time frames.

Effective management periodically reviews system and component licenses to compare all installed licensed systems and components with the respective license terms. This allows management to detect unauthorized installations and validate appropriate license use. If there is a discrepancy between the total number of licenses allowed by the agreement and the installed software, management should address the inappropriate usage. Audit personnel should consider this when developing the scope of their reviews.

There are several other types of agreements management should consider and review in addition to licenses. For example, a third party may offer maintenance agreements, which outline available maintenance services (e.g., provision of new versions, releases, or updates). Another type of agreement is a development agreement, which outlines terms for the development of systems or components. This agreement may be internal or with a third party. If the agreement involves a third party, the entity may not retain ownership rights even if the entity paid to have the system or component developed.

A license or agreement should address the availability and cost of system and component updates and modifications (i.e., maintenance). When drafting agreements, effective management determines whether a third-party vendor provides access to source or object code (“code”). Management should have the vendor’s permission and participation for modifications to the code for systems and components. Unauthorized modifications to the code may void maintenance agreements.

A license or agreement should direct third-party vendors to deliver appropriate documentation. This should include application and user documentation. Management should ensure that the agreement specifies that updated application and user documentation will be provided when any changes are made to procured systems or components.

IV.C.1 Software Licenses

Effective ITAM includes software license oversight. Software licenses have varying provisions and requirements for ownership and usage. It is important to consider license provisions and all consequences for violating provisions. In more critical instances (i.e., critical to providing business services), entities may engage specialized legal expertise to understand and mitigate software license risks. If an entity develops software and licenses that software to others, management should be aware of the liabilities that come with licensing activities, including considerations related to software maintenance, integration, compatibility, and fraud. Tracking and managing the usage and implementation of different types of licenses for which an entity paid helps ensure that the entity is operating within the licenses’ specific requirements. There are several types of software licenses, including free and open-source software licenses and proprietary licenses.

IV.C.1(a) *Free and Open-Source Software Licenses*

There are two types of free and open-source software (FOSS) licenses:

- **Public domain (and equivalent) license:** Public domain software is software not protected by copyright laws of any nation that may be freely used without permission of or payment to the creator and that carries no creator warranties.³⁷ This reduces creator liability relative to the software's use. Software creators may renounce software ownership and any usage limitations to ensure that the software is able to be used by anyone regardless of jurisdiction license requirements and to limit their liability.³⁸
- **Open-source license:** Typically, open-source software used by entities has some type of attached license. Companies often license open-source software through a third party that makes software use and maintenance easier. Just as with proprietary software licenses, it is important to understand the license provisions such as who owns the software source code, and any restrictions on what can be done with the software. Examples of open-source software license subtypes are lesser general public licenses, permissive licenses, general public licenses, and copyleft licenses.³⁹

FOSS is typically acquired and used in an as-is manner. An entity may not be aware of the developer(s) in public domain FOSS. There may or may not be updates made available for the software, and changes made to the software may be made by other individuals besides the developer. Risks associated with FOSS include the potential for unidentified or unpatched vulnerabilities and development changes by unknown parties. An accurate inventory of FOSS should be maintained as part of an effective ITAM process, and management should understand and abide by the requirements of FOSS licenses. Additionally, some licenses require users to contribute software additions or enhancements, or they may prohibit the use for commercial purpose or profit. Management should be aware of what information is shared when contributing an enhancement to the FOSS development community.

IV.C.1(b) *Proprietary Software Licenses*

In proprietary software licenses, the software publisher retains software ownership, and the entity and end users agree to accept and abide by the terms of the software licenses. A licensee and its employees may only use the software as allowed by the license and typically cannot copy, modify, or distribute the software and its underlying code. An end user license agreement (EULA) provides specifics regarding provisions or restrictions. EULAs typically apply to for-profit open-source software and non-open-source software, and they are often used for commercial purposes. Some examples of proprietary licenses include noncommercial use-only

³⁷ Refer to [NIST Glossary](#).

³⁸ For more information, refer to public-domain equivalent licenses, such as Creative Commons' [CC0](#).

³⁹ Copyleft is a general licensing method for making a program free while requiring all modified and extended versions of the program to be free as well. There are strong and weak copyleft licenses. Refer to Department of Defense (DOD), [DoD Open Source Software FAQ](#).

licenses, proprietary licenses, and trade secret licenses. Regardless of the types of licenses encountered, they often cover the following:

- Ownership rights of the software.
- Permission to use the software and usage rights.
- Number of users allowed to use the software.
- Inclusions or add-ons (e.g., support, maintenance, and software upgrades).
- Warranty terms.
- Installation location and frequency.
- Permissions and limitations regarding copying, modifying, and distributing software and the underlying code.
- Copyrights.
- Terms for license termination.
- Software performance guarantees.
- Penalties and fees for noncompliance.
- Length of the agreement and its terms.

For more information on ITAM, which includes management of software licenses, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" booklet.

IV.C.2 Hardware Licenses

Entities identify and manage hardware licenses in ITAM programs to ensure that their hardware use is consistent with agreements between the manufacturer, any third party, and the entity. Entities may access components (e.g., circuit boards, servers, switches, tokens, universal serial buses, mobile devices, service ports, and cameras) in solution development. Hardware licenses, like software licenses, should identify any limitations on hardware use.

If an entity licenses COTS hardware, the hardware may come as is and any alterations or modifications may void the warranty in the license. If the hardware is proprietary, items such as warranties, modifications, and maintenance should be included in the license agreement. If an entity builds hardware and then licenses that hardware to other entities, effective management maintains awareness of the liabilities that come with licensing activities, including considerations related to hardware maintenance, integration, compatibility, and fraud.

For more information on ITAM, which includes management of hardware and software licenses, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" booklet.

IV.C.3 Copyright Protection

Copyright laws⁴⁰ protect proprietary as well as open-source software. Examples of elements covered by copyright protections generally include the following:

⁴⁰ Refer to U.S. Copyright Office, [Copyright Law of the United States \(Title 17\)](#).

- **Reproduction:** The copyright owner maintains rights in any reproduction of the original work.
- **Adaptation:** The copyright owner has rights to adaptations based on the original work.
- **Publication:** The copyright owner has the right to distribute the work to the public.
- **Performance:** The copyright owner has the right to perform the work publicly.
- **Display:** The copyright owner has the right to display the work publicly.

Unlicensed system or component use or licensing agreement violations expose entities to litigation. Common challenges in deploying software, consistent with licenses and copyrights, include keeping track of deployed instances when the entity is large and decentralized, keeping track of deployed instances when deployments are made to virtual environments and are not automatically tracked, instances being shared when the license does not provide for sharing, and license limits on concurrent system or component use.

Measures that management may employ to protect against copyright violations include obtaining a site license that authorizes system or component use at all of the entity's locations, informing users of the rules governing site licenses, and acquiring an automated program that scans for unauthorized system or component use or copyright violations. While these measures may help identify copyright violations, the best control mechanism is a well-communicated corporate policy that management enforces and auditors validate for compliance.

IV.D Secure Development

Secure development is an approach to creating products and services that incorporates security into every phase of the product's or service's development and use. Secure software development includes practices "to reduce the number of vulnerabilities in released software, to reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and to address the root causes of vulnerabilities to prevent recurrences."⁴¹ While this booklet primarily focuses on the secure development of software, there are also techniques for securely developing hardware.⁴² System, component, and service development, acquisition, and maintenance inherently presents security risks. This is true whether the system, component, or service is developed internally or acquired.

When management outsources development to third parties, it should monitor the third parties' conformance to contract requirements, Information Security Standards,⁴³ and other legal and

⁴¹ Refer to NIST SP 800-218, [*Secure Software Development Framework \(SSDF\) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*](#).

⁴² For more information on mitigation of hardware development risks, refer to DOD's [*Securing Defense-Critical Supply Chains*](#).

⁴³ Refer to 15 USC 6801 and 6805(b), [GLBA](#), further implemented by FFIEC members as follows: FDIC: 12 CFR 364, appendix B, "[Interagency Guidelines Establishing Information Security Standards](#)," and 12 CFR 364, supplement A to appendix B, "[Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#)"; FRB: Regulation H, 12 CFR 208, appendix D-2, "[Interagency Guidelines Establishing Information Security Standards](#)," and Regulation Y, 12 CFR 225, appendix F, "[Interagency Guidelines Establishing Information Security Standards](#)"; NCUA: 12 CFR 748, appendix A, "[Guidelines for Safeguarding](#)

regulatory requirements. A third party providing development services should maintain policies, standards, and procedures that promote secure development consistent with the entity's requirements and the board's risk appetite. When acquiring systems and components, management should evaluate the third party's secure coding standards (e.g., through independent certification or audit) and consider related supply chain risks.⁴⁴ It is also important that third-party system or component developers use secure coding standards, that its use is independently verified, and that management reviews the verification. This is important to verify when products are initially purchased and to review periodically as products are updated and patched. Furthermore, system maintenance should consider security impacts of integration with legacy systems and components. For more information, refer to the *FFIEC IT Handbook's* "[Outsourcing Technology Services](#)" and "[Information Security](#)" booklets.

General software quality management practices contribute to secure systems and components. For example, when thorough testing results in functional flaws being corrected, security vulnerabilities can also be identified and corrected. There are quality assurance tests that can specifically identify security flaws such as fuzz testing⁴⁵ and penetration testing. There are also quality management tools such as secure code reviews and source code security analyzers⁴⁶ that can systematically and efficiently identify security vulnerabilities and other flaws for remediation. Entities that use these practices and tools are more likely to produce secure systems and components than those that do not.

Manual or automated code reviews help identify vulnerabilities. Manual code reviews⁴⁷ are performed by entity personnel or a third party and may be less costly than an automated code review.⁴⁸ However, limitations on reviewers' knowledge or experience may result in unidentified issues, such as syntax errors and code vulnerabilities due to human error. Additionally, manual reviews may not be effective for extensive volumes of testing. Automated code reviews, on the other hand, may be more sophisticated, can reduce human error, and generally provide more timely identification of weaknesses. These tools are scalable and can be continuously updated as technology and vulnerabilities evolve. Entities review software code that has been implemented to mitigate the risk that vulnerabilities may be introduced through routine updates and patches. If

[Member Information](#)"; and OCC: 12 CFR 30, appendix B, "[Interagency Guidelines Establishing Information Security Standards](#)."

⁴⁴ For more information on supply chain risks affecting development, refer to the "[Development](#)" and "[Supply Chain Considerations](#)" sections of this booklet.

⁴⁵ Fuzz testing refers to a black box software testing technique, which basically consists of finding implementation bugs using malformed or semi-malformed data injection in an automated fashion by tools referred to as "fuzzers," which are programs or scripts that submit some combination of inputs to the test target to reveal how it responds. For more information, refer to OWASP's [Fuzzing](#).

⁴⁶ According to NIST, "Source code security analyzers examine source code to detect and report weaknesses that can lead to security vulnerabilities."

⁴⁷ Manual code review is the process of personnel reviewing the source code line by line to identify possible vulnerabilities.

⁴⁸ Refer to NIST Internal Report (IR) 8397, [Guidelines on Minimum Standards for Developer Verification of Software](#).

an automated code review process is implemented, management should ensure that the embedded rules of the code review tools are appropriately configured and used. Management selects code review types that are effective for the entity's project and available resources, and management validates that the code review process meets its needs.

System vulnerability scanning is another tool for mitigating security risks during development.⁴⁹ Scanning software is implemented in development environments so that vulnerabilities are identified and remediated before they are exposed to users and exploited by malicious actors. Requirements for system vulnerability scanning can be included in contracts and ancillary agreements if the underlying system is critical enough. Entities also continue to scan systems for vulnerabilities once systems are deployed and being maintained to mitigate the risk that vulnerabilities are introduced as the system is upgraded. Refer to *FFIEC IT Handbook's* "[Information Security](#)" and "[Architecture, Infrastructure, and Operations](#)" booklets.

IV.E Data

Mitigating the risk of data compromise is important in addition to controlling software and system development. To mitigate the risk of data compromise, entity personnel establish and maintain data inventories that include data characteristics such as storage location, criticality, and sensitivity. They also implement and maintain controls that protect the data consistent with their characteristics. For example, an entity may implement a policy that highly sensitive data will not be used in development and test environments. Instead, an entity may create synthetic data to use in development and testing that is a proxy for the actual, highly sensitive data. Another control example is documenting system data use so that security engineers can implement controls that protect data throughout process execution.⁵⁰ For more information, refer to the *FFIEC IT Handbook's* "[Information Security](#)" and "[Architecture, Infrastructure, and Operations](#)" booklets.

IV.F Secure Operating Environments

Management should maintain a secure operating environment throughout development, acquisition, and maintenance activities whether entity employees are operating the system or a third party's employees are operating the system. Entities use various controls to secure operating environments, such as configuration management, access control, and business continuity planning and testing. Effective application of formal policies addressing the least privilege principle help control access to systems, components, and data. An effective entity establishes documented policies to communicate and implement operating environment controls and provides for periodic audits for validation of the controls to determine whether systems and

⁴⁹ Like network port and service identification, vulnerability scanning identifies hosts and host attributes (e.g., operating systems, applications, or open ports), but it also attempts to identify vulnerabilities rather than relying on human interpretation of the scanning results. Refer to NIST SP 800-115, [Technical Guide to Information Security Testing and Assessment](#).

⁵⁰ NIST states in SP 800-37, rev. 2, [Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#), that "such documentation includes, for example, data flow diagrams, entity relationship diagrams, database schemas, and data dictionaries."

components are functioning as intended. Additional operating environment control examples are listed below:

- Identifying personnel allowed to access development, test, and production environments.
- Determining under which conditions they may access systems, components, and data within production environments.
- Maintaining authorization procedures for granting and verifying access.
- Determining how long users require access.
- Segregating operating environments (e.g., development, test, QA, and production) and specifying access controls for each operating environment, while accounting for new business functions.
- Ensuring resilience when developing, acquiring, or maintaining systems, components, services, and data.
- Maintaining control over remote access (e.g., timing, location, personnel, and multifactor authentication [MFA]).
- Providing appropriate controls over access to and by specific devices.
- Maintaining business line and IT representation when determining security and resilience measures.
- Maintaining ITAM processes for current and planned assets.

For more information, refer to the *FFIEC IT Handbook*'s "[Architecture, Infrastructure, and Operations](#)," "[Outsourcing Technology Services](#)," and "[Information Security](#)" booklets.

IV.G Microservices

Microservices refers to an architectural and organizational approach to building systems that involves much smaller components than historical approaches and requires attention to mitigate risks that could be material. NIST defines "microservices" as "a set of containers that work together to compose an application." This includes a series of interconnected containers or applications working in coordination (referred to as "orchestration"). Microservices-based architectures and applications are prevalent in cloud-based systems but can also be run in non-cloud-based virtualized environments.

Traditionally developed, or monolithic,⁵¹ applications comprise multiple lines of code developed as a single application. To work properly, these applications reside on a single server or virtual machine. Any updates rely on an update to the entire application. By contrast, microservices-based applications consist of small, self-contained (i.e., containers), independent services that use APIs to communicate and work together. Each microservice has a singular purpose (e.g., messaging, calculations, or database access). Microservices are generally technologically heterogeneous and can be written in different languages, use different development platforms, and be spread across multiple servers or virtual machines. Because microservices architecture has independent containers working together to create an application, updates can be applied to any one independent container without having to update the entire application. Additionally,

⁵¹ A monolithic application (or [monolith](#)) refers to a single unit, as opposed to a microservice architecture, which comprises smaller, independently deployable services.

each microservice can be reused to create new applications. These properties of microservices facilitate scalability and a faster, more agile application development process.

During acquisition or development of systems using microservices, effective control practices are used to mitigate the risk of systems malfunctioning and risk of security incidents. An example of an effective control is deploying and using highly secure and stable service registries for tracking the services included in a system. A microservice has two broad functions:⁵²

- Business logic, which implements the business functionalities, computations, and service composition or integration logic.
- Network processes, which manage the interservice communication mechanisms and are built on top of the underlying OS-level network stack.

NIST provides four drivers underlying the design principles of microservices:⁵³

- Each microservice must be managed, replicated, scaled, upgraded, and deployed independently of other microservices.
- Each microservice must have a single function and operate in a bounded context (i.e., have limited responsibility and dependence on other services).
- All microservices should be designed for constant failure and recovery, and therefore must be as stateless⁵⁴ as possible.
- One should reuse existing trusted services (e.g., databases, caches, and directories) for state management.

Additionally, NIST provides a list of the following design principles for microservices:

- **Autonomy:** Ability to operate independently as a self-contained entity that delivers all of the functions of an operations stack.
- **Loose coupling:** Minimal dependency between services so the change in one service does not require a change in another service.
- **Reusability:** Use of a service in different ways for different purposes.
- **Composability:** Ability to be assembled easily and configured to meet specific needs.
- **Fault tolerance:** Property of a system that allows proper operation even if components fail.
- **Discoverability:** Ability to be located and identified using discovery services.
- **Alignment of APIs with business processes:** Aligning microservices, APIs, and business processes during the design phase allows for easier changes to the services when business processes change.

⁵² Refer to NIST SP 800-204A, [Building Secure Microservices-Based Applications Using Service-Mesh Architecture](#).

⁵³ Refer to NIST SP 800-204, [Security Strategies for Microservices-Based Application Systems](#).

⁵⁴ Refer to [NIST Glossary](#).

Because microservices can be replicated or deployed across servers, a microservice architecture generally has a directory for microservices to publish their locations, also referred to as a service registry. NIST provides the following strategies for service registry configuration:⁵⁵

- Service registry capabilities should be provided through servers that are either dedicated or part of a service mesh⁵⁶ architecture.
- Service registry services should be in a network that has been configured with certain quality of service parameters to ensure its availability and resilience.
- Communication between an application service and a service registry should occur through a secure communication protocol (e.g., hypertext transfer protocol secure or transport layer security).⁵⁷
- Service registries should be validated to ensure that only legitimate services perform the registration, refresh operations, and query the database to discover services.
- Service registration and service deregistration functions should follow the principles of bounded context and loose coupling. Management should set parameters for the processes of registration to and deregistration from the service registry.⁵⁸
- If a third-party registration pattern⁵⁹ is implemented, registration and deregistration should only take place after the performance of a health check⁶⁰ on the application service.
- A distributed service registry should be deployed for large microservices applications, and data consistency should be maintained among multiple service registry instances.⁶¹

⁵⁵ [Ibid.](#)

⁵⁶ NIST SP 800-204A, [Building Secure Microservices-Based Applications Using Service-Mesh Architecture](#), defines “service mesh” as “a distributed computing middleware that optimizes communications between application services.”

⁵⁷ NIST defines “transport layer security” as “an authentication and security protocol widely implemented in browsers and web servers.” For more information, refer to NIST SP 800-63-3, [Digital Identity Guidelines](#).

⁵⁸ As noted in NIST SP 800-204, [Security Strategies for Microservices-Based Application Systems](#), the application service should not have tight coupling with an infrastructure service, such as a service registry service, and service self-registration and deregistration patterns should be avoided. When an application service crashes or is running but unable to handle requests, its inability to perform deregistration affects the integrity of the whole process. Therefore, registration and deregistration of an application service should be enabled using a third-party registration pattern, and the application service should be restricted to querying the service registry for service location information as described under the client-side discovery pattern.

⁵⁹ For purposes of this discussion, a pattern refers to repeatable processes to assist in the standardized design, monitoring, and maintenance of microservices.

⁶⁰ A health check or health testing is testing in an implementation immediately before or during normal operation to determine that the implementation continues to perform as implemented and as validated. Refer to [Law Insider’s Dictionary](#).

⁶¹ Refer to NIST SP 800-204, [Security Strategies for Microservices-Based Application Systems](#), for more information on distributed service registry, which involves several service registry agents cooperating to provide controlled access to resources. Distribution of the registry agents results in improved availability, higher concurrency, better response times to user queries, and enhanced flexibility.

Microservices are exposed to similar threats as web-based applications (e.g., cross-site scripting or injection attacks). Controls to prevent or mitigate these attacks should be included in the microservices code.⁶² Microservices can have security, reliability, and latency issues. Having multiple microservices can increase the entity's attack surface. Effective management evaluates implementation options that meet the entity's security requirements. Management of microservices-based architectures should include monitoring services, which may be running on different servers or written in different languages. Management should consider the following monitoring controls:

- Monitoring at the gateway and service level.
- Implementing a centralized dashboard to display the status of multiple services and network segments.
- Creating a baseline and implementing intrusion detection to provide alerts on deviations from the baseline.

To preserve resilience when developing and using microservices, NIST recommends the following control examples:⁶³

- Load balancing by having multiple instances of the same service and evenly distributing the load of those instances.
- Implementing circuit breaking by setting a threshold for failed responses from a microservice. When the threshold is exceeded (i.e., the circuit breaker is tripped), requests should not be forwarded to that microservice. The goal is to prevent cascading failures and allow time to investigate and address the issue.
- Throttling or limiting the rate of requests to a microservice.
- Redirecting requests to new versions of the microservice.⁶⁴
- Limiting traffic to new versions of a microservice until management can validate the correctness of a response and understand the performance.⁶⁵

For more information on the development and use of microservices, refer to the “[Development](#)” section of this booklet.

⁶² For more information on specific controls, refer to “[OWASP API Security Project](#).”

⁶³ Refer to NIST SP 800-204A, [Building Secure Microservices-Based Applications Using Service-Mesh Architecture](#).

⁶⁴ This is referred to as blue/green deployments. When a new version of a microservice is deployed, requests from customers using the old version can be redirected to the new version using the API gateway that can be programmed to maintain awareness of the locations of both versions. For more information, refer to NIST SP800-204A, [Building Secure Microservices-Based Applications Using Service-Mesh Architecture](#).

⁶⁵ This process is referred to as “canary releases,” in which only a limited amount of traffic is initially sent to a new version of a microservice because the correctness of its response or performance metric under all operating scenarios is not fully known. Once sufficient data are gathered about its operating characteristics, the requests can be proxied to the new version of the microservice. For more information, refer to NIST SP 800-204A, [Building Secure Microservices-Based Applications Using Service-Mesh Architecture](#).

IV.H Containers

A container is a method for packaging and securely running an application in a virtualized environment. Containers enable applications to be portable, reusable, and automatable in terms of their creation, use, and destruction. Containers provide software developers the ability to segment applications in separate environments to support well-defined functionality. This allows the entity to coordinate the development, testing, implementation, and operation of applications in a more consistent, precise, and efficient manner. Containers enable virtualized segmentation, which allows for increased security and transparency but may require additional configuration to support effective integration. In addition to the use of containers in the production environment, it is beneficial to leverage containers in the development and test environments, which helps to promote consistency.

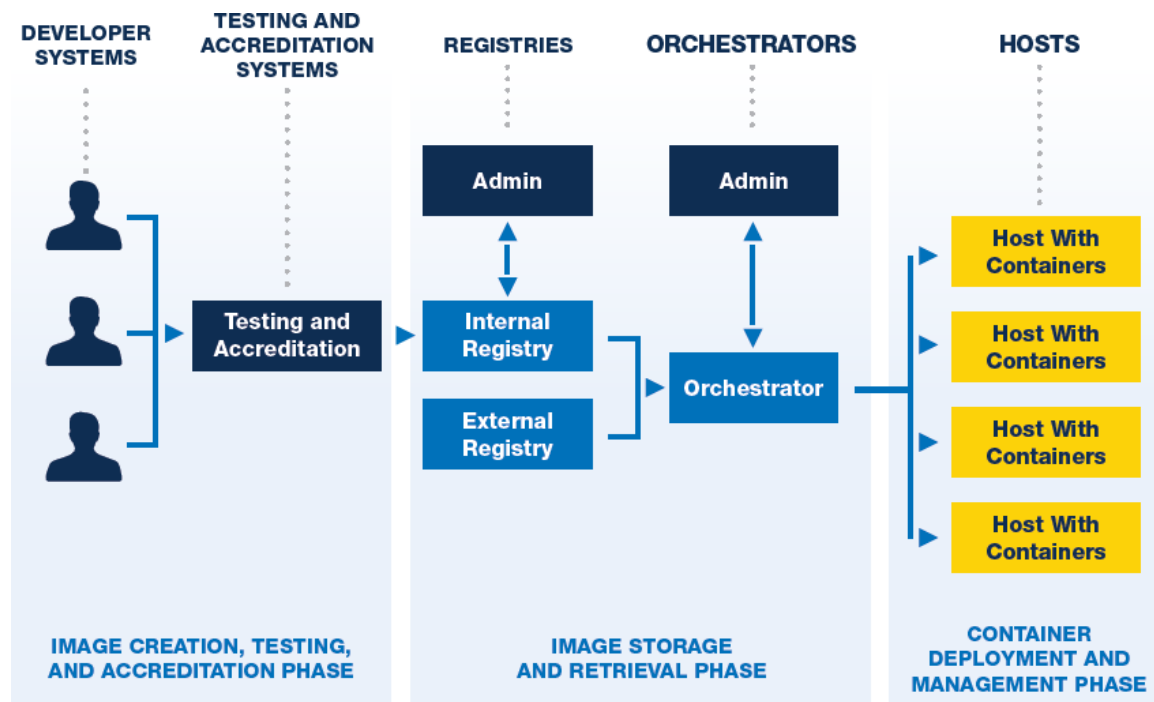
Figure 1 depicts the following five foundational architectural tiers and components and the three life cycle phases for container development and technology architecture.⁶⁶ The foundational architectural tiers and components are as follows:

- Developer systems, in the image creation, testing, and accreditation phase, generate container images and send them for testing and accreditation.
- Testing and accreditation systems, in the image creation, testing, and accreditation phase, validate and verify the contents of container images, sign container images, and send container images to the registry.
- Registries (internal and external), in the image storage and retrieval phase, store images and distribute container images to the orchestrator on request.
- Orchestrators facilitate the conversion of container images into containers during the image storage and retrieval phase and deploy containers to hosts in the container deployment and management phase.
- Hosts run and stop containers as directed by the orchestrator in the container deployment and management phase.

The three phases noted in figure 1 are (1) image creation, testing, and accreditation; (2) image storage and retrieval; and (3) container deployment and management for container development and technology architecture.

⁶⁶ For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

Figure 1: Container Technology Architecture Tiers and Components and Life Cycle Phases



When setting up containers, it is important to consider data isolation. Data may be stored separately from configuration information and software (i.e., as separate building blocks). When data and configuration information are stored separately from the containerized software, the software, data, or configuration information can be created, used, and destroyed without consequence to the other building blocks in the container. Management may use persistent storage⁶⁷ for ongoing access to containerized applications, data, and configuration information. The aspects of isolation and persistent storage allow for new versions of containers to be created and used efficiently, without losing previously used data. When a new version of the software or containerized image is executed or initialized, connections to the persistent storage need to be restored along with any authorization and access rights considerations.

Container images are typically designed to be portable across machines and environments so that an image created in a development lab can be easily moved to a test lab for evaluation, then copied into a production environment to run without needing to make any modifications.⁶⁸ This deployment process (i.e., copying the image into production) results in a version of the application that is running and available to respond to requests. According to NIST, “When an image is deployed into a container, the image itself is not changed, but instead a copy of it is

⁶⁷ Merriam-Webster defines “[persistent](#)” as “continuing without change in function or structure.” For purposes of this discussion regarding storage in containers, “persistent storage” refers to the long-term access to application information beyond the container’s lifetime.

⁶⁸ Refer to NIST SP 800-190, [Application Container Security Guide](#).

placed in the container and transitioned from being a dormant set of [application] code to a running instance of the [application].”⁶⁹

The use of containers is not without risks; therefore, during container development, management should consider the risks and countermeasures provided in NIST 800-190,⁷⁰ such as those in table 1.

Table 1: Container Risks and Countermeasures

Risks	Countermeasures
Image risks	
Image vulnerabilities ⁷¹	Consider containers and images when selecting or using vulnerability management tools.
Image configuration defects	Adopt tools and processes to validate and enforce compliance with secure configuration best practices, such as implementing privileged user controls and validation of image configuration settings. ⁷²
Embedded malware	Monitor images for embedded malware by monitoring for malware signature sets and detecting behavioral patterns and anomalies.
Clear text secrets ⁷³	Use orchestrators and APIs to manage security of access to and provision of secrets to specific containers that require them based on predefined settings.
Untrusted images	Maintain a set of trusted images and registries. Only use images from this set to run in the environment, thus mitigating the risk of untrusted or malicious components being deployed. Consider processes to ensure that images and registries are secure, trusted, and periodically validated and that the hosts they reside on are from these approved lists. ⁷⁴
Registry risks	
Insecure connections to registries	Configure development tools, orchestrators, and container runtimes to connect only to registries over encrypted channels. The goal is to ensure that all data pushed to and pulled from a registry occur between trusted end points and are encrypted in transit.
Stale images in registries	Reduce registries to minimize unsafe and vulnerable images that should no longer be used. Access images using unchanging names that specify discrete versions of images to be used to ensure that specific and uncorrupted images are deployed as part of each job. ⁷⁵

⁶⁹ [Ibid.](#)

⁷⁰ [Ibid.](#)

⁷¹ Container image vulnerabilities may not be detected by traditional vulnerability management tools.

⁷² For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁷³ Many apps require secrets to enable secure communication between components. The risk is that if someone steals the image, that person can learn the secrets, such as username and password, to connect to a backend database, connection strings, and private keys. Refer to NIST SP 800-190, [Application Container Security Guide](#).

⁷⁴ For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁷⁵ Another option is using a “latest” tag for images and referencing this tag in deployment automation, but this may not always be effective. Regardless of whether an organization chooses to use discrete names or to use a “latest” tag, it is critical that processes exist to ensure that the most recent unique name or the images tagged “latest” represent

Risks	Countermeasures
Insufficient authentication and authorization restrictions	Any access to registries that contain proprietary or sensitive images should involve authentication. Gaining write-access privileges to a registry should entail appropriate authentication to ensure that only images from trusted entities can be added to the registry. Audit all write-access privileges to registries and log any read actions for sensitive images. ⁷⁶
Orchestrator Risks	
Access considerations, such as unbounded administrator access ⁷⁷	Orchestrators should use a least-privilege access model in which users are only granted the ability to perform the specific actions on the specific hosts, containers, and images that their job roles require. Test team members should have limited or no access to containers used in production. ⁷⁸
Unauthorized access	Tightly control access to cluster-wide administrative accounts, as these accounts provide the ability to affect all resources in the environment. Use appropriate authentication methods (e.g., MFA and single sign-on when applicable). Use tools for encrypting data used with containers that allow the data to be accessed properly from containers regardless of the node on which they are running. ⁷⁹
Orchestrator node trust ⁸⁰	Configure orchestration platforms to provide features that create a secure environment for all the applications they run. Maintaining a secure-by-default posture is particularly important with third-party deployments of the entity's containers. Orchestrators should be able to perform the following: introduce nodes securely to the cluster, ⁸¹ maintain a persistent identity for the nodes throughout their life cycle, and maintain an accurate inventory of nodes and their connectivity states. Orchestration platforms should be resilient (i.e., a compromise of one node should not compromise the overall security of the cluster). ⁸²
Poorly separated inter-container network traffic ⁸³	Configure orchestrators to separate network traffic into discrete (e.g., internal versus external applications) virtual networks by sensitivity level, and

the most up-to-date versions. For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁷⁶ For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁷⁷ A single orchestrator having administrator access. Access should be limited according to need. For example, applications may be managed by different teams with differing sensitivity levels. As many orchestrators were designed with the assumption that user interaction would be with administrators, there is the potential for unauthorized access; therefore, authorization and access concerns are relevant. Refer to NIST SP 800-190, [Application Container Security Guide](#).

⁷⁸ For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁷⁹ For more information, refer to NIST SP 800-190, [Application Container Security Guide](#), and the FFIEC IT Handbook's "[Information Security](#)" booklet.

⁸⁰ The orchestrator is the most foundational node. Weak orchestrator configurations can expose the orchestrator and other container technology components to increased risk. Refer to SP NIST 800-190, [Application Container Security Guide](#).

⁸¹ An example of a cluster is a set of nodes that run containerized.

⁸² A compromised node should have the ability to be isolated and removed from the cluster without disrupting or degrading overall cluster operations. For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁸³ If a virtual overlay network is used to manage container traffic, security and management tools may not have clear visibility into the traffic. If traffic has varying sensitivity levels on the same network, more sensitive data may be susceptible to attack due to expanded access to the network users with lesser privileges. For example, if the public-

Risks	Countermeasures
	communication between the two should occur through a small number of well-defined interfaces. ⁸⁴
Mixing of workload sensitivity levels on the same host ⁸⁵	Configure orchestrators to isolate deployments to specific sets of hosts by sensitivity levels. Implement rules that prevent high-sensitivity workloads from being placed on the same host as those running lower-sensitivity workloads. Segmenting containers by purpose, sensitivity, and threat posture provides additional defense-in-depth. ⁸⁶
Container Risks	
General container runtime-related risks ⁸⁷	Use tools or processes that continuously assess configuration settings across the environment and actively enforce them. Use segmentation to provide control and isolation over containers to minimize unauthorized access and loss of data. Run containers with the default secure computing profiles ⁸⁸ provided by their runtime. Consider using additional profiles for higher risk applications. Use tools to identify vulnerabilities in the container runtimes deployed to upgrade any instances at risk and to ensure that orchestrators only allow deployments to properly maintained container runtimes.
Unbounded network access from containers ⁸⁹	Employ a combination of network monitoring and filtering tools (e.g., application-aware tools) ⁹⁰ to mitigate the risk from inter-container traffic across networks of differing sensitivity levels.

facing website is compromised, attackers may be able to use shared networks to attack an internal app using sensitive information. Refer to NIST SP 800-190, [Application Container Security Guide](#).

⁸⁴ For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁸⁵ An orchestrator may place a container running a public-facing web server on the same host as one processing sensitive data, because that host happens to have available resources at the time of deployment, as the orchestrator manages scale and density of traffic. In the case of a critical vulnerability in the web server, a container processing sensitive data may be at greater risk of compromise due to the greater access to the host of the container. Refer to NIST SP 800-190, [Application Container Security Guide](#).

⁸⁶ Concepts such as application tiering and network and host segmentation should be taken into consideration when planning app deployments. By segmenting containers in this manner, it is much more difficult for an attacker who compromises one of the segments to expand that compromise to other segments. In larger-scale environments with hundreds of hosts and thousands of containers, this segmentation is automated to be practical. Common orchestration tools can help management in the segmentation process. For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁸⁷ Container runtimes include such risks as (1) insecure container runtime configurations and (2) capability for containers running in privileged mode to access host configurations, potentially compromising the host and all other containers on it.

⁸⁸ Secure computing profiles can be used to limit the system-level capabilities allocated to containers at runtime. For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁸⁹ By default, in most container runtimes, individual containers can access each other and the host OS over the network. If a container is compromised and acting maliciously, allowing this network traffic may expose other resources in the environment to risk. Tools and operational processes that are not container-aware are not able to inspect this traffic or determine whether it represents a threat. Refer to NIST SP 800-190, [Application Container Security Guide](#).

⁹⁰ Application-aware tools provide the ability of a system to recognize and classify applications passing through it. These tools allow systems to make decisions based on an application, its features, and the content it's carrying. These tools should be able to not just see the inter-container traffic but also dynamically generate the rules used to

Risks	Countermeasures
Rogue containers ⁹¹	Maintain separate environments for development, test, and production with specific controls (e.g., role-based access control) for container deployment to mitigate the potential for rogue containers. There should be a clear audit trail process during container development to give management information that associates any container build or modification to specific users.
Application vulnerabilities, such as risks inherent in the general use of applications	Implement additional container-aware tools ⁹² using behavioral learning (i.e., heuristics) and appropriate security profiles to detect anomalies and events, such as writing to unexpected locations and file types, sending traffic to unexpected network destinations, and storing or executing malware. Additionally, containers should be run with their root file systems in read-only mode to monitor for compromise, to isolate tampering to these specific locations, and separate them from the rest of the application.
Host OS Risks	
Large attack surface ⁹³	Minimize unnecessary functionality by using OSs designed to host only containers and have other services and functionality disabled to reduce the attack surface. Additionally, host OSs should have read-only file systems and have hardening practices implemented by default. Regularly scan and update the container runtime and lower-level components (e.g., kernel) in a timely manner.
Shared kernel ⁹⁴	Use separate, dedicated hosts for containerized and noncontainerized workloads. Isolating the workloads enables the application of appropriate safeguards to containers and avoids affecting noncontainerized workloads.
Improper user access rights, such as allowing users to log on directly ⁹⁵ to hosts to manage containers	Employ least privilege access. Audit all authentication to the OS, monitor all login anomalies, and log any privileged user activities to identify anomalous (and potentially unauthorized) access patterns.

filter this traffic based on the specific characteristics of the apps running in the containers. For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁹¹ Rogue containers are unplanned or unsanctioned containers in an environment. They may be used in development builds or test images and may pose additional risk to the organization, especially when they persist in the environment without the awareness of development teams and security administrators. Refer to NIST SP 800-190, [Application Container Security Guide](#).

⁹² Container-aware tools provide the ability to monitor the container environment and provide precise detection of anomalous and malicious activity within it. For more information, refer to NIST SP 800-190, [Application Container Security Guide](#).

⁹³ The larger the attack surface is, the better the odds are that an attacker can find and access a vulnerability, leading to a compromise of the host OS and the containers running on top of it. Refer to NIST SP 800-190, [Application Container Security Guide](#).

⁹⁴ The use of a shared kernel results in a larger attack surface as the level of isolation provided by container runtimes is not as high as that provided by hypervisors. Runtime container security means vetting all activities in the container application environment, from analysis of container and host activity to monitoring the protocols and payloads of network connections. Refer to NIST SP 800-190, [Application Container Security Guide](#).

⁹⁵ When users log on directly to the host with elevated privileges to manage specific containers, there is the possibility of accessing and affecting other containers on that host. Refer to NIST SP 800-190, [Application Container Security Guide](#).

Risks	Countermeasures
Host OS component vulnerabilities ⁹⁶	Use appropriate tools provided either by the OS vendor or other trusted organizations to regularly check for and apply updates to all software components used in the OS to mitigate potential vulnerabilities. This is particularly important for the kernel and container runtime components as newer releases of these components often add additional security protections and capabilities beyond simply correcting vulnerabilities. Deploy application components and their dependencies ⁹⁷ in a container to identify or prevent anomalies and configuration changes, promote resilience, and allow management to reduce its attack surface, prevent persistent storage of data on the host, promote statelessness ⁹⁸ on the host, and reduce application-level host dependencies.
Host OS file system tampering ⁹⁹	Run containers with the minimal set of file system permissions required. NIST recommends that containers should not be able to make sensitive directories available on a host's file system, especially those directories containing configuration settings for the OS. Monitor what directories are placed, made available, and accessed on the file system.

IV.I Application Programming Interfaces

An API is software code that allows two or more different programs to communicate with each other. APIs are an important part of various applications, including web, mobile, and software-as-a-service (SaaS) applications. APIs often link microservices and may be public, private, or a collaboration between customers, partners, and unaffiliated third parties to share information and allow their software to function together. Another function of APIs is to facilitate communication between containers. For more information on APIs and how they fit with other elements of an entity's IT environment, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" booklet.

When developing, acquiring, and maintaining APIs and related services, there are several considerations.¹⁰⁰ Examples include the following:

- Aligning the API with business processes, particularly when designing a microservice.
- Iterating the interface definition with developers before the service is used so that the resulting API serves as a contract between clients and services.

⁹⁶ All host OSs, even container-specific ones, provide foundational system elements, such as access and authentication. As a foundational element in container technology, host OS vulnerabilities can affect everything running on the host, including containers and apps. Refer to NIST SP 800-190, [Application Container Security Guide](#).

⁹⁷ In IT infrastructure, dependencies are relationships of reliance in and among infrastructure assets and systems that must be maintained for those systems to operate and provide services. For more information, refer to CISA's "[Infrastructure Dependency Primer](#)."

⁹⁸ According to NIST Glossary, statelessness or quality of being "[stateless](#)" refers to "a data representation or a process that is self-contained and does not depend on any external data store."

⁹⁹ A change to a sensitive system file on the host OS could affect the stability and security of the host and all other containers running on it. Refer to NIST SP 800-190, [Application Container Security Guide](#).

¹⁰⁰ For more information on developing, acquiring, and maintaining APIs, refer to NIST SP 800-204, [Security Strategies for Microservices-Based Application Systems](#).

- Determining and implementing appropriate security related to APIs.¹⁰¹

Risks related to APIs include the following:

- Inappropriate access controls.
- Inadequate user authentication.
- Excessive data exposure.
- Lack of resources for processing access requests, including rate limiting problems.
- Allowing modification of object properties.¹⁰²
- Misconfigured security.
- Injection flaws.
- Lack of appropriate ITAM and documentation leading to maintenance weaknesses and exposed end points.
- Lack of appropriate logging and monitoring.
- Lack of integration with the entity's incident response program.

IV.I.1 API Gateway

Understanding how APIs can act as a gateway to microservices is important. Unlike a legacy application where the endpoint may be only a single server, a microservices-based application consists of multiple endpoints. Therefore, a single-entry point (i.e., gateway) for all clients to access multiple component microservices of the application would allow for improved access. Another situation in which an API gateway may be deployed is as a front-end-to-backend¹⁰³ connector, as in the case of legacy enterprise software. This occurs when an entity migrates from a legacy enterprise application by gradually replacing its components with independent microservices over time. Direct communication between clients and multiple end points often results in excessive point-to-point connections; therefore, the API gateway's primary function is to route inbound requests to the correct downstream services to minimize the number of connections. All client requests first go through the API gateway, which then routes requests to the appropriate microservice. The API gateway often handles a request by invoking multiple microservices and aggregating the results. In some instances, the API gateway may be used as part of a back end for front-end services, which enables support for clients with different communication vectors (e.g., browser or mobile device), and then requests are divided into multiple gateways. Many API gateway use cases can support APIs written in different languages.¹⁰⁴

¹⁰¹ For more information on API security, refer to the *FFIEC IT Handbook's* "[Information Security](#)" and "[Architecture, Infrastructure, and Operations](#)" booklets. "[OWASP API Security Project](#)" also discusses API security issues and controls.

¹⁰² Object properties provide a simple association between name and value. All properties have a name, and value is one of the attributes linked with the property, which defines the access granted to the property.

¹⁰³ The front end of a system involves the parts that users see and interact with, whereas the system's back end includes the logic, data, and structure.

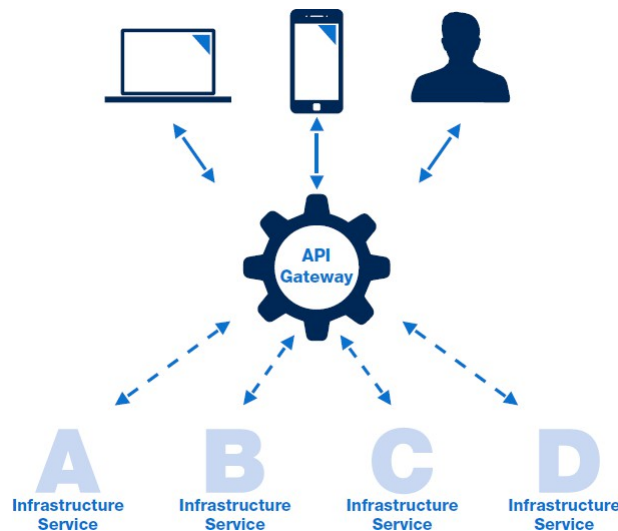
¹⁰⁴ Examples of different languages include Java, JavaScript, and Jolie.

Because the API gateway is the entry point for microservices, management should configure it with the necessary infrastructure services.¹⁰⁵ In addition to its main service of handling requests, an API gateway also helps with the following infrastructure services:

- Service discovery.
- Authentication and access control.
- Load balancing.
- Caching.
- Providing custom APIs for each type of client.
- Performing application-aware health checks.
- Service monitoring.
- Attack detection.
- Attack response.
- Security logging and monitoring.
- Circuit breaking.

These additional infrastructure services can be created or implemented in the code that uses the API gateway. Figure 2 provides a simple illustration of the API gateway location during a request. It shows that the API gateway routes requests from various sources (e.g., laptops, mobile devices, and users) to the various infrastructure services.

Figure 2: Location and Interaction of API Gateway



Microgateways are API gateways used to define and enforce customized policies for microservices-based applications. If used, they should be protected through service-specific security policies. Microgateways are usually implemented as containers and should contain policies for application requests and responses. When policies and their enforcement are implemented as a container, they are unchanging; therefore, they provide a degree of protection

¹⁰⁵ Refer to NIST SP 800-204, [Security Strategies for Microservices-Based Application Systems](#).

against accidental and unintended modifications. Modifications could result in security breaches or conflicts. In other words, microgateways implemented as containers may help prevent breaches and conflicts because any security policy updates require the microgateway's redeployment. It is essential that the microgateway deployed for a microservice instance communicate with service registry and monitoring modules, allowing them to keep track of the operational status of the microservice that the microgateway is designed to protect.

When used with microservices, an API gateway or microgateway may serve to implement the following core features and functions:

- **Optimized end point:** The API gateway simplifies the process by providing aggregation, which results in fewer requests and responses. The API gateway can serve as a public interface for multiple individual APIs and their requests. Additionally, it performs the necessary protocol translation for client requests.
- **Circuit breaker:** Developers can set a threshold in the API gateway for microservice failed responses to requests and cut off requests when the failure is above the threshold. This avoids the possibility of a cascaded failure and allows management time to analyze logs, implement necessary fixes, and push necessary updates to address the failing instance of the microservice.
- **Load balancing:** When there are multiple instances of the same service, the load can be evenly distributed across the instances to avoid delayed responses or service crashes due to overload on any one instance.
- **Rate limiting (throttling):** The rate of requests going into a microservice should be limited to ensure continued availability of service for all clients.
- **Blue/green deployments:**¹⁰⁶ When a new version of a microservice is deployed, requests from customers using the old version can be redirected to the new version because the API gateway can be programmed to be aware of the locations of both versions.
- **Canary releases:** Only a limited amount of traffic is initially sent to a new version of a microservice to verify the accuracy of its response and performance. Once sufficient data demonstrate that the microservice is operating as designed, then the API gateway can direct the requests to the new version of the microservice.

IV.I.2 API Risk Mitigation

Mitigation strategies for common API risks include the following:¹⁰⁷

- **Inappropriate access controls:** API endpoints are vulnerable to unauthorized access as attackers can manipulate the specific object ID or other identifier that is sent with the request. Management should apply extra layers of security, such as for broken object-level

¹⁰⁶ This type of deployment provides an application release model when user traffic is progressively transferred from a prior version (i.e., old or blue) of an app or microservice to a nearly identical new (i.e., green) release. Both the blue and green versions are running in production at the same time.

¹⁰⁷ For more information, refer to "[OWASP API Security Project](#)."

authorization,¹⁰⁸ beyond those for standard end-point security, and implement appropriate authorization checks at the object level.

- **Inadequate user authentication:** Authentication processes are not functioning correctly or are inappropriate for the way the API is used (e.g., designed for internet of things [IoT] versus a web application) or without considering potential vectors of attack. Management should validate the user authentication process for the use of the API and consider MFA.¹⁰⁹
- **Security misconfiguration:** Security settings may be missing or inappropriate for the current expected functionality of the API, giving an attacker the opportunity to gain unauthorized access or knowledge of the system. Attackers may use automated tools to detect and exploit these flaws, leading to data or device compromise. Management should implement appropriate security, patch and update APIs, and disable unnecessary functions.
- **Excessive data exposure:** Developers try to implement APIs generically without addressing the sensitivity of the exposed data. Automated tools can have difficulty detecting this type of vulnerability because they cannot differentiate between legitimate data provided from the API and inappropriately provided sensitive data. This problem creates the potential for unauthorized data access. Developers should review the responses from the API to ensure that a request contains only legitimate data and to understand how the requestor will use the data. Developers should consider creating and implementing a scenario-based response process (including error codes) to validate that data returned by the APIs are appropriate for the scenario.
- **Lack of resources and data limiting:** API requests consume resources such as network, central processing unit (CPU), memory, and storage. When APIs do not implement rate limiting or limits are not set properly, it may lead to an API being unresponsive or unavailable (i.e., denial of service). Management should appropriately set all API processing parameters (e.g., execution timeouts, maximum allocatable memory, number of file descriptors, number of processes, request size, number of requests per client or resource, and number of records per page to return in a single request response). If even one of the limits is missing or set inappropriately, an API may be vulnerable.
- **Broken function level authorization:** Implementing proper authorization checks can be difficult because applications can contain many types of roles or groups and complex user hierarchy (e.g., subusers and users with more than one role). Because these checks are difficult to implement, what appears to be a legitimate API call or request may not be authorized, allowing unauthorized access to functionality, particularly administrative functions. Management should ensure that all access is denied by default and employ specific role-based permissions for users to gain access to functions. Appropriate personnel should review API end point security.
- **Mass assignment:**¹¹⁰ Users can update multiple object properties without appropriate authorization. The design of APIs provides for easier exploitation of mass assignment because they expose the underlying implementation of the application along with the

¹⁰⁸ Object-level authorization involves access-control tools applied at the code level to validate appropriate access to objects (e.g., fields such as names or values) by only authorized users.

¹⁰⁹ For more information, refer to FFIEC's [Authentication and Access to Financial Institution Services and Systems](#) on multifactor authentication.

¹¹⁰ The MITRE Corporation defines "[mass assignment](#)" as "a feature that allows simultaneous modification of multiple object attributes."

properties' names. Management should deny access to properties unnecessary for the user's role and only allow access when necessary.

- **Injection:** Client and external system data may not be validated and filtered appropriately, allowing malicious data to be introduced into systems and components via the API. Injection can lead to information disclosure, data loss, denial of service, or complete host takeover. Management should validate and filter all data coming to an API with appropriate parameters.
- **Improper asset management:** Management may not properly maintain API and related asset inventories or may not update and patch API security in a timely manner. This may either allow unauthorized access to sensitive data or compromise the server through older, unpatched API versions connected to the same database. Management should maintain current, accurate inventories of APIs and related assets, including services,¹¹¹ and regularly review them. Management should maintain logging of API activity (e.g., authentication, errors, redirects, rate limiting, and end points, including their parameters, requests, and responses). Management should consider security measures, such as API security firewalls, segregation of production and nonproduction data, and timely removal of older API versions.
- **Insufficient logging and monitoring:** Without sufficient, timely logging and monitoring, including API activity, it is difficult to identify patterns of potential malicious activity (e.g., threats and potential security weaknesses), which may lead to compromise of systems, components, and data. Management should perform continuous logging and monitoring of relevant API activity (e.g., failed authentication attempts, denied access, and input validation errors). Automated security information and event management tools with appropriately configured dashboards may help management monitor and manage API-related logging. To maintain confidentiality and integrity of sensitive data in activity logs, effective management secures logs and ensures only appropriate access to them.

With the volume and potential significance of API-related vulnerabilities, it is critical to incorporate planning for the exploitation of these vulnerabilities during API development and the entity's incident response plan. Neglecting to do so can result in the compromise of confidentiality, integrity, availability, and resilience as well as inadequate or untimely response during an incident. For more information on security and other topics related to APIs, refer to the *FFIEC IT Handbook's* "[Information Security](#)" and "[Architecture, Infrastructure, and Operations](#)" booklets.

IV.J Methodologies

A methodology¹¹² is used to facilitate the development, acquisition, or maintenance of a system or component project. Management should establish appropriate methodologies to enable effective management and control of system and component development, acquisition, and maintenance activities. Management can apply various methodologies, or a hybrid, to different projects based on stakeholder needs and project objectives. Methodologies can be a combination of strategies, design philosophies, and accepted practices designed as a structured, organized set

¹¹¹ For more information, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" booklet.

¹¹² *Merriam-Webster* defines "[methodology](#)" as "a particular procedure or set of procedures."

of rules that allow a project team to work together effectively. If the entity employs multiple methodologies, the chosen methodology should be defined for each IT project.

Effective management aligns implementation of any methodology with the overall strategic and business objectives. Planning, education, and communication are important elements to help ensure that critical resources are available when needed for IT projects. Management should promote effective planning through IT project management and support training for developers, quality management members, testers, and maintenance personnel. Entity staff should be proficient and qualified in the selected methodologies. Common examples used in the financial industry include waterfall and agile; however, examiners may encounter others.

IV.J.1 Waterfall

The waterfall methodology was the first widely used model. It is considered a traditional model for development, acquisition, and maintenance projects. This methodology provides a logical, rigid approach to managing a sequential series of tasks or steps in which each phase is completed before the next phase of the project can begin. This methodology may be useful for stable, less complex projects with well-defined objectives and requirements that are not prone to change. A primary benefit of this methodology is its ease of use and implementation. Additionally, because of the sequential progression of the project, coding issues are identified earlier, and project status is more easily measured than in other methodologies. However, it may be difficult or cost-prohibitive to return to a previous project phase to make corrections or changes in requirements requested by stakeholders. Other drawbacks include excessive time to produce a product, stakeholder difficulty in defining the desired end product, and difficulty making changes once started.

The waterfall methodology is a multiphase approach that begins with a requirements phase when stakeholders define the project requirements and most of the communication between stakeholders occurs. Once the first phase is completed, a product or service can then be designed, developed, tested, and implemented. This methodology allows only minimal stakeholder changes or iterations, and a final product is not provided until the implementation. Moreover, this methodology progresses through other phases until the final phase, which is the maintenance phase, during which any issues are corrected.

IV.J.2 Agile

An alternative to traditional project management methods (also known as predictive or waterfall management) is the use of adaptive or agile management methods. Incremental and iterative development principles form the foundation of agile methodologies.¹¹³ Such principles involve breaking down a project into smaller, manageable modules that can be designed, developed, vetted, and installed in repeated cycles allowing for additional features, adjustments, and corrections with each iteration. With incremental and iterative development, management does

¹¹³ The agile development methodologies represent a family of development types rather than a single methodology. Organizations exploring agile methodologies are working to define core values and guiding principles for enabling high-performing teams in implementing and executing with agility. These methodologies emphasize close communication and collaboration between the project team and stakeholders.

not need to identify all requirements at the beginning of the project, as changes may be added during later iterations. Agile projects are different from waterfall projects because they rely on (1) defining requirements before and during execution; (2) delivering frequent, iterative, and incremental products (i.e., not always fully completed); and (3) welcoming changes at any point in the process.¹¹⁴ Incremental and iterative development may be used for larger projects in which the final product's requirements are well-defined, but details may change or need enhancement during the process.

There are different models of incremental and iterative development (e.g., iterative, spiral,¹¹⁵ and prototyping modeling¹¹⁶), but they follow the main principle of a defined repetitive process. An agile methodology is an incremental and iterative development methodology that relies heavily on stakeholder interaction throughout the development process. During each phase, a deliverable is produced for the stakeholders, who provide feedback. The benefits of an agile methodology include earlier availability of a version of the deliverable and improved stakeholder satisfaction due to the regular feedback. A primary drawback of an agile methodology is the additional resource requirements (e.g., time, personnel, and funding) needed to implement the additional iterations.

Generally, an agile methodology involves dividing a project into smaller modules or “sprints.” Each sprint represents an independent project, with phases (e.g., planning, requirements, design, coding, testing, and documentation) similar to those of other development methodologies. In some cases, sprints may become part of a larger project. The project is evaluated at the end of each sprint, and adjustments are implemented as appropriate. An agile methodology is designed to anticipate change at regular intervals based on feedback from stakeholders, such as customers and business analysts, and derive business value from the feedback.

When applied effectively, the overall business goal of an agile methodology is to minimize risk of introducing defects, prevent cost overruns, and quickly resolve changes in scope before there is a significant impact to the project. An agile methodology aims to satisfy stakeholder requirements by providing rapid, continuous deliveries of useful systems and components, delivered in short intervals. It aims to release working elements of the systems and components at the end of each iteration, even if the overall product is incomplete. The feedback is used to make changes to the existing deliverable and the overall project plan.

Cross-functional teams representing various business lines are created to facilitate development. The diverse representation of these teams promotes consideration of multiple perspectives, improving visibility during the development process. The result of each iteration should be a

¹¹⁴ NIST Advanced Manufacturing Series 100-40, [Agile for Model-Based-Standards Development](#).

¹¹⁵ In the spiral model, the project iteratively goes through specific development phases (e.g., identify, design, build, and evaluate) with refinement in each iteration (or spiral) until development is complete. For more information, refer to National Aeronautics and Space Administration, [A Software Development Simulation Model of a Spiral Process](#).

¹¹⁶ Prototyping modeling involves developing a product with the look, feel, and limited functionality of the product under development. It can be used in conjunction with other models allowing developers to build prototypes during development. The prototype is built, tested, and adjusted until a working model is developed and can be produced as a final product or deployed throughout a system.

functional deliverable for the customer. Real-time feedback¹¹⁷ from customers or stakeholders is a key aspect of an agile methodology.

An agile methodology employs a flatter organizational structure to allow iterative delivery of systems or components. A common role supporting an agile methodology is the scrum master,¹¹⁸ which is similar to the traditional project manager role. However, unlike the project manager, a scrum master supports and serves the product owner and the development team by helping to remove obstacles to project deliverables.

An agile methodology may create unique challenges in documentation of development; therefore, the entity's documentation requirements should be clearly defined in the entity's project management requirements. Effective documentation relies on real-time communication between the development team and stakeholders, including end users. In any methodology, a lack of clarity or poor communication can negatively affect project deliverables and timelines (e.g., delays, scope creep, costs, and quality). This may have increased significance in an agile methodology because multiple parts of the overall project in process may be affected, leading to a greater impact than if only one segment of a project in process is affected.

Individual agile methodologies¹¹⁹ may differ in their specific processes; however, they are based on some common principles.¹²⁰ However, agile principles could be at odds with security principles. For example, the agile principle of speed to delivery could cause developers to leave out important security controls that would take longer to include but be invisible to the end user. To mitigate the risk of security flaws in an agile project, leaders can establish security standards that must be met before a solution is deployed for production use.

In prototyping models of systems and components (e.g., rapid application development), developers could bypass established change controls, leading to security and integrity risks. Following established control procedures when using these models is as important as when using any other development methodology type.

¹¹⁷ Feedback loops from customers and stakeholders may take several forms (e.g., emails, meetings) for communicating expectations and needed changes.

¹¹⁸ NIST defines a "[scrum master](#)" as "the role performing the management of the iteration and increments." A scrum is an agile project management approach that helps teams structure and manage their work through a set of values, principles, and practices toward a common goal.

¹¹⁹ Examples of agile methodologies include Extreme Programming, Scrum, Lean Software Development, Crystal Methodologies, Adaptive Software Development, Feature Driven Development, and Dynamic Systems Development Methodology.

¹²⁰ Common principles include short development iterations, minimal design upfront, emergent design and architecture, collective code ownership and ability for anyone to change any part of the code, direct communication and minimal or no documentation (i.e., the code is the documentation), and gradual building of test cases. Refer to Noopur Davis, [Secure Software Development Life Cycle Processes: A Technology Scouting Report](#), and related guidance, such as CISA, [Securing the Software Supply Chain: Recommended Practices Guide for Developers](#), and [Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default](#).

IV.K Quality Management

Quality management refers to coordinated activities to direct and control an organization regarding quality. It helps management assess whether newly developed, procured, or modified systems and components are operating as envisioned, and are designed and comply with an entity's policies, standards, and procedures. Entities assess quality through manual, automated, or hybrid methods throughout the SDLC. Quality management should be an independent function from development, and prudent practices typically include implementing compensating controls when segregation of duties cannot be fully achieved. For example, developers should not test and validate systems and components that they developed.

Quality management comprises the functions of QA and quality control (QC), which together focus on providing confidence that quality requirements will be fulfilled. Although the goal is similar, QA and QC differ somewhat. QA refers to a planned, systematic pattern of all actions necessary to provide adequate confidence that a system, component, or facility conforms to established requirements. QC refers to the operational techniques and procedures (such as design analysis and inspection for defects) used to achieve quality requirements. QA and QC may be implemented separately or together, depending on the size and complexity of the entity and its development, acquisition, and maintenance activities.

Quality management is a critical part of well-managed development, acquisition, and maintenance activities. Comprehensive quality management, risk management, and testing standards provide a means to manage project risks and promote expected functionality, security, and interoperability in systems and components in a secure, resilient manner. Quality management policies, standards, and procedures should be applied to internally and externally developed programs and should address the following:

- **Commitment:** Successful projects generally include commitment from all involved parties. Senior management should adequately support and promote projects throughout an entity to promote success of a project. Failure by management to implement or support quality management programs hinders its ability to quickly detect project weaknesses and programming errors. Correcting weaknesses and errors detected late in a project life cycle is often more difficult and costly and may be less effective.
- **Expectations:** To improve quality management and minimize deficiencies, stakeholders should clearly define their expectations and effectively communicate their requirements initially and throughout a project. For example, expectations and requirements could include reliability, resilience, performance, simplicity, usability, interpretation of error messages, accessibility, interoperability, and robustness.
- **Completeness:** Each phase of a project life cycle should include procedures to follow and expected deliverables. Quality management personnel should verify the business case for a project, required functional features, and appropriateness of project considerations to determine completeness in each project phase before moving to the next phase. Audit and compliance personnel should verify that quality management includes quality standards to validate that the project meets internal and external requirements.
- **Scalability:** Projects vary in size and complexity. Quality management standards should match project characteristics and risks and may differ by project size and type. Quality

reviews may consider whether the entity's systems and components can scale, as necessary.

- **Measurability:** To accurately evaluate a project's success, management should assess results against defined expectations and requirements to determine project success. Quality management personnel should assess the quality of products and processes against measurable standards, metrics, and expectations.
- **Tracking:** Quality management personnel should validate that project personnel properly document a project's progress; record, report, and monitor problems to resolution; and communicate progress and concerns to management.
- **Independence:** Quality management personnel should be independent of the project they are reviewing to objectively assess elements, such as progress, problem resolution, documentation, and adequacy of the project.
- **Security:** Information security personnel perform a critical function in ensuring the confidentiality, integrity, availability, and resilience of internally developed and procured systems.¹²¹ Quality management personnel should validate the existence and effectiveness of information security considerations. The extent of security validation should be commensurate with risks associated with the project.
- **Legal and regulatory:** Legal and compliance personnel provide guidance throughout a project to ensure that it conforms with applicable statutory and regulatory requirements to mitigate project risks. Quality management personnel should assess statutory and regulatory requirements for deliverables (e.g., digital accessibility)¹²² and determine whether the systems and components can meet those requirements.

IV.L Documentation Standards

Thorough documentation allows stakeholders to clearly understand system and component functionality, security, control features, and resilience. Documentation conveys how a system or component was developed, how it functions, and where appropriate security and resilience points are included. Entity personnel can refer to documentation to effectively operate and maintain the systems and components. Additionally, well-prepared and maintained documentation reduces resilience risks, such as the loss of institutional knowledge common with personnel turnover. Documentation helps transfer key information (e.g., narratives, flowcharts, and any special system coding or file layouts) over time and across groups. Management should maintain documentation for both internally developed systems and components and externally procured products and services. Due to the sensitive nature of system and component documentation (e.g., internet protocol addresses, server names, and security controls), management should restrict access to sensitive documentation based on job description and need.

Examples of items that documentation may contain include feature and function descriptions, design specifications, programming descriptions, build procedures, and operating instructions. Also, documentation should be updated as systems and components are updated to ensure that the benefits described above continue.

¹²¹ For more information, refer to NIST SP 800-53, rev. 5, [Security and Privacy Controls for Information Systems and Organizations](#).

¹²² For more information, refer to [Section 508 of the Rehabilitation Act of 1973](#).

For acquired systems and components, management should obtain documentation from the third party and incorporate it into the entity's own stored documentation. Before purchase, effective management ensures (through an internal review or a third-party certification) that a procured system's documentation meets the entity's documentation needs and standards.

System documentation that includes current build and configuration instructions allows administrators to recover the system after a disruptive event. For a recovery process to be effective, these build and configuration instructions should be kept current as the system is maintained and changed. There are many build and configuration processes that are automated, and the scripts that automate those processes should be documented appropriately for future reference. However, in those cases it may be the manual action (unautomated) documentation that is at the highest risk of becoming stale.

Common documentation examples include the following:

- **System or component descriptions and topologies** that provide functional purposes, narrative explanations, and pictorial depictions of operating environments and the interrelated input, processing, and output functions of integrated systems and components.
- **System and program flowcharts and models** that identify the source and type of input information, processing, and control actions (automated and manual), and the nature and location of output information for a system or component. Additionally, program flowcharts present graphical views of the procedural program sequencing and provide a practical way to illustrate complex programs and routines. Administrators can use these flowcharts to view a system holistically or drill down to specific functions or interrelated components of a system or program.
- **System file and information layouts** provide specification useful in information collection, storage, and display.
- **Program documentation** details specific data input, processing, and output instructions, and should include documentation about system security. Examples of program documentation include program listings, source code, narrative comments, technical programming scripts,¹²³ and nontechnical descriptions of the scripts.
- **Manuals and procedures** inform IT personnel and end users on the operation of systems and components.

IV.M Post-Implementation Review

Organizations formally perform a post-implementation review (PIR) for system development and implementation projects to continuously improve. Processes and techniques that were effective are passed to future projects as effective practices. Problems and their solutions are also passed along to help future projects avoid pitfalls. In agile projects when there are multiple implementations, smaller reviews are completed after each task or deliverable is implemented. Typical PIR steps are

¹²³ Merriam-Webster defines a "[script](#)" in computing as "a sequence of instructions or commands for a computer to execute."

- Gathering data including project initiation documents, post-implementation metrics, and post-implementation stakeholder interview results.
- Analyzing any gaps between project initiation goals and objectives and actual outcomes, including the reasons for any gaps.
- Summarizing the analysis and any recommendations in a report to management.¹²⁴

Common project aspects analyzed in a PIR include the following:

- User satisfaction.
- Actual benefits compared to projected benefits.
- System or component defect level when implemented, which helps measure system testing effectiveness.
- Project management effectiveness.
- Actual costs and timeline versus business case projections.

When entities analyze project aspects like those above and pass the results to management and future project teams, they raise future project success probability and mitigate the risk of future project failure.

IV.N IT Project Management

Action Summary

Consistent use of appropriate project management policies, standards, and procedures can help personnel be effective in identifying and mitigating project risks before they materialize.

Examiners should review the following:

- Project plans, proposals, and status reports to determine the effectiveness of IT project manager collaboration with stakeholders (e.g., through the PMO) for oversight and completion of IT projects.
- Board and committee minutes to evaluate how the entity prioritizes projects relative to business goals and objectives, evaluates the project's effect on operations, and monitors and supports projects during execution.
- Project plans and proposals to determine how well they identify the project purpose, the requirements to address business needs, and the deliverables for each project phase.
- Change management documentation to determine the appropriateness of change decision-making levels and the consistency of approved changes with the project charter and plan.
- Testing and quality management plans to determine the adequacy of quality controls.
- Project closeout documentation to evaluate the entity's ability to inform future projects.

¹²⁴ Refer to U.S. Government Accountability Office's [The Post-Implementation Review](#).

Project management is the use of specific knowledge, skills, tools, and techniques to deliver something of value to people.¹²⁵ Effective project management includes established policies, standards, and procedures that project personnel apply enterprise-wide. Examples of projects include developing a new product or service, expanding into a new geographic market, and investing in a new system. When reviewing and prioritizing projects, effective management considers the project's effect on operations and the entity's needs (e.g., IT, information security, lines of business, customer needs, and regulatory and legal compliance). Entity projects often include a supporting IT project due to the underlying systems and components in business operations. For instance, when management considers offering a new product or service or expanding into a new geographic market, there are often IT implications. Effective IT project management processes, which are a subset of and align with the enterprise project management policies, standards, and procedures, should address issues specific to IT projects. Effective management develops and follows consistent processes to identify risks and oversee IT projects to address any risks identified. IT projects generally include IT system development, acquisition of a new IT system or component, or significant maintenance of or change to an IT product or service. If the entity has a PMO, IT project managers should work with the PMO to oversee and carry out IT projects.

An IT project should be managed in relation to the entity's size and complexity and consistent with the project's criticality and risks. An ineffectively managed IT project may result in late deliveries, cost overruns, or systems or components that do not meet entity, user, customer, or regulatory requirements. Systems or components that do not meet entity minimum standards or customer requirements can result in underused, insecure, or unreliable products or services. Adding functions, security, or automated controls into systems or components late in the initial development or after implementation to address missed requirements may incur substantial costs (e.g., personnel, time, and money), resulting in less effective systems or components. Furthermore, poor project management can lead to legal issues, such as violations of law and regulation and monetary penalties.

The project management discipline discussed in this section and the SDLC discipline discussed in the next section overlap significantly. In practice, effective system and component development teams integrate discipline use without duplicating effort.

IV.N.1 IT Project Phases

A general project management life cycle is shown in figure 3. The type of IT project (e.g., development, acquisition, or maintenance) will affect the project management life cycle chosen. For example, when an SDLC is chosen for a development project (e.g., adaptive versus predictive), the procurement processes chosen for an acquisition project, and the change control practices chosen for a maintenance project will affect how the project is managed. Furthermore, the activities completed within a project's life cycle are based on the characteristics of a project and the employed project management methodology.

¹²⁵ Refer to PMI's "[What Is Project Management?](#)"

Figure 3: Project Management Life Cycle



A project team often begins a project by creating a proposal to management that explains the business case including the desired system and component features and project scope, the planned benefits, the estimated time required, and the estimated cost.¹²⁶ Management reviews the proposal and determines whether the project is feasible and makes sense for the entity. If management approves the proposal and initiates the project, the business case serves as the basis for developing a detailed project plan.

The four main phases shown in figure 3 (Initiation, Planning, Execution, and Closeout) are described further in the following subsections.

IV.N.1(a) *Initiation*

The project's initiation phase begins with identifying stakeholders who determine the project's purpose, scope, and final deliverables. The following would typically be completed during this phase:

¹²⁶ PMI, [A Guide to the Project Management Body of Knowledge](#), fifth edition, p. 50.

- A project request that provides the business case including a description of the work, the benefits, alternatives considered, the impact of not doing the work, initial estimates of resources and schedule, and strategic match.
- A project charter that identifies the project owner (i.e., the responsible party), and defines the mission and main goals of the project.
- Initial business and technical requirements.¹²⁷

When the project involves developing a new system or component or making significant changes to an existing system or component, management analyzes and determines whether to develop or acquire (referred to as “build or buy”) the solution. A feasibility study¹²⁸ helps in the process of making this determination. Considerations in the feasibility study include availability of internal expertise, cost of building the solution compared with procuring it, availability of an external product that meets the entity’s requirements, solution implementation timeline, and the project’s complexity. Refer to table 2 in the “[Feasibility Study](#)” section of this document for additional feasibility considerations. Regardless of whether the decision is to build or buy, the feasibility analysis helps management to verify the reasonableness of the preliminary assumptions and to identify resource requirements in greater detail.

IV.N.1(b) *Planning*

In the planning phase, management forms a project team¹²⁹ that defines and refines project deliverables to achieve the objective and develops the project plan. Project plan common elements are tasks and milestones, task timelines, and names of those who are responsible for completing each task. Project teams engage stakeholders to define deliverables that achieve objectives and meet the entity’s functional, IT, information security, and legal and regulatory requirements. Requirements include systems, components, and resources that will support and interact with any new product or service. Clearly defined deliverables (including documentation deliverables) help stakeholders understand expectations. The project team should also define testing requirements and objective acceptance criteria, which are unbiased and predefined criteria for determining whether the project meets the stated objectives through milestones and project completion. Additionally, security and resilience design should be included from the beginning of the project to be most effective. Information regarding project management governance is in the *FFIEC IT Handbook*’s “[Management](#)” booklet.

¹²⁷ The NIST Glossary defines “[requirement](#)” as “a statement that translates or expresses a need and its associated constraints and conditions.”

¹²⁸ A feasibility study considers the critical aspects of a proposed project; assesses the degree to which the requirements, designs, or plans can be implemented; and helps determine the likelihood of the project’s success. A formal feasibility study may not be performed at smaller, less complex entities; however, management should perform some analysis of system or component needs for a given project.

¹²⁹ Depending on the IT project type and complexity, the project team may include multidisciplinary stakeholders from varying lines of business. An effective project team’s roles and responsibilities are clearly defined and communicated so everyone involved is aware of their responsibilities.

IV.N.1(c) *Execution*

During the project's execution phase, the project team completes the project plan tasks. The team tracks and compares actual task execution with the project plan, maintains a log of problems (e.g., inability to meet milestones, resource changes, and unanticipated risks), tracks problem resolution, reports on effects to the project timeline, and monitors interdependency issues. During the execution phase, scope creep is a common problem that can occur as developers address issues or receive subsequent requests to add or modify a system's features. It may result from inadequately defined requirements, a lack of a project change control process, inaccurate time and budget analysis, or a weak project manager or executive sponsor. Establishing change approval procedures during development and cutoff dates (after which time requested changes are deferred to subsequent versions) helps mitigate scope creep.

Strong change approval procedures enforced by management can mitigate the risks that come with scope creep. Procedures can include independent project monitoring for additions or modifications of functional and nonfunctional features to help enforce management review and approval. Procedures can also include project plan variance management reporting that could indicate scope creep (e.g., delays in completion of tasks or cost overruns). Significant project plan variances may require the entity to reassess and re-baseline project plans. Project managers regularly report the project's status to stakeholders, senior management, and, when appropriate, the board in order to inform of changes and issues.

Strong testing and other QC procedures can mitigate the risk that the entity's project goals and stakeholder requirements are not met during the execution phase. Testing helps find deficiencies or defects and helps ensure that the system or components operate as intended. Depending on the project type, testing may be scheduled throughout the project during any phase. For example, testing may not always occur during every sprint when using an agile development methodology. Users, designers,¹³⁰ developers, and IT staff may be involved in testing. Throughout the testing process, management should maintain comprehensive and accurate documentation reflecting the testing methodology employed, tests performed, and test results.

IV.N.1(d) *Closeout*

During the project's closeout phase, the project team delivers the agreed-upon scope items as outlined in the project plan. For example, in a systems development or acquisition project, project closeout is when the project team transitions the systems to the operations staff (i.e., moves application from a staging to a production environment). Often during the project closeout, project teams analyze the project (i.e., post-implementation review) to identify effective project practices and discuss issues encountered and how they were resolved. This information is used to inform and improve project management practices. Project teams review project documentation in the closeout phase to ensure that it is complete, supports maintenance, and can be used by future teams to identify effective practices.

¹³⁰ Designers may include personnel engaged in creation and execution of plans for a project or structure (e.g., graphic designers, web developers and digital designers, web and digital interface designers, computer programmers). See Bureau of Labor Statistics, [Occupational Outlook Handbook](#), for more information on job descriptions.

IV.N.2 Monitoring and Controlling

Monitoring and controlling are important parts of the processes of IT project management. This takes place throughout all phases of IT project development (refer to figure 3). Monitoring and controlling are helpful for tracking, reviewing, and evaluating the progress of an IT project. Monitoring and controlling helps management identify IT project management risks (e.g., errors, cost overrun, scope creep, and missing milestones). A combination of management and the project manager or sponsor are responsible for monitoring and controlling the entire project throughout all phases.

During the initiation phase, monitoring and controlling activities include the following:

- Validating that relevant stakeholders are identified and all stakeholders' project requirements are well-defined.
- Coordinating the project phases, including tasks and activities, sufficiency of resources, and process steps and timing for each phase.
- Validating that the project scope is sufficiently identified and refined to minimize scope creep.
- Evaluating the application of project management policy, standards, and procedures.
- Validating that appropriate success criteria are identified and the project is feasible.
- Determining effective establishment of reporting lines, reporting processes, and reports.

During the planning phase, monitoring and controlling activities include the following:

- Validating the appropriateness of the project plan's tasks and time frames as well as resource sufficiency.
- Reviewing the project plan iteratively and validating any approvals for any updates.
- Validating stakeholder support and engagement.
- Verifying that the project plan and associated project documents are appropriate, comprehensive, and approved.

During the execution phase, monitoring and controlling activities include the following:

- Meeting regularly with the project team to track progress, address impediments or issues, and track task and milestone completion.
- Monitoring, measuring, and analyzing project performance compared to the project plan and identifying any variance.
- Validating that any changes are authorized, quality is maintained, scope creep is mitigated, and stakeholders are informed.
- Recommending corrective or preventive action.
- Verifying that configuration management policies and procedures are followed.
- Monitoring expenditures compared to the project budget and addressing any cost overruns.

During the closeout phase, monitoring and controlling activities include the following:

- Validating that the project team follows closeout processes when the project is complete.
- If a project is discontinued before implementation, determining and documenting the reasons for the abnormal project closure for use by future project teams.
- Verifying that project deliverables were accepted.
- Overseeing a post-implementation review.
- Confirming that the system or components have been added to inventories that support routine maintenance, such as patching.

IV.N.3 IT Project Documentation

IT project documentation helps ensure clear communication among the project team, management, and other stakeholders. For example, strong written documentation provides a record of key decisions (e.g., project approvals, timeline, and scope changes) that the project team can refer to throughout the project.

Types of IT project documentation range from simple documents, such as meeting minutes and project status reports, to more complex documents such as feasibility studies, project plans, requirements, and PIRs. Project documentation allows management to track and monitor security, resilience, and compliance concerns throughout the project and after its completion. Entities establish documentation standards and procedures to mitigate the risk of inconsistent or incomplete documentation. When determining the amount of project documentation needed, various factors to consider include an entity's size and complexity, the project type (e.g., development, acquisition, or maintenance), and the project's complexity. The following subsections describe common examples of project documentation.

IV.N.3(a) IT Project Request

IT project requests outline proposed projects including the reason for initiating the project. Effective project requests convey proposed business objectives and project requirements between the project team, management, and other stakeholders. Project requests also identify project responsibility and accountability, including identifying the project sponsor. Project requests often include the following:

- Project sponsor.
- Customer or user.
- Other stakeholders.
- Purpose and proposed scope of the project.
- Project deliverables.
- Project constraints (e.g., time, budget, and technology).
- Business case.¹³¹

¹³¹ A business case generally accompanies the project request and provides additional information to help set appropriate parameters for the project.

IV.N.3(b) *Business Case*

A business case conveys business related information to help management determine whether to fund a project. The goal is to justify the project resources (e.g., budget and staffing) to address a business need. Typically, the project’s sponsor helps to develop and owns the resulting business case.¹³² Business cases often include the following:

- The need or problem the project will address (e.g., systems not meeting operational requirements or loss of market share).
- Alternative solutions including estimated staffing, timeline, costs, benefits, and risks.
- The proposed solution with rationale (e.g., buy a new system or develop a new component).

Effective business cases address both the parameters for implementing and maintaining the solution. For example, both the costs to build and maintain various system options are analyzed before a proposed solution is presented.

IV.N.3(c) *Feasibility Study*

A feasibility study is an analysis of a known problem or need and the proposed solution conducted independent of the project request team. It helps stakeholders evaluate a proposed solution considering relevant factors—including economic, technical, legal, and scheduling considerations—to determine a project’s probability of success. Table 2 outlines feasibility study considerations.

Table 2: Feasibility Study Considerations

Business considerations	• Entity objectives. • Effect on existing operations. • IT security risk assessment to determine security risks and mitigation needs. • Entity’s IT and information security requirements addressing data confidentiality, integrity, availability, and resilience. • Expected benefits. • Potential entity changes regarding facilities or the addition or reduction of users, IT staff, key security roles, or managers. • Budget, scheduling, training, or personnel constraints (including for oversight of third-party relationships). • Licensing needs. • Potential legal or regulatory issues that could affect the project’s feasibility. • Estimated completion dates of IT projects and major project milestones. • Expected benefits and risks for consumers relative to the new product or service. • Third party’s due diligence throughout the supply chain.
Functional requirements	• End user needs. • Internal control and information security requirements. • Operating, database, and backup system requirements (e.g., type, capacity, performance, scalability, and resiliency). • Hardware requirements (e.g., infrastructure needs, processing chips, and credit card or point-of-sale components). • Facility needs (e.g., raised floor, cabling, and heating, ventilation, and air conditioning [HVAC]).

¹³² Refer to PMI, “[Is This Really Worth the Effort? The Need for a Business Case.](#)”

	• Network requirements (e.g., physical, virtual, software-defined, and hyper-converged networks; types of storage; number of users; and type, volume, and frequency of data transmission). • Connectivity and interface requirements with internal or external applications, third-party service providers, internal or external users, and customers. • Third-party hardware and software vendor requirements related to entity functional requirements. • Product development, design, and testing standards throughout the supply chain. • Supply chain considerations related to entity business considerations and functional requirements. • Entity's requirements compared to third-party products, services, and activities implemented in the supply chain.
Cost-benefit analysis	• Expected useful life of the proposed product or application. • Alternative solutions (e.g., build or buy). • Estimated costs of projects (e.g., overall and by project phase). ◦ Nonrecurring project costs (e.g., hardware, software, and overhead). ◦ Recurring operational costs (e.g., personnel, maintenance, telecommunications, and overhead). • Soft (or intangible) costs.¹³³ • Tangible benefits (e.g., increased revenues, decreased costs, and return on investment). • Intangible benefits (e.g., improved public opinion or more useful information).

IV.N.3(d) *IT Project Plans*

IT project plans describe how a project will be executed, monitored and controlled, and closed. Entities use project plans to communicate tasks, time frames, and responsible parties to project stakeholders throughout a project. The details in an IT project plan identify necessary technical steps in sequence and help the team identify any missing tasks that are needed to achieve the project's objectives. The project plan also identifies interconnectivities and interdependencies throughout the project—how segments of the project are interrelated. Generally, IT project plans consider the following:

- Approved project scope.
- Roles and responsibilities.
- Communication among the project team, stakeholders, and management.
- Schedule, including completion of key tasks and achieving milestones.
- Quality management tasks (e.g., testing both developed systems and patches for procured systems).
- Risk management tasks (e.g., periodic risk reviews).
- Task budgets.
- Implementation tasks (e.g., training and deployment).

IV.N.3(e) *Closeout Documentation*

Entities use closeout documentation to apply lessons learned from past projects to future projects. These lessons can include practices and techniques that were effective, problems that could be avoided if particular processes are used, and how high-performing project teams were

¹³³ Soft costs generally include indirect dollars spent in other areas (e.g., sales, general, and administrative expenses) to support a change in business model, equipment, or practices.

formed. Many lessons can be memorialized by updating existing policies, procedures, and standards. Several documents can be used to improve future projects, such as the following:

- Project plans with projected and final task completion dates.
- PIR.
- Risk reviews including suggested changes to project management-related policies, standards, and procedures.

IV.O System Development Life Cycle

Action Summary

Management should implement an SDLC to manage systems and system components throughout their life cycle and achieve the objectives of confidentiality, integrity, availability, and resilience to achieve the entity's business objectives.

Examiners should review the following:

- The documented management and control processes, including for supply chain partners.
- Responsibility and accountability assignment.
- Key stakeholder involvement level.
- Stakeholder communication and tracking of all SDLC phases and actions.

One NIST SDLC definition is that it is “the scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, ongoing operation and maintenance, and ultimately its disposal that instigates another system initiation.”¹³⁴ The acronym SDLC is also used to refer only to software development and implementation (standing for the software development life cycle). However, this booklet uses the acronym SDLC to refer to the broader concept encompassing the entire system and its components. If an entity engages in internal development activities, management should have a documented process (e.g., SDLC) that management and personnel use to manage and control development activities. Effective SDLC processes are well-documented by organizations such as NIST.¹³⁵ Using proven processes helps to mitigate the various risks of building, maintaining, and retiring systems. Implementing the SDLC allows management to organize these activities into smaller, more manageable segments or phases. Data security should be considered throughout all phases of the SDLC to maintain confidentiality, integrity, availability, and resilience.

The SDLC discipline discussed in this section and the project management discipline discussed in the last section overlap significantly. In practice, effective system and component development teams integrate discipline use without duplicating effort.

¹³⁴ Refer to [NIST Glossary](#).

¹³⁵ Refer to NIST SP 800-160, vol. 1, rev. 1, [Engineering Trustworthy Secure Systems](#).

IV.O.1 SDLC Phases

Action Summary

During the SDLC phases, system development project teams work to achieve project objectives, mitigate the risk of lower quality development projects, and address security. These considerations are considered throughout all phases.

Examiners should review elements of each phase such as the following:

Initiation Phase

- The system's purpose, expected benefits, how it supports business objectives, and any legal and regulatory requirements.
- Initial security impact analysis and validation of the appropriate project specifications.
- Extent to which the project request is communicated to stakeholders in the supply chain.

Development or Acquisition Phase

- Design specifications, including security control design.
- Risk assessments, including using the results of security risk assessment, to supplement the baseline security controls.
- Risk mitigation strategies.
- Test, conversion, implementation, and training plans, accounting for confirmation of the functionality and controls.
- Change management documentation.
- Draft user, operator,¹³⁶ and maintenance manuals.

Implementation and Assessment Phase

- Design reviews and system tests, including any new specification testing.
- Deployment approach (e.g., phased-in, simultaneous).
- Training, including user and system support documentation.
- PIR.

Operations and Maintenance Phase

- Performance and controls monitoring.
- Change management controls, including as used to control configurations.
- ITAM inventory and associated audits.

Sunset and Disposal Phase

- Plans and validation measures for accessing and retrieving data from archives.
- Off-boarding procedures, including for third-party providers.
- The entity's post-disposal review, including any lessons learned documentation.

¹³⁶ Refer to [NIST Glossary](#).

Effective management understands the SDLC phases and the actions needed in each phase. The phases may be divided differently depending on the entity, the project type and characteristics, and the SDLC used. Management should identify the actions and assign responsibility and accountability for completing those actions. Key stakeholders of the system or component being developed or modified should monitor progress in each phase including the output of each phase. This involvement mitigates the risk that the system or component does not deliver the requested functionality. Management should maintain confidentiality, integrity, availability, and resilience throughout all phases of the SDLC.

An entity that defines its SDLC phases helps ensure transparency and accountability to, and agreement and system or component acceptance by, the stakeholders. Figure 4 illustrates the five general SDLC phases (Initiation, Development or Acquisition, Implementation and Assessment, Operations and Maintenance, and Sunset and Disposal) identified by NIST.¹³⁷

Figure 4: NIST Example of a System Development Life Cycle



IV.O.1(a) *Initiation*

The initiation phase begins when entity personnel identify an opportunity to build, buy, or modify a system or component and formally seek approval with an IT project request. The project team should describe the IT project's purpose, identify expected benefits, and explain how the proposed system or component supports the entity's objectives. The project team should summarize the confidentiality, integrity, availability, resilience, and legal and regulatory

¹³⁷ Refer to NIST Information Technology Laboratory (ITL) Bulletin, "[The System Development Life Cycle \(SDLC\)](#)."

requirements. They should identify alternative solutions and justify their recommended solution. Through IT project request development, stakeholders should gain a common understanding of the project's objectives, security considerations, and risk management planning to mitigate the risk of project failure.

During the IT project request review, management can accept, reject, or request changes before it allocates resources. Management can also commission a formal feasibility study to inform its decision. If the IT project request is to modify an existing system, management should consider performing a security impact analysis¹³⁸ to identify any negative impact to existing security controls. Such a security impact analysis may be performed as part of the feasibility study.

Planning, particularly in the project's early stages, should help the project team and management coordinate development activities and manage risks effectively. Planning helps the project team and management add or clarify the project's specific activities, resources, costs, and benefits. A critical part of planning is to coordinate stakeholder discussions to identify and document as many of the entity's functional, security, and network requirements as possible.

Primary items entity personnel typically include in planning consist of the following:

- Responsibilities of third-party service providers, internal audit, information security, and IT staff.
- Entity SDLC processes.
- SDLC phase acceptance criteria including review and approval procedures to help ensure that development teams complete all SDLC phase or independent sprint requirements before moving into subsequent phases.
- Control and security features to be designed and built, or acquired, and implemented.
- Change management processes to minimize disruption to the project plan.
- Risk management processes, including project methodology selection.
- Cost tracking mechanisms, including to track overhead (e.g., office space, hardware, and software used during the project) as well as other related costs (e.g., budgeting personnel expenses, outsourced activities).

When evaluating IT project requests, effective management considers input from all stakeholders. For example, management evaluates the appropriateness of the requested functional requirements. Each function has design and development implications. Each function requires testing, documentation, and ongoing support. Therefore, the exclusion of unnecessary functions can significantly reduce the resources required to support a request. Management considers and analyzes all requests to determine whether to develop or acquire the system or component.

¹³⁸ For more information on conducting a security impact analysis, refer to NIST SP 800-128, [*Guide for Security-Focused Configuration Management of Information Systems*](#).

IV.O.1(b) *Development or Acquisition*

During the development or acquisition phase, the system or component is designed and developed or acquired. Key system or component designs are created or reviewed before development begins or the acquisition is completed. When a project is initially proposed and reviewed, the decision to develop or acquire may be uncertain. Early stakeholder involvement in design creation or acquisition specification review mitigates the risk that the system design does not support the functional requirements. The more predictive the SDLC is, the more design work will occur earlier in the SDLC. The more adaptive the SDLC is, the more design work will be spread throughout the SDLC phases.

When an entity acquires a system or component, important design considerations include how much configuration is possible, whether the system or component can be restored to a secure configuration, and whether there are restrictions on users or services that can make configuration changes. Entity personnel can configure systems and components to avoid specific known threats and risks based on the entity's risk appetite. For example, if a product or service is used by bank customers, it may be important that the product or service's security and functionality allows the capability for the customer to change some configurations (e.g., change location restrictions, adjust monetary limits, and allow use of physical access controls).

System and component security should be a high priority throughout this phase. If an IT security risk assessment was conducted as part of the feasibility study, it can be used early in this phase to design baseline controls to address risks identified. If an IT security risk assessment was not completed as part of the feasibility study, it can be completed early in this phase. Designing security controls early in the development and acquisition phase is important to system or component confidentiality, integrity, availability, and resilience. If the system or component is being developed or acquired, it is important to address security concerns, such as those for customer information, and personnel should "identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems."¹³⁹ Therefore, it is important to identify security controls requirements and consider appropriate controls that might affect the entire supply chain. It is typical for system and component functionality and design to change throughout the phase, which can change security effectiveness. The security impact analysis performed during the SDLC initiation phase can be helpful to evaluate security adequacy before, during, and after system and component changes are made in this phase.¹⁴⁰ Early implementation

¹³⁹ Refer to [GLBA](#) and 15 USC 6801 and 6805(b), further implemented by FFIEC members as follows: FDIC: 12 CFR 364, appendix B, "[Interagency Guidelines Establishing Information Security Standards](#)," and 12 CFR 364, supplement A to appendix B, "[Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#);" FRB: Regulation H, 12 CFR 208, appendix D-2, "[Interagency Guidelines Establishing Information Security Standards](#)," and Regulation Y, 12 CFR 225, appendix F, "[Interagency Guidelines Establishing Information Security Standards](#)"; NCUA: 12 CFR 748, appendix A, "[Guidelines for Safeguarding Member Information](#)"; OCC: 12 CFR 30, appendix B, "[Interagency Guidelines Establishing Information Security Standards](#)." Additionally, refer to FTC 16 CFR 314, "[Standards for Safeguarding Customer Information](#)," for similar provisions for service providers.

¹⁴⁰ For more information on conducting a security impact analysis, refer to NIST SP 800-128, [Guide for Security-Focused Configuration Management of Information Systems](#).

of security controls can minimize their cost, allow for efficient deployment, and reduce integration issues.

Appropriate personnel should define and create initial testing, conversion, implementation, and training plans and obtain management approval during the development or acquisition phase. Development personnel should initially test the design during development to confirm that the system's or component's functionality is meeting requirements and controls, including security controls, are functioning as intended. Testing early and throughout this phase helps a team identify functional or security flaws when remediation can be less expensive.

The potential for scope creep increases during this phase, and project stakeholders monitor and mitigate this risk. Effective entities have a process to review the appropriateness of new or modified requirements and development changes to minimize scope creep, as discussed in the [“IT Project Management”](#) section of this booklet.

Designers should document completed designs and functions, including information security designs. Design documents may include system architecture, software architecture, and data structure design. Detailed documentation enhances a developer's ability to modify systems and components after they are placed into production. The documentation should include appropriate information such as all related systems and components (including IoT product components and devices), any accreditation, certification, or evaluation results. Documentation can be used by management to compare original objectives and specifications with systems and components ready for implementation. The development team typically drafts user, operator, and maintenance manuals during this phase.

IV.O.1(c) *Implementation and Assessment*

The objective of the implementation and assessment phase is to prepare the system, operational environment, entity, and end users for system or component use, and to assess whether the system or component meets business needs and operational requirements. In this phase, the team configures and enables system or component features, tests the features' functionality, and installs or implements the system or component after obtaining appropriate approvals.

It is important to thoroughly test before implementation to help ensure that the system or component meets all entity specifications. These tests should be documented so that as the system or component is changed, previous tests are used and adjusted to validate rather than creating new tests. Building on original testing documentation also may result in subsequent tests being more comprehensive than if they were not leveraged.

The more complex and critical the development or acquisition, the more important it is to rigorously assess the product before implementation. For example, conversions of core banking systems require more detailed reviews and higher levels of approvals from management given their significance to delivery of business services, as opposed to a lower level of oversight for routine maintenance of a less critical system. These reviews would occur before implementation. In the more complex and critical implementations, approval from many stakeholders such as business continuity management, information security, and third-party risk management may be

necessary. For more information on routine changes and conversions, refer to the “[Implementing Changes](#)” section of this booklet.

Primary implementation phase tasks include communicating the implementation schedule to internal and external stakeholders, training users, and installing the system or component. To be most effective, the implementation schedule takes into account the business impact (e.g., conversions are scheduled on long weekends to allow additional time before affecting weekday business). Management and other appropriate personnel perform tasks such as the following during the implementation phase:

- Execute the implementation plan, including the following:
 - Assessing risk for issues that may occur during implementation activities (e.g., rollout, conversion, or update).
 - Conducting user acceptance testing (UAT).
 - Updating the asset inventory.
 - Training (internal and external).
- Input, import, or convert data and validate the functionality of the system or component using those data.
- Confirm the confidentiality, integrity, availability, and resilience of systems and data.
- Confirm the interoperability of systems and components.
- Configure and test system and component security controls.
- Validate performance parameters (e.g., throughput, capacity, error rates, and memory usage) and ensure that the system or component operates as expected.
- Conduct a final audit of information security and adherence to policies and procedures, as well as risk tolerance levels. Determine whether the findings of the audit meet the entity’s predetermined requirements for system deployment.
- Create and test back-out or rollback plans to prepare for unforeseen and unrecoverable problems that may occur during implementation. Entity personnel may accomplish this by various back-out or rollback methods (e.g., using one or more restart points or reverting to the legacy system or prior version).
- Conduct PIRs (e.g., survey users, review complaints, plan future functionality, and identify other improvements). Additionally, the reviews may identify lessons learned and process improvement information.

Implementation strategies vary and are designed to mitigate different types of implementation risk. Examples of implementation types may include the following:

- **Parallel implementation** consists of running the old and new system or component simultaneously until the new system or component is evaluated and approved. If the new system fails, operations can continue using the old system while issues are corrected. Running two systems or components simultaneously requires additional resources (e.g., costs, personnel, and time), but is a logical strategy if no system downtime is tolerable.
- **Pilot implementation** involves releasing the complete, new system or component to a limited (i.e., pilot) group of users. After successful rollout to that pilot group, management decides how to proceed with the rollout process. Advantages of using a piloting strategy

include minimizing the risks of a comprehensive rollout to the entire user population, as well as opportunities to test the system with the initial rollout and any additional rollouts.

However, this strategy may also be time-consuming and expensive. A risk to this strategy is that it may allow for large numbers of insignificant enhancements instead of focusing on critical system issues.

- **Phased implementation** involves deploying a new system or component in phases (i.e., rolling out modules, features, or functionality incrementally over time) generally according to a predetermined schedule. This strategy helps mitigate the risk that a foundational flaw is discovered at the end of the project rather than earlier when it would be easier to correct. This strategy potentially requires less training and fewer resources spent at one time, and potentially fewer errors on which to focus during each phase. This strategy may lengthen the implementation time frame. In addition, there may be integration and interoperability concerns, such as reverse compatibility issues with legacy components while the old system is being replaced in phases.

Training is critical to the success of the implementation and assessment phase as are training plans and supporting materials for operating, using, and maintaining the system. Training is often the first exposure to the system for most users and should be provided before system or component deployment to the production environment. Training enables users to familiarize themselves with the new or updated system or component. A positive training experience typically improves user acceptance. During this phase, appropriate personnel should coordinate training logistics, including who should be trained, what the training involves, and when training should be conducted. Effective management organizes a training and awareness campaign and notifies users of any implementation and training responsibilities. This helps establish user expectations regarding system and component capabilities. Those responsible for supporting the system or component in the entity should have a combination of technical documentation, training, and hands-on assistance enabling support personnel to provide operational support to the users. Once the product is implemented, management should perform a PIR (see the “[Post-Implementation Review](#)” section of this booklet for more information).

IV.O.1(d) *Operations and Maintenance*

In the operations and maintenance phase, systems and components are in production and operating; enhancements and other modifications are developed and tested; and hardware and software components are changed. Entity personnel should continuously monitor system and component performance and adjust the system or component so that it operates consistent with pre-established user, security, and other entity requirements. Entity personnel should manage and document configuration changes whether baseline or unique. Documenting system and component changes and assessing the potential impact of these changes on a system’s or component’s security, functionality, performance, and resilience are essential activities in this phase.

Maintenance can occur periodically or regularly, such as annually, semiannually, quarterly, or weekly. In agile-based methodologies, maintenance may occur continuously. The maintenance frequency varies across systems and components, and the timing is prompted by business and operational need.

An entity's change control processes play an important role in the operations and maintenance phase. Changes to a system or component can affect baseline configurations and controls, and this impact should be analyzed. To mitigate the risk of an enhancement or other modification disrupting or degrading operations, effective entities follow established change management policies, standards, and procedures. For more information, refer to the "[Maintenance](#)" section of this booklet and the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" and "[Information Security](#)" booklets.

Examples of commonly performed tasks in this phase are the following:

- Ensuring that systems and components are operational and available during the defined hours of operation.
- Implementing nonemergency change requests during scheduled outages.
- Ensuring that all processes, manual and automated, are documented.
- Ensuring adequate resource availability for operations, maintenance, and resilience.
- Performing and testing system, component, and data backups.
- Validating the entity's physical security measures.
- Ensuring that contingency plans for resilience are updated, tested, and funded.
- Ensuring that all operations and maintenance personnel take appropriate, ongoing training.
- Maintaining and monitoring system and component performance measurements, statistics, and system logs.
- Ensuring that third-party SLAs are being monitored and met.
- Performing configuration, security, and design assessments to ensure that system and component parameters and configurations are correct.
- Patching software for systems and components.
- Managing and controlling configurations and changes to the system. This includes installing, configuring, upgrading, and maintaining systems, components, and data, as well as related documentation.

Management is responsible for operations and maintenance phase task performance regardless of whether tasks are performed by entity or third-party personnel. For more information, refer to the *FFIEC IT Handbook's* "[Outsourcing Technology Services](#)," "[Business Continuity Management](#)," "[Architecture, Infrastructure, and Operations](#)," and "[Information Security](#)" booklets.

IV.O.1(e) *Sunset and Disposal*

In the sunset and disposal phase, plans are developed for the orderly termination of systems or components and the preservation of data that reside in them during the transition to a new system or component. Data to be preserved include entity data and client and consumer data. The systems, components, and data may be migrated to another system, archived, reassigned, or destroyed. There are several risks in the disposal phase such as the risk of sensitive data disclosure to unauthorized individuals, business functionality impairment, and intellectual property loss. Archive solutions may address the frequency and speed of any

future data retrieval. Additionally, effective entities have a process in place to periodically validate the accessibility of archived data.

Specific tasks and activities occurring during this phase depend on the risk and complexity of the systems, components, or services. Considerations in system retirement and disposal include the following:

- Disposal or transition plan involving all applicable parties that identifies critical steps, decisions, and milestones to properly terminate, transition, and dispose of a system, component, service, and data.
- Hardware and software components to preserve, including for archive use.
- Data archive and migration—data could be migrated to the new system, archived, or a combination of the two.
- System and component documentation preservation.
- Advanced notification to all end users and stakeholders of the system or component sunset plan and the planned termination date.
- Plans for end-user migration to a replacement system or component.
- Plans for permanently erasing (i.e., sanitizing) data from the terminated system or component. Methods for sanitization include deleting, overwriting, and destroying data.¹⁴¹

If the system or component requiring disposal is managed by or the related data are stored by a third party, comprehensive off-boarding procedures help mitigate risks related to unauthorized access to sensitive information. Procedures should address items such as access, security, data governance and storage, and recordkeeping requirements (e.g., legal, regulatory, compliance, and audit). Effective management has a process to validate that its third party appropriately performs all necessary steps associated with system, component, data, and service sunset and disposal. The third party should maintain and make available to management evidence (e.g., certification) of disposal and archival activities to demonstrate completion.

Effective entities perform a post-sunset and disposal review that confirms the necessary processes were completed and documents lessons learned from shutting down and archiving the terminated system or component. The review should identify archived data and documentation locations. The review may be conducted again within six months of system or component disposal to identify any missed issues that only surface after an extended period of the system or component not being available.

For more information on sunset and disposal, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)," "[Information Security](#)," and "[Outsourcing Technology Services](#)" booklets.

¹⁴¹ For more information on data sanitization processes, refer to the *FFIEC IT Handbook's* "[Information Security](#)" booklet.

IV.P Third-Party Relationship Risk Management

Entities can realize significant benefits from working with third parties such as gaining access to new technologies, human capital, delivery channels, products, services, and markets. However, the use of third parties can reduce an entity's direct control over activities and may introduce new risks or increase existing risks¹⁴² in development, acquisition, and maintenance activities. Increased risk often arises from greater operational or technological complexity, newer or different types of relationships, or potentially inferior performance by the third party. As part of sound risk management, entities engage in more comprehensive and rigorous planning, due diligence, oversight, and management of third-party relationships that support higher-risk development, acquisition, and maintenance activities, including critical activities. Considerations discussed are relevant to each entity's development, acquisition, and maintenance activities, based on specific facts and circumstances, but may not apply to all of an entity's third-party relationships.

IV.P.1 Planning

As part of sound risk management, effective planning allows an entity to evaluate and consider how to manage risks before entering into a third-party relationship. Higher risk and greater complexity development, acquisition, and maintenance services warrant more careful planning and other considerations to mitigate the risk that the relationship will result in material negative impacts on the entity. Refer to the [Interagency Guidance on Third-Party Relationships: Risk Management](#) and FFIEC IT Handbook's "[Outsourcing Technology Services](#)" booklet for more information on planning concepts.

IV.P.2 Due Diligence and Third-Party Selection

Conducting third-party due diligence¹⁴³ before selecting and entering into relationships is an important part of sound risk management when engaging third parties in development, acquisition, and maintenance activities. Due diligence gives management the information needed to determine whether a relationship would help achieve a banking organization's strategic and financial goals. Third parties that would support an entity's higher risk or more complex development, acquisition, and maintenance activities typically warrant a greater degree of due diligence.

In some instances, the appropriate entity personnel may not be able to obtain the desired initial due diligence information from a third party. For example, the third party may not have a long operational history, may not allow onsite visits, or may not share (or be permitted to share) information that is requested. While the methods and scope of due diligence may differ, the

¹⁴² Refer to the [Interagency Guidance on Third-Party Relationships: Risk Management](#).

¹⁴³ Merriam-Webster defines "[due diligence](#)" as "the care that a prudent person might be expected to exercise in the examination and evaluation of risks affecting a business transaction." Due diligence includes assessing the third party's ability to perform the activity as expected, adhere to an entity's policies related to the activity, comply with all applicable laws and regulations, and conduct the activity appropriately.

entity's project management process should identify and document any limitations, understand the risks of such limitations, and consider potential alternatives.¹⁴⁴ Management should evaluate the conclusions from such supplemental efforts based on the entity's own specific circumstances and performance criteria for the activity. Refer to the [Interagency Guidance on Third-Party Relationships: Risk Management](#) and FFIEC IT Handbook's "[Outsourcing Technology Services](#)" booklet for more information on due diligence concepts.

IV.P.3 Contract Negotiation

When evaluating whether to enter into a relationship with a third party, an entity's management typically determines whether a written contract is needed; and, if the proposed contract can meet the entity's business goals and risk management needs, then entity management typically negotiates appropriate contract provisions¹⁴⁵ for development, acquisition, and maintenance activities. In certain circumstances, it may be advantageous to negotiate initial development, acquisition, and maintenance contracts with other organizations (e.g., banking associations or user groups). As part of its oversight responsibilities, the board should be aware of—and, as appropriate, may approve or delegate approval of—contracts involving higher-risk development, acquisition, and maintenance activities. Refer to the [Interagency Guidance on Third-Party Relationships: Risk Management](#) and FFIEC IT Handbook's "[Outsourcing Technology Services](#)" booklet for more information on contract negotiation concepts.

IV.Q Supply Chain Considerations

Action Summary

Management should implement SCRM policies and procedures consistent with the entity's size, criticality to the financial system, and complexity.

Examiners should review the following:

- Relevant policies, standards, procedures, project plans, and any SDLC documentation to determine how the examined entity has incorporated SCRM into its enterprise-wide risk management practices.
- System and component control configurations and reports used by management to monitor, control, and protect communications at the key access points of information systems that inform SCRM activities.
- Entity's architectural designs, system and component development techniques, and systems engineering principles as well as those applicable to the entity's third parties to maintain effective information security throughout the supply chain.

¹⁴⁴ Refer to the [Interagency Guidance on Third-Party Relationships: Risk Management](#).

¹⁴⁵ [Ibid.](#)

- System and service inventories to determine how well the inventories identify all systems and services, how well they categorize each system and service’s criticality, and how well they identify the entire supply chain needed to provide the system or service.
- Entity’s methods for initially assessing and monitoring after implementation for provenance of systems, components, and data.
- Communication processes and documented communication of threat intelligence and vulnerability identification with supply chain partners.
- Entity management’s assessment of supply chain partners’ programs to address inauthentic or unapproved systems or components (e.g., counterfeit or shadow IT).
- SCRM controls in maintenance-related situations including monitoring for unauthorized modifications, communicating changes, and monitoring for EOL.

NIST defines “supply chain” as “a system of organizations, people, activities, information, and resources, possibly international in scope, which provides products or services to consumers.”¹⁴⁶ Supply chains evolve continuously through mergers and acquisitions, joint ventures, and other partnership agreements. Supply chains can be dispersed around the world.

Entities interact with a supply chain when they develop, acquire, and maintain logical or physical systems or components (e.g., computers, servers, and other hardware components, software, or services), and when they engage with a third party for a service. Even when an entity develops its own systems and components and manages its own infrastructure, it will still periodically interact with one or more supply chains when purchasing additional external hardware, software, raw materials, and services. As entities increase their reliance on third parties for systems, components, and services, supply chains are more complex, diverse, and interconnected.

If the entity incorporates systems and components from third parties in their development and maintenance activities, consideration of SCRM in the SDLC is appropriate. Awareness of risks arising from integration with suppliers’ systems and components helps with management of associated risks such as compatibility issues, backdoors, or unauthorized access points. Whether developed in-house or by a supply chain partner, additional scrutiny should be applied when custom development of systems and components occurs to ensure proper configuration to meet business and information security needs.

Supply chain risk is defined as “the potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products or services. Supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain.”¹⁴⁷ Examples of supply chain risks include counterfeit goods (e.g., unauthorized systems or components sold as authentic goods), substandard materials, loss of functionality, theft of data

¹⁴⁶ Refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

¹⁴⁷ Refer to [NIST Glossary](#).

or intellectual property (e.g., customer data and logos), and malware inserted into authentic systems and components.

Another supply chain risk is the potential to contract with a third party on the [U.S. Department of the Treasury’s Office of Foreign Assets Control \(OFAC\) Sanctions List](#) or located in countries that are on the list. Management should ensure that the entity’s supply chain partners are not on the OFAC list.¹⁴⁸ This may include evaluating the third party’s ownership structure (including identifying any beneficial ownership whether public or private, foreign or domestic).¹⁴⁹ To accurately determine whether a third party is on the list or affiliated with companies on the list, it is important to consider any nested relationships through common ownership or any subsidiary or affiliate relationships. It is important to understand risks related to supply chains by tracking interdependencies between all parties involved (e.g., owners and third-party service providers, including vendors) in the supply chain.

Supply chain risks increase when supply chain partners are unstable financially or during times of economic, cyber, or logistical disruption to the operations and continuity of key supply chain elements.¹⁵⁰ These partners include third parties and their supply chain partners (also referred to as fourth parties). Some supply chain attackers use indirect paths and trusted relationships to gain access to the entity for disruptive purposes, financial gain, or to obtain intelligence. Attackers often exploit a third-party service provider’s supply chain to access multiple other victim businesses (i.e., the service provider’s customers) for subsequent attacks.

IV.Q.1 Supply Chain Risk Management

SCRM is the systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplier’s product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).¹⁵¹ SCRM builds on traditional acquisition and procurement practices by adding processes to identify, measure, monitor, and control risks throughout the supply chain. SCRM processes provide entity management with information to help supplement third-party risk management activities (e.g., due diligence and contract negotiation) and procurement of systems or components by presenting all elements in the supply chain for evaluation.

¹⁴⁸ Per the U.S. Department of the Treasury’s Office of Foreign Assets Control’s (OFAC) “[Basic Information on OFAC and Sanctions](#),” “U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S.-origin goods to comply.”

¹⁴⁹ Refer to [Interagency Guidance on Third-Party Relationships: Risk Management](#).

¹⁵⁰ Refer to NIST IR 8419, [Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives](#).

¹⁵¹ Refer to [NIST Glossary](#).

Management should monitor, control, and protect communications (i.e., information transmitted or received) applicable to supply chain-related activities at key access points (e.g., external boundaries and key internal boundaries). Effective management uses architectural designs, software development techniques, and systems engineering principles to promote effective information security in the supply chain by identifying and mitigating potential SCRM-related risk.

An attempt should be made to identify potential single points of failure among all entities in the entity's supply chain due to the numerous interconnectivities and risks from all partners. Review of documents, such as system and network topologies and process flow diagrams, may help with identification of these single points of failure.

NIST identifies SCRM high-level controls in various documents.¹⁵² Management should consider the following controls in all development, acquisition, and maintenance activities.

- **SCRM policies, standards, and procedures** that
 - Align with other internal and external policies, standards, and procedures (e.g., information security and business continuity management).
 - Instruct staff on how to choose hardware, software, and third-party service providers from an SCRM perspective.
 - Address system and component supply chain traceability.
 - Specify supply chain due diligence for new vendors, third-party service providers, and ongoing supply chain monitoring. The initial assessment should occur during the initiation phase of a project, before new products or services are provided, or new contracts are signed. Due diligence activities should include at least identification and understanding of the criticality of supported function(s), its critical components, and the sensitivity of the information that may be accessible by the supplied system, component, or third party.
 - Identify security standards (e.g., percentage of open-source components allowed and access requirements) for purchased products and supply chain partners. It is important for management to consider starting with applicable, established national and international standards as a baseline for security requirements for the entity's supply chain.
 - Specify information protection processes including what data may be shared, the sharing method, and to whom information is shared (the specific roles). Processes should account for appropriate privacy protections and any dissemination prohibitions, safekeeping, and clearance (e.g., security and access control) requirements.
 - Detail information retention and disposal requirements, especially when sensitive and proprietary information of a supply chain partner is concerned.
- **SCRM plan** contains steps to assess, monitor, and respond to risks associated with supply chain interaction and procurement activities. The plan describes entity and supply chain implementations, requirements, constraints, and implications at the system level. The SCRM

¹⁵² Refer to NIST SP 800-53, rev. 5, [Security and Privacy Controls for Information Systems and Organizations](#), and NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

plan can be stand-alone but is often part of an entity's information security program and third-party risk management program. The plan should address supply chain risks associated with geographic location (e.g., defining acceptable locations). The entity should define roles and responsibilities for personnel (e.g., development, acquisition, and maintenance) to address various risks associated with supply chain activities.

- **General controls and processes** are based on the SCRM plan and entity risk assessments. Management analyzes the risks and designs controls to mitigate risks to an acceptable level as defined by entity senior management and the board. To promote confidentiality, integrity, availability, and resilience throughout the supply chain, controls and processes should include development, information security (e.g., access control and other relevant laws and regulations),¹⁵³ procurement, supplier diversity,¹⁵⁴ and contractual provisions (e.g., clauses stating that contractual requirements apply to any subcontractors). Management should provide the following:
 - Appropriate protections in the information systems, components, and networks for data in transit and at rest for the supply chain partners' information, such as source code testing data, blueprints, and intellectual property.
 - Tamper-resistance and detection controls for critical components.¹⁵⁵
 - Appropriate logging, disparate data correlation, and alerting controls (e.g., access logs, usage pattern reports, and time of day access reports) to obtain evidence in the event of a supply chain compromise.
 - Appropriately segregated and isolated environments between the entity and its supply chain partners to minimize the effect of information leakage across IT environments (e.g., development, testing, and production).
 - Controls over the use of security assessment and monitoring tools within and between IT environments.
 - Logical and physical access controls, such as identification and authentication (e.g., out-of-band validation) for user access to systems and components throughout the supply chain, providing for timely update and periodic review.
 - Current access and authentication lists and appropriate controls to minimize the potential for insider threats as entities develop and acquire systems and components.
 - Formal process for assigning identifiers (e.g., names, numbers, and blockchain) to systems and components (e.g., digital and physical) for management and control throughout the supply chain.
 - Provisions for physical and logical resilience and appropriate implementation of controls in the entity's agreements with supply chain partners.
 - Appropriate monitoring tools and processes at the boundaries between the entity's systems and supply chain partners' systems.

¹⁵³ Refer to FTC 16 CFR 314, "[Standards for Safeguarding Customer Information](#)."

¹⁵⁴ Management should consider supplier diversity for resilience purposes. If only one supplier is relied upon for products or services and is unable to provide them, business could be interrupted; therefore, additional suppliers should be considered. Conversely, too many suppliers may be difficult to manage, and confidentiality, availability, and integrity or quality of service may be compromised.

¹⁵⁵ Criticality analysis can help determine which components are critical.

- **Inventory** is a foundational building block for supply chain management. The entity may rely on third parties to support its strategy and operational functions. Management should develop, document, and maintain an accurate inventory of third parties that reflects the entity's key supply chain partners. Management determines the third party's criticality based on the systems and components the supplier's products and services support and the entity's level of dependency on the supplier for business function. The inventory should be detailed enough for identifying criticality and supply chain risk for tracking and reporting. The inventory should be periodically reviewed and updated, including
 - Description of the supplied products and services (e.g., model or software version).
 - Programs, projects, systems, and components that use the supplier's products and services (i.e., interconnectivities).
 - Assigned criticality level that aligns to the criticality of the program, project, system, component, or service.
- **Configuration management** allows management to track changes made throughout the SDLC to systems, components, and documentation, which is important for tracking details of changes made (e.g., what changes were made, who made them, and who authorized them). Configuration management processes help identify evidence (e.g., baselines and authorizations) used for investigations of potential supply chain cybersecurity compromise. Configuration management is critical to the entity's ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. It is important to consider configuration management minimum security requirements for the supply chain. Management should apply appropriate configuration management controls to its own systems and encourage or require the use of comparable controls by all parties in the entity's supply chain through contracts. For more information, refer to the *FFIEC IT Handbook's* "[Information Security](#)" booklet.
- **Resilience** should be considered from the beginning of the SDLC and maintained throughout the useful life of the system or component. This aids in cost reduction and efficiency of implementation and includes planning for alternative third-party service providers and vendors of systems, components, and services. Another resilience consideration is alternative delivery routes if the primary one is unavailable, especially when it applies to a critical provider. Management can improve resilience by using platform-agnostic systems and components that allow for portability that will improve resilience throughout the supply chain. Having multiple third-party sources (i.e., heterogeneity)¹⁵⁶ for supply of systems and components can result in alternatives for availability and reduce the potential impact of a supply chain compromise. In those situations, an alternative source of supply allows an entity to more rapidly switch to an alternative system or component that may not be affected. Additionally, having heterogeneous components may help decrease the attack surface and impact of a compromise. This is because all systems and components are not alike; therefore, while they may be exposed to similar risks, they may not be exposed to identical vulnerabilities. Additionally, many risk mitigation solutions used for contingency planning (e.g., alternative storage and processing sites and telecommunication pathways) may have their own supply chains with additional risks. Entity management should understand and mitigate all relevant risks associated with interdependencies throughout the various supply

¹⁵⁶ Heterogeneity techniques include the use of distributed storage and processing, different Oss, virtualization techniques, and multiple sources of supply.

chains potentially affecting the entity. Management should plan for certain scenarios, including

- Unplanned system or component failure and subsequent replacement.
- Planned replacement related to feature improvements, maintenance, upgrades, and modernization.
- Product or service disruption (e.g., loss or degradation of data or operations).

Potential supply chain disruptions affect the entity's operations (e.g., transportation issues, system and component availability problems, or financial difficulties of entities in the supply chain). Management should consider provisions for excess capacity, bandwidth, and redundancy in agreements with supply chain partners and take appropriate mitigation steps, as necessary. For more information, refer to the *FFIEC IT Handbook's* "[Business Continuity Management](#)" booklet.

- **Provenance** involves the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. Provenance may include personnel and processes used to interact with or make modifications to the system, component, or associated data.¹⁵⁷ Effective management documents provenance for systems, components, and data, and monitors for changes in the chain of custody that may increase risk to the entity throughout the SDLC. Management should consider producing software bills of material (SBOM)¹⁵⁸ for applicable and appropriate classes of software (e.g., purchased, open-source, and in-house developed software). SBOMs should be digitally signed using a verifiable and trusted key, enabling entities to establish provenance. For more information on SBOMs, refer to the "[Software Bill of Material](#)" section of this booklet.
- **Supply chain partner assessments and reviews** should be part of the entity's third-party and supply chain risk management processes, as appropriate. SCRM assessments should include the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information systems or components traversing the supply chain and should align with enterprise risk management processes and governance. As part of the risk assessment, the entity should have an accurate inventory of suppliers that identifies their criticality to the business. It is important for entity personnel to consider any information pertinent to the security, integrity, resilience, quality, trustworthiness (e.g., not on the OFAC list), or authenticity of their supply chain partners and products. Management should consistently evaluate supply chain partners consistent with the specific context and purpose for which the assessment is being conducted, selecting additional factors for consideration based on supply chain risk. The quality of information (e.g., its relevance, completeness, and accuracy) relied on for an assessment is an important consideration; therefore, management should document the reference sources.

If an entity has a PMO, it can help define requirements, methods, and tools for supply chain partner assessments. Irrespective of the entity's project management methodology, effective project management processes can help identify critical components, especially those that are

¹⁵⁷ Refer to [NIST Glossary](#).

¹⁵⁸ NIST Glossary defines "[SBOM](#)" as a "formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open-source and commercial software components. The SBOM [lists] these components [for a given] product."

used by multiple business lines, functions, systems, and components. For example, effective management considers the following practices:

- Determine whether there is potential foreign ownership or influence and whether the supply chain partner may have relationships with OFAC-sanctioned individuals, organizations, or countries.
- Evaluate supply chain partner oversight of its subcontractors (i.e., fourth parties) or developers.
- Identify the level of open-source systems and components used by the entity, and determine how the supply chain partner demonstrates its compliance with applicable open-source licensing agreements.
- Conduct research on COTS systems and components (e.g., via publicly available resources) or request proof to determine whether the supply chain partner (e.g., original equipment manufacturer [OEM]) has performed testing as part of their quality or security processes.
- Use authorized resellers or distributors with an ongoing relationship with the supply chain partner for systems and components not directly acquired from an OEM entity.
- Acquire directly from vetted OEMs or their authorized distributors and resellers when obtaining alternative sources for continued support. Decisions about using alternative sources (i.e., other than OEMs or authorized resellers and servicers) should consider input from all stakeholders (e.g., business lines, IT, CISO, and compliance).
- Track chain of custody of systems, components, and underlying code as they move throughout the supply chain to minimize the potential for counterfeit or altered products. Use of mechanisms, such as radio frequency identification (RFID), digital signatures, bar code scanning, or blockchain to employ supply chain protection techniques in the acquisition, development, and use of code may be deployed throughout the entity to facilitate tracking chain of custody. These techniques include ensuring that¹⁵⁹
 - Code (including mobile code) originates from vetted sources when acquired.
 - Vetted system and component integrators are used for the development of custom code before installing.
 - Verification processes are in place for acceptance criteria before installation to verify the source and integrity of code.
- **Audit and assurance (internal)** to validate management's assessment of risks in the supply chain, including activities to assess an entity's supply chain partners. Internal audit and assurance activities may include the following:
 - Review of system or component documentation.
 - Review of processes for tracking reports to measure adherence to SLAs.
 - Use of service provider system and organization control (SOC) reports and other independent review reports to validate that supply chain partners meet the entity's minimum standards and implement timely corrective actions for identified deficiencies.

¹⁵⁹ Refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

- Verification of suppliers' claims of conformance to contractual security and compliance requirements.
- Validation of system or component integrity.
- Use of validation tools and techniques (e.g., scanning) for detecting malware or counterfeit goods (e.g., unauthorized systems or components sold as authentic goods). Additionally, management may use manual inspection techniques for identifying genuine components.
- Verification of ongoing training to ensure that appropriate personnel are aware of emerging supply chain risks.
- **Supply chain operational security** is important because of the interconnectedness of numerous relationships with supply chain partners and the difficulty in coordinating multiple operational security efforts, which creates the opportunity for a potential breach. Effective management communicates with its supply chain partners to promote awareness of threat intelligence and relevant vulnerabilities in the entity's supply chain to inform operational security processes. In some situations, entity management may choose to withhold information from supply chain partners to prevent parties with malicious intent from using the information to compromise the entity. To protect against compromise,
 - Management should consider employing techniques to introduce randomness¹⁶⁰ into entity operations and assets in the entity's systems or networks.
 - Management should consider concealment techniques, such as masking metadata that may be accessible in downloads or deliveries of systems and components, whether developed or acquired.
 - If management considers advanced security protection techniques (e.g., misdirection, honeypots) beyond standard industry techniques (e.g., basic randomness and concealment), it should discuss these techniques with the entity's legal counsel and board, as appropriate, before implementation, as they may present liability and additional risk to the entity.
- **Agreements**¹⁶¹ between the entity and its supply chain partners should include provisions addressing common supply chain risks, including their applicability to any subcontractors. Agreements should address risks, including the following:
 - Personnel¹⁶² security controls (e.g., background checks and screening, termination and transfer procedures, and consequences of insider threats) for individuals with access to the entity's supply chain.

¹⁶⁰ For purposes of this discussion, randomness includes randomly switching among several delivery enterprises or routes or changing the time and date of receiving supplier software updates if previously predictably scheduled. For more information, refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

¹⁶¹ Agreements may include contracts, contract addendums, service level agreements (SLA), and operating agreements.

¹⁶² Supply chain-related personnel, whether internal or third-party, may include acquisition and contracting professionals, program managers, supply chain and logistics professionals, shipping and receiving staff, IT professionals, business owners, system owners, and information security engineers.

- Off-boarding procedures to maintain security of entity or supply chain partner information at the close of a contract or end of service to prevent the misuse of sensitive entity or customer information. Agreements should address relationship termination to facilitate a secure off-boarding process (e.g., removing data from cloud environments).
- Most recent set of applicable security and functionality requirements as a baseline, with provisions for future enhancement as risk mitigation needs dictate.
- Processes to monitor and track the vulnerability of the supply chain, based on the criticality or risk profile of the supply chain partner, system, component, or service. A system, component, and service inventory may help management to identify assets that may be subject to known vulnerabilities. This may provide a starting point for determining the level of vulnerability monitoring needed for systems, components, and services throughout the entity's supply chain.
- Information sharing (e.g., collection, analysis, and distribution) of threat intelligence, incidents, and other key risk indicators throughout the supply chain. The intelligence gathered enables management to proactively identify and respond to threats in the entity's supply chain. Therefore, management should consider information-sharing clauses in agreements and contracts.
- Procedures and responsibilities of supply chain partners when actionable (i.e., management needs to take action to mitigate the risk in some way) information is learned, indicating that a supply chain partner or a system, component, or service is a target of a specific threat.
- Provisions for boundary (e.g., network perimeters) protections, which should be incorporated into agreements with supply chain partners, when applicable. This should address initial implementation of boundary control requirements for interconnected networks in the supply chain.
- Inclusion of protections (e.g., encryption) for sensitive information at rest or in transit, applicable throughout the supply chain. This is a consideration for assessing compliance with Gramm–Leach–Bliley Act (GLBA) provisions.
- **Incident response** agreements should include the entity's notification requirements for imminent threats (e.g., system, component, service, or supply chain partner may be the target of an attack), incidents, and compromises that may affect the entity.¹⁶³ It is important for management to consider addressing the following incident response-related information in its agreements with its supply chain partners:
 - Definition and triggers of an incident.

¹⁶³ Refer to [Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers](#), referenced in agency guidance FDIC FIL-74-2021, "[Computer-Security Incident Notification Final Rule](#)," and OCC Bulletin 2021-55, "[Computer-Security Incident Notification: Final Rule](#)." Implementation is further discussed in FDIC FIL-12-2022, "[Computer-Security Incident Notification Implementation](#)"; FRB SR Letter 22-4/Consumer Affairs (CA) 22-3, "[Contact Information in Relation to Computer-Security Incident Notification Requirements](#)"; and OCC Bulletin 2022-8, "[Information Technology: OCC Points of Contact for Banks' Computer-Security Incident Notifications](#)."

- Roles and responsibilities, including clear boundaries of responsibility, for incident response processes, including third-party expertise.¹⁶⁴
- Methods and timing of incident communication with regulators and supply chain partners. These should be defined in agreements with supply chain partners to ensure an efficient, coordinated incident response effort (e.g., speed of communication, response, corrective actions, and other related activities).
- Incident response training (e.g., threat briefing or incident response exercises) when appropriate.
- Incident response testing with critical supply chain partners, as appropriate.
- Review of the agreement based on lessons learned after incidents and any new intelligence.
- **Tamper resistance and detection** processes allow entity management to recognize when unauthorized changes to systems and components are made in transit between the supply chain partner and the entity. Entity or supply chain partner personnel should inspect critical systems and components to ensure that tamper-resistant controls are in place and to determine whether there is evidence of tampering. Systems and components should be reviewed for tampering before use and periodically thereafter. Provisions for this type of review should be included in contracts with supply chain partners.
- **System or component authenticity and integrity** is critical for managing cybersecurity risks throughout the supply chain. Without effective SCRM and ITAM processes, it may be possible for entity personnel or third parties to use counterfeit systems and components. This may allow for potential security, functionality, quality, and legal weaknesses (e.g., counterfeit components may void contracts, warranties, or insurance coverage), leading to compromise of confidentiality, integrity, and availability of systems, components, services, and data throughout the supply chain. By deploying effective system and component integrity controls, management can mitigate cybersecurity risks, such as insertion of malicious code and use of counterfeits, throughout the supply chain. Effective controls include anti-counterfeit policies and procedures that protect against introducing counterfeit systems and components into the entity's infrastructure (e.g., ATM processor boards with extra communication chips built into the circuitry, noncertified hardware developers). System and component integrity controls may include the following:
 - System and component integrity policy and procedures, including the use of various integrity verification tools and techniques. These tools and techniques may include the following:
 - Digital signature or checksum verification.
 - Acceptance testing for physical systems and components.
 - Verification testing confined to limited-privilege environments, such as sandboxes.
 - Code execution restrictions in limited-privilege environments before implementation in production.
 - Validation that binary or machine-executable code is obtained directly from the OEM or a verified supplier or distributor.

¹⁶⁴ Roles and responsibilities include identification, determination, escalation, notification, handling, analysis, monitoring and tracking, and provisions for third-party expertise (e.g., forensics).

- Process to communicate with supply chain partners to identify, report, and correct system and component flaws in a timely manner.
- Protection from code threats originating from an unauthorized or malicious source in the supply chain. These protections should be applied throughout the supply chain.
- Monitoring for supply chain system and component security and threat intelligence alerts and advisories from supply chain partners. Effective management takes appropriate actions in response. Monitoring processes should include monitoring that lessons learned from prior compromises are appropriately acted upon. For example, if malicious code implanted during software development leads to a compromise, effective controls are implemented to further ensure code legitimacy in the future. It is important for management to consider
 - Correlation of available threat intelligence information (e.g., internally produced and from supply chain partners) to identify potential threats or vulnerabilities requiring mitigation.
 - Employment of enhanced monitoring over activities performed by higher-risk personnel (e.g., users with elevated authority or privileges).
- Determining periodically whether any counterfeit or shadow IT systems and components exist in the supply chain. Typically, management addresses this issue through contractual provisions with supply chain partners regarding their mitigation program for shadow IT risk. If any are discovered, management should assess the impact of removal, then remove any suspect systems or components from the entity's infrastructure as appropriate.¹⁶⁵
- **Maintenance** includes performing system and component updates and replacements and may be performed by a third party. When performed by a third party, maintenance becomes part of the supply chain and SCRM principles should be applied. Management should perform the following when implementing maintenance processes throughout the supply chain:
 - Define agreements that identify roles, responsibilities, and practices that may be used for maintenance activities, especially when third parties are responsible for maintaining the entity's systems or components.
 - Monitor for unauthorized modification or removal of the entity's systems or components (e.g., use of counterfeit systems, counterfeit components, and malware) in the supply chain. Agreements with supply chain partners should address monitoring and communication to affected parties throughout the supply chain.
 - Monitor systems and components for planning for EOL to prepare for replacement or upgrade to the systems and components. Effective management considers any potential availability issues in the supply chain for systems and components or has agreements to continue support for legacy systems or components until a change can be made without significant disruption to operations.
- **System or component EOL and disposal processes** outline the steps personnel should take when components are nearing EOL and need to be decommissioned and removed from the entity's infrastructure. Standard EOL processes should be followed. Additional processes related to supply chain activities may involve the following:

¹⁶⁵ For more information on shadow IT and IT asset management, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" booklet.

- Inclusion of data disposal processes to allow entity management to mitigate the risk that entity data maintained by supply chain partners may be retained or compromised.
- Consideration of supply chain partner interdependencies associated with the removal of a system or component from the entity's environment, as well as throughout the supply chain. For example, the removal of a supply chain partner's system or component that may disrupt the entity's ability to provide continuous service to customers.
- Sanitization or destruction of information from supply chain partner systems, components, and media before disposal or release for reuse. Agreements should address this for all locations and providers in the supply chain. Off-boarding procedures should be addressed in agreements to maintain data confidentiality, integrity, and availability until the relationship with that supply chain partner is officially terminated.
- Application of data protection controls (e.g., tracking chain of custody) throughout off-boarding processes for an entity's data and for the data received from supply chain partners.

Additionally, as a part of SCRM, entity management should consider interconnectivity risks throughout the supply chain. What may initially be assessed as a low-risk activity or asset may be considered a high-risk activity or asset based on the interconnectivity or reliance on that system or component. For example, a system or component (e.g., HVAC, smart TVs, and IoT devices) may not appear high-risk, yet the system or component may be connected to critical systems and components throughout the supply chain, and subject to remote access risks. Therefore, management should have a process to validate the effectiveness of the security of systems and components throughout the supply chain when performing development, acquisition, and maintenance activities, and make appropriate adjustments to risk assessments to account for interconnectivity risk.

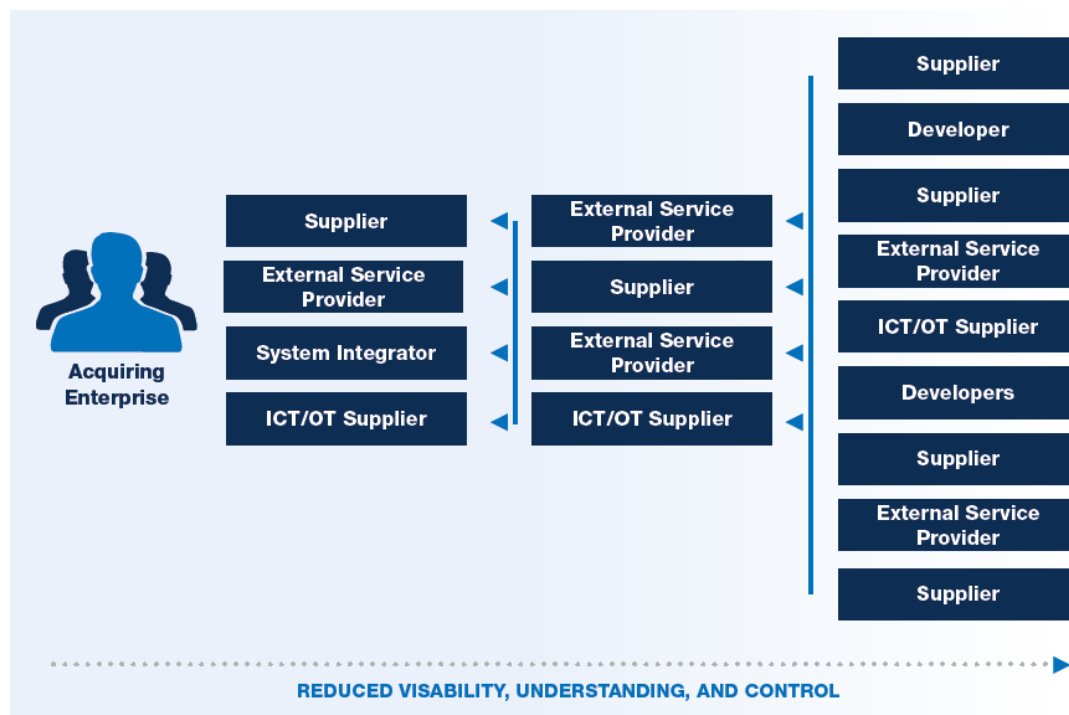
To effectively manage supply chain risks, management should have a clear understanding of interconnectivity in the entity's supply chain. To facilitate this understanding, management should consider using available information, such as that provided by third-party user groups and associations,¹⁶⁶ which can augment ongoing monitoring and due diligence, threat intelligence, and security throughout the supply chain. A vulnerability to one system, component, or supply chain partner may pose a vulnerability to the entire supply chain. Figure 5 depicts diverse supply chain relationships that affect an entity's visibility and control of the supply chain. Entities depend on the supply chain to provide a variety of products and services to enable the enterprise to achieve its strategic and operational objectives. As NIST states, acquirers often lack visibility and understanding of how acquired technology is developed, integrated, and deployed and how the services that they acquire are delivered. Additionally, acquirers with inadequate or absent SCRM processes and practices may experience increased exposure to cybersecurity risks throughout the supply chain. The level of exposure to cybersecurity risks throughout the supply chain depends largely on the relationship between the products and services provided and the

¹⁶⁶ Associations may include standards-setting organizations, such as the National Automated Clearinghouse Association ([Nacha](#)), and [PCI Security Standards Council](#) (for the payment card industry) and information-sharing organizations (e.g., [Financial Services Information Sharing and Analysis Center \[FS-ISAC\]](#), and other information-sharing and analysis centers [[ISAC](#)]).

criticality of the missions, business processes, and systems they support.¹⁶⁷ Entities have a variety of relationships with their suppliers, developers, system integrators, external system service providers, and other information communication and technology/operational technology-related¹⁶⁸ service providers.¹⁶⁹

Effective management considers risk management factors over the entire life cycle of a third-party relationship, including planning, due diligence, contract negotiation, ongoing monitoring, and termination. For more information on these factors, refer to the *FFIEC IT Handbook's* “[Outsourcing Technology Services](#)” and “[Management](#)” booklets. Additionally, for more information on supply chain relationships, refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

Figure 5: Supply Chain Relationships



¹⁶⁷ Refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#), for more information.

¹⁶⁸ NIST Glossary defines “[information and communication technology](#)” as “encompassing the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.” It defines “[operational technology](#)” as “programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).”

¹⁶⁹ Refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

IV.Q.2 Software Bill of Material

An SBOM is a formal record containing the details and supply chain relationships of various components used in building software.¹⁷⁰ “A primary purpose of an SBOM is to identify components and their relationships to one another, using some combination of baseline component information.”¹⁷¹ There are benefits to supply chain partners including developers, purchasers, and operators of software. An SBOM can help developers of systems and components be aware of any software they might use in development of entity solutions. For purchasers, an SBOM helps identify software supporting a product potentially subject to compatibility issues. An SBOM enables an entity and its operators to determine in a relatively short time whether the entity is affected by a vulnerability and where in the supply chain the entity may have been affected¹⁷² because management can match vulnerabilities to elements in the SBOM.

Management may use an SBOM to identify what systems and components fall outside the entity’s risk tolerance thresholds (e.g., has a significant vulnerability, inappropriate use of open-source components, or is linked to an untrusted provider). An SBOM may help with the management of OEM licensing and compliance and enable management to quickly identify interdependencies and other supply chain risks. An SBOM gives management visibility into systems and components used in the entity’s infrastructure, including open-source systems and components and IoT products.¹⁷³ This visibility allows management to perform activities such as the following:

- Determine whether any of the software or components used in the entity’s infrastructure are subject to specific vulnerabilities or potential risks associated with publicized breaches, as determined through entity threat intelligence processes.
- Uniquely identify systems and components used by customers and authorized entities.
- Trace users and the use of licenses, allowing management to determine whether access control information is accurate and whether its use is appropriate.

Tools used to read an SBOM should “uniquely identify individual components in a standard format,”¹⁷⁴ so that all references are uniform throughout the supply chain. Additionally, an SBOM should be updated whenever software elements are changed or software is updated.

¹⁷⁰ Refer to [NIST Glossary](#).

¹⁷¹ Refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

¹⁷² Refer to National Telecommunications and Information Administration (NTIA), [Framing Software Component Transparency: Establishing a Common Software Bill of Materials \(SBOM\)](#) and “[SBOM Myths vs. Facts](#).”

¹⁷³ For more information, refer to NIST IR 8425, [Profile of the IoT Core Baseline for Consumer IoT Products](#), and NIST IR 8259A, [IoT Device Cybersecurity Capability Core Baseline](#).

¹⁷⁴ Refer to NTIA’s [Framing Software Component Transparency: Establishing a Common Software Bill of Materials \(SBOM\)](#) and “[SBOM at a Glance](#).”

SBOMs typically do not identify intellectual property, patents, algorithms, or code; if they do, management should implement appropriate security for this proprietary information.

NIST states that as SBOMs mature, management should help ensure that they do not deprioritize existing SCRM capabilities (e.g., vulnerability management practices and vendor risk assessments) under the mistaken assumption that SBOMs replace these activities. Accurate SBOMs are meant to provide improved transparency, which is complementary to an entity's risk management practices, not a substitute for them. "Entities that are unable to appropriately ingest (i.e., recognize and understand), analyze, and act on the data that SBOMs provide likely will not improve their overall SCRM posture."¹⁷⁵

IV.Q.3 Enterprise Risk Management and Supply Chain Risks

SCRM touches on risk management activities across the entity and should be incorporated into enterprise and technology risk management activities. A few examples of security elements tied to SCRM include the following:

- **Confidentiality:** Supply chain partners may receive sensitive entity and customer information.
- **Integrity:** Systems or components may not operate as designed, leading to a data integrity issue, or third parties may intentionally or unintentionally change entity, partner, customer, or consumer data.
- **Availability and resilience:** Systems, components, or services may not be available or recoverable when needed.

According to NIST, "Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders."¹⁷⁶ Supply chain activities occur throughout the SDLC; therefore, SCRM should be embedded throughout the SDLC.¹⁷⁷ Additionally, when applicable, management should incorporate third parties into business continuity and resilience activities throughout the supply chain.

¹⁷⁵ Refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

¹⁷⁶ Refer to NIST 800-53, rev. 5, [Security and Privacy Controls for Information Systems and Operations](#).

¹⁷⁷ Refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#).

V DEVELOPMENT

Action Summary

Implementation of sound processes for the development of systems and components supporting the entity's business needs and operations is important.

Examiners should review the following:

- Documentation of training in secure design and coding techniques for those entity personnel who are responsible for development.
- Development standards, including procedures for managing changes and a back-out plan.
- Evidence of communication throughout the supply chain regarding identification of critical systems and components, potential threats and vulnerabilities, configurations, and responsibilities for selection and maintenance of system and network components.
- Entity coding standards and list of entity-approved software development languages.
- Documentation of security certification for completed systems and component-related code.
- Development designs used to validate security and functionality throughout the supply chain.
- Risk assessment documentation related to the use of or switch to a development operations (DevOps) approach, or extending to a development security operations (DevSecOps) approach, and effectiveness of controls.

Development is the systematic application of knowledge toward the production of useful materials, devices, and systems. In this context, it involves the processes of defining, designing, developing, testing, and implementing systems or components. Development includes validation and demonstration of a chosen technology, use of test and production environments, improvement of developed prototypes, integration into systems and subsystems, and hardware builds. Understanding development concepts is important to all entities whether development is performed in-house or by a third party on the entity's behalf. Additionally, development can be a complex topic, which requires the entity's board, senior management, and business line management to understand risks and communicate effectively. For entities that develop or modify their own systems and software, effective management requires training in secure design and coding techniques of those responsible for development. If formal standards are not in place and development processes are not controlled, the following can occur, affecting confidentiality, integrity, availability, and resilience:

- Corruption (e.g., malware or sabotage) of the development process.
- Unintentional creation of vulnerabilities (e.g., backdoors or open ports).
- Omission or errors in process or code (e.g., intended processes that were forgotten or calculations that are incorrect) resulting in production issues (e.g., disruptions or delays).

Entity personnel should maintain and follow documented development policies, standards, and procedures that result in systems and components that meet the entity's requirements for confidentiality, integrity, availability, and resilience. Standards and procedures should identify approved development tools and tool configurations in the development process or in a specific development methodology.

When engaged in development, management may consider using design and coding techniques, appropriate tools (e.g., computer-aided design), and prototypes. When development personnel use design and coding techniques, they should appropriately manage risks (e.g., eliminating inaccurate techniques or outdated tools and prototypes). Prototypes may help illustrate a system's or component's functionality to stakeholders and help management identify, evaluate, and highlight design risks not apparent during the impact analysis or before production. Then the design risks may be resolved more efficiently. There are alternatives to prototyping, such as defining and building a system or component with only enough features to accomplish the essential user objectives of the system.

As part of the SDLC, effective management works toward developing a trustworthy system. From a security perspective, a trustworthy system¹⁷⁸ meets specific security requirements and other critical requirements defined and set by entity management. To help develop a trustworthy system, management should employ secure program coding practices. Secure coding practices help developers minimize the potential for known source code-related vulnerabilities in the development phase.

Examples of secure coding practices include the following:¹⁷⁹

- Validate all inputs and validate and properly encode all outputs.
- Avoid using unsafe functions.
- Detect and correct errors effectively.
- Provide logging and tracing capabilities.
- Consider use of automated features that encourage secure coding practices in development environments, when appropriate.
- Establish procedures for manually applying secure coding practices when automated methods are insufficient or unavailable.
- Use tools (e.g., linters¹⁸⁰ or formatters) to analyze code, identify common mistakes and bad coding style, and standardize the style and formatting of the source code.
- Check for common system, code, and development environment vulnerabilities.
- Assign developers to review code to complement (not replace) independent code review and verify compliance with security requirements.

¹⁷⁸ Refer to NIST SP 800-160, vol. 1, rev. 1, [Engineering Trustworthy Secure Systems](#).

¹⁷⁹ Refer to NIST SP 800-218, [Secure Software Development Framework \(SSDF\) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities](#).

¹⁸⁰ For purposes of this booklet, a "linter" is a type of tool used to perform code analysis to flag issues, such as programming errors, bugs, and stylistic errors.

- Identify and correct vulnerabilities before release of software to production to prevent exploitation.

Developers should communicate throughout the supply chain to ensure that partners are aware of potential threats and vulnerabilities when developing, testing, and maintaining systems and components. Additionally, the individuals responsible for selecting system and network components should incorporate supply chain processes when choosing such components. Developer training should include secure coding and the use of tools to find vulnerabilities in systems and components across the supply chain. For more information, refer to the “[Supply Chain Considerations](#)” section of this booklet.

V.B Development Standards and Controls

Management should establish development standards, including procedures for controlling changes during the development process that address the following:

- **System controls**, including a system’s or component’s functionality, security, automated control features, and coding standards.
- **Quality management** (also referred to as quality assurance and quality control [QA/QC]), including the development and implementation of a system or component so it meets predefined specifications and management’s expectations.
- **Release management**, including migration of the final release of systems or components from a development or development testing environment into the production environment for deployment. This may include multiple steps. A release can be completed manually, or the release process could be automated. Established rollback instructions, or back-out plans, should be developed and available in the event of unforeseen deployment problems.
- **Documentation** to facilitate stakeholders’ understanding of the following:
 - Development process.
 - Error correction and program modification processes.
 - System or component business functionality.
- **Reporting**, including processes for generating and managing reports (e.g., types of reports, timing, and stakeholders who should receive them) during development to help management make important budgeting and other data-driven decisions. Reports could include project updates, technical issue logs, and change management logs.

Development standards should articulate the entity’s minimum development requirements. For example, development standards may address the selection of programming styles, languages, and tools; layout or format of scripted code; naming conventions; and program library requirements. Effective management communicates in policy its reasons for using specific programming styles and languages on a project or service in project documentation. This is done to identify decisions made by management so developers can understand the reasons certain programming styles and languages were used and whether they remain appropriate for current functionality and stakeholder needs. Examples are included in table 3.

Table 3: Descriptions and Reasons for Using Programming Styles and Example Languages

Programming style	Description	Why	Example languages ¹⁸¹
Compiled	Source code converted into machine language before the code can operate	- Useful when resources are limited and execution speed (for transactions) is essential. - Less portable than hybrid or interpreted languages due to the need to recompile for each new system.	C, C++, GO, Swift, Objective-C, Visual Basic
Hybrid (compiled and interpreted)	Uses a combination of compiled and interpreted languages programming style	- Portable and slower than compiled. - Requires more resources (e.g., CPU and random access memory [RAM]) than compiled, but less than interpreted language.	Java, C#, Clojure, Scala, Spark, Prolog
Interpreted ¹⁸²	Lines of code that can operate without first being compiled	- Less complex than compiled or hybrid programming styles, but requires more resources (e.g., CPU and RAM). - Easier to find trained developers, as less technical knowledge is needed to implement the code.	Python, JavaScript, PowerShell, PHP, Structured Query Language (SQL), Ruby, Perl, Lua, Delphi
Assembler	Converts assembly instructions into machine language	- Useful when you need to minimize resources (e.g., CPU and RAM) needed to implement the code. - Often used for firmware.	Assembly
Markup language	Language with rules and instructions accompanying the code, which facilitates use by humans and programs	Useful when text needs to be formatted in a specific way (e.g., font, color, and size).	HTML, XML, SGML
Legacy	Older programming languages that potentially are unsupported, general use is declining	- Personnel with knowledge of code development and use is declining, making it difficult to maintain and upgrade. - Concerns related to programming style in sunset phase of SDLC.	FORTRAN, COBOL, APL, ALGOL, LISP, PASCAL, Assembly, REXX, JCL

The use of naming conventions¹⁸³ for a software program’s modules and any related subroutines, databases, or programs that interact with an application help a team of developers work more efficiently together. For example, naming convention use promotes consistency so programmers can link subroutines into a unified program more efficiently. Naming conventions also facilitate understanding so IT staff not involved in the original development can later modify systems

¹⁸¹ Languages may be applicable in several different language styles; these are just examples.

¹⁸² An interpreted programming style refers to processing a script or other program expressions line by line and in accordance with the language requirements, without first compiling a program into machine instructions.

¹⁸³ NIST defines a “[naming convention](#)” as “a collection of rules, which when applied to data, results in a set of data elements named in a logical and standardized way. These names inform the user about the contents of the data value domain, and the usage of the data element, in a concise manner.”

efficiently. Finally, use of naming conventions often facilitates software code reuse and repurposing.

To establish development standards and controls, prudent practices include thorough development testing and validation of systems and component-related code. Effective management keeps completed systems and component-related code that have passed security certification in program libraries as discussed in the “[Additional Control Considerations in Change Management](#)” section of this booklet.

Due to supply chain risk in development, for both in-house and supply chain partners, it is important to consider using the following standards and controls when developing information systems and components:

- Design security controls to be difficult to disable (e.g., tamper-proofing techniques), and, if they are disabled, trigger notification methods such as audit trails, tamper evidence, or alarms.
- Design delivery mechanisms (e.g., downloads for software) to avoid unnecessary exposure or access to the supply chain and systems or components traversing the supply chain.
- Design relevant validation mechanisms to be used during implementation and operation.

Developer configuration management is critical for reducing cybersecurity risks, both in-house and throughout the supply chain. Developers should manage the configurations of the development environments in which they are working. They should create configuration guides for the systems and components they are developing for distribution with the system or component. By implementing configuration management standards and controls, developers reduce the occurrence and likelihood of flaws while increasing accountability and ownership for the changes. Developer configuration management should be performed by developers, including any third parties involved in the process.

If management decides, based on assessments of risk throughout the supply chain, that customized development of certain critical systems and components is necessary, then it should have agreement on standards and controls used in customized system and component development throughout the supply chain. Whether developed in-house or by a supply chain partner, additional scrutiny should be applied when custom development of systems and components occurs to ensure proper configuration to meet business and information security needs. Management should work with suppliers and partners to ensure that critical systems and components are identified. Effective management helps ensure that suppliers or the entity itself has a continued ability to maintain customized systems and components that are critical to the entity’s operations. For example, having the source code, build scripts, and tests for a software component could enable an entity to have a third party maintain the system or component if necessary. For more information, refer to the “[Escrowed Source Code Agreements and Documentation](#)” section of this booklet.

V.C Testing

Action Summary

Management should maintain testing policies, standards, procedures, as well as other process controls that are effectively used to mitigate risks in internally and externally developed systems and components.

Examiners should review the following:

- Testing policies, standards, and procedures, as well as other process controls, to evaluate how well entity personnel use testing to confirm that systems and components meet the entity's requirements.
- Testing scope documentation, including for application interoperability and vulnerability discovery.
- Documentation regarding controls over the use of production data in testing.
- Documentation of the type of testing, testing results, corrective actions, and testing completion.
- Documentation of testing for any new controls added to systems and components to avoid conflicts (e.g., integration and interface, security) resulting in failed business processes.
- Any updates to manuals and training plans after testing.

Testing is essential to the development process to promote confidentiality, integrity, availability, and resilience. Whether developed internally or by a third party, appropriate personnel should test systems and components to identify and correct defects before deployment, including security-related defects.

Testing should be sufficient to confirm that systems and components meet the entity's architectural, functional, information security, and legal/regulatory requirements. To help mitigate the risk that an integration point contains an undiscovered defect, entities test the system or component being developed, including how well that system or component interoperates with other systems and components. This scope is commonly achieved through a combination of code-level, system-level, and code vulnerability testing.

Starting test plans no later than the development and acquisition phase helps teams test more comprehensively than if they wait to create test plans later in the SDLC. Additionally, the level of detail in the test plan and script should match the level of risk the system or component presents to the examined entity's business. The more detailed test plans and scripts are, the higher the likelihood that testers will identify defects before system or component implementation.

Using production data in testing may provide assurance that the system or component functions as expected; however, there are significant risks (e.g., unauthorized access to or modification of sensitive entity or customer information). Management should determine the need for using

production data in testing and employ appropriate controls if its use is deemed necessary. When possible, testers should use simulated synthetic data or sanitized¹⁸⁴ production data during system or component development and testing¹⁸⁵ to protect sensitive customer and entity data. Data used for testing should not include sensitive customer information unless the data are sanitized¹⁸⁶ before testing, and this should be addressed in policy. Due to the risks involved with actual customer data, when sanitizing data is not feasible, management should document an exception to board-approved policy for its use. Implementation and maintenance of controls similar to those used in the production environment should be used to appropriately protect the data for compliance with legal and regulatory requirements. The Information Security Standards require safeguarding of sensitive customer information regardless of the environment (e.g., testing, QA, or production) where the information resides.¹⁸⁷ For more information, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" and "[Information Security](#)" booklets.

The types of testing¹⁸⁸ performed should be appropriate for the development activity's inherent risk. Effective management has a methodical process to define and conduct testing necessary to demonstrate the effectiveness of a developed system or component. Typically, testing is performed in stages, and knowledgeable testing specialists and relevant stakeholders should be involved in testing. Regardless of the process, various tests may be used individually or in combination at different points in the development and testing phases. During system or component development, developers perform code reviews, which typically occur as part of the testing process. Appropriate personnel can perform testing manually, with automated tools, or a combination of both.

¹⁸⁴ Data sanitization disguises (i.e., anonymizes) sensitive information in test and development databases by overwriting the information with realistic looking but false data of a similar type. Some forms of sanitization include NULLing out, masking data, substitution, shuffling records, and encryption. For more information, refer to NIST SP 800-160, vol. 1, rev. 1, [Engineering Trustworthy Secure Systems](#).

¹⁸⁵ Refer to NIST SP 800-160, vol. 1, rev. 1, [Engineering Trustworthy Secure Systems](#).

¹⁸⁶ Data sanitization can help minimize risks related to unauthorized access of that data. Unsanitized data passed to other systems or subsystems (e.g., command shells, relational databases, and commercial off-the-shelf [COTS] components) may be vulnerable. Attackers may be able to exploit unused functionality to access, manipulate, or exfiltrate the data causing legal and operational risk to the entity. Additionally, that data may provide information to attackers, allowing for unauthorized lateral movement throughout the network, systems, and components.

¹⁸⁷ Refer to [GLBA](#), further implemented by FFIEC members as follows: FDIC: 12 CFR 364, appendix B, "[Interagency Guidelines Establishing Information Security Standards](#)," and 12 CFR 364, supplement A to appendix B, "[Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#)"; FRB: Regulation H, 12 CFR 208, appendix D-2, "[Interagency Guidelines Establishing Information Security Standards](#)," and Regulation Y, 12 CFR 225, appendix F, "[Interagency Guidelines Establishing Information Security Standards](#)"; NCUA: 12 CFR 748, appendix A, "[Guidelines for Safeguarding Member Information](#)," OCC: 12 CFR 30, appendix B, "[Interagency Guidelines Establishing Information Security Standards](#)." Additionally, refer to FTC 16 CFR 314, "[Standards for Safeguarding Customer Information](#)," for similar provisions for service providers.

¹⁸⁸ For purposes of this section, NIST IR 8397, [Guidelines on Minimum Standards for Developer Verification of Software](#), defines "testing" as "any technique or procedure performed on the software itself to gain assurance that the software will perform as desired, has the necessary properties, and has no important vulnerabilities."

While the testing types, such as dynamic testing, may be performed during multiple phases, commonly performed testing in the development and acquisition phase includes the following:

- **Static analysis:** Personnel detect software vulnerabilities by examining the application source code and binary code and attempting to analyze and identify all possible behaviors that might arise at runtime.¹⁸⁹ An example of static analysis is software application security testing, which analyzes the quality of the code.¹⁹⁰
- **Unit testing:**¹⁹¹ Developers perform unit tests to assess the functionality of small modules of code.
- **Security testing:** Developmental testing helps ensure that the technical and security features and functions of the system perform as intended.¹⁹² This may include initial penetration testing of the code.
- **Dynamic analysis:** Personnel use testing that operates by executing a program using a set of input use cases and analyzing the program's runtime behavior. Testing may be extensive (i.e., time-consuming) depending on the number of scenarios analyzed. An example of dynamic, execution-based scans is dynamic application security testing, which is intended to simulate real-world attacks.¹⁹³

The development team should document the results of testing performed. Documentation should include the type of testing performed, scope of the testing, test results, further action based on results of the test (e.g., error correction, patch, or retest), and whether the testing is considered complete. Appropriate personnel can provide a report communicating the test results to management as appropriate.

Commonly performed testing in the implementation and assessment phase includes the following:

- **System testing:** Testing is performed on a complete system to evaluate its compliance with specified requirements.
- **Additional security testing:** If new controls are added to the system, additional acceptance tests of those new controls should be performed to help ensure that new controls meet security specifications and do not conflict with or invalidate existing controls or functionality.
- **Integration testing:** Personnel perform an orderly progression of testing in which software elements, hardware elements, or both are combined and tested to evaluate their interactions,

¹⁸⁹ Refer to NIST 800-163, rev. 1, [Vetting the Security of Mobile Applications](#).

¹⁹⁰ For more information, refer to [OWASP Vulnerability Management Guide \(OVMG\)](#).

¹⁹¹ Information Systems Audit and Control Association (ISACA) Glossary defines "[unit testing](#)" as "a testing technique that is used to test program logic in a particular program or module. The purpose of the test is to ensure that the internal operation of the program performs according to specification. It uses a set of test cases that focus on the control structure of the procedural design."

¹⁹² Refer to NIST ITL Bulletin, "[The System Development Life Cycle](#)."

¹⁹³ For more information, refer to [OWASP Vulnerability Management Guide \(OVMG\)](#).

until the entire system has been integrated.¹⁹⁴ A primary goal of integration testing is to ensure that systems and components function appropriately together. This is especially difficult when software uses components developed by different vendors, in different languages, and the implementation sources are not all available.¹⁹⁵

- **UAT:** Personnel perform testing that involves taking use cases or procedures for how the system was designed to perform and ensuring that someone who follows the procedure gets the intended result; however, it does not necessarily demonstrate how well the system supports users in performing those functions.¹⁹⁶ Therefore, UAT is not used to determine usability. UAT generally occurs toward the end of development testing activities. UAT may be useful for validating procedures and user training on the operation of new or significantly changed systems and components.
- **Regression testing:** Personnel execute testing that involves the performance of the same tests many times to determine whether to return to the prior state. A retest of a system or component helps to assess functionality after programmers make code changes following previous tests. Regression testing generally includes systems that may not have changed but may be affected by a new or changed system or component.
- **Stress testing:** For purposes of this discussion, this refers to testing performed to determine the limitations of a system or component. IT personnel periodically test to determine whether the entity's system or component can handle the anticipated maximum volume or duration of activity while maintaining required functionality. This may be performed using automated testing tools that generate simulated scenarios.

Regardless of the testing methods used, management should implement practices to document, report, and address identified issues, including security-related issues, in a timely manner. Tracking corrections and modifications resulting from testing facilitates the completeness of the overall program documentation. During the implementation and assessment phase, effective management reviews and finalizes all supporting documentation, such as user, operator, and maintenance manuals as well as any conversion, implementation, and training plans associated with a new release or significant update.

V.D DevOps and DevSecOps

DevOps builds on agile principles and is a software engineering culture and set of practices designed to unify software development and operations. DevSecOps takes DevOps one step further by integrating security ("Sec" stands for "security"). The following subsections of this booklet provide more information on DevOps and DevSecOps.

¹⁹⁴ Refer to [ISACA Glossary](#).

¹⁹⁵ For more information, refer to Leonard J. Gallagher and Jeff Offutt, [Test Sequence Generation for Integration Testing of Component Software](#).

¹⁹⁶ Refer to NIST IR 7741, [NIST Guide to the Processes Approach for Improving the Usability of Electronic Health Records](#).

V.D.1 DevOps

DevOps is a “set of practices for automating the processes between software development and information technology operations teams so that they can build, test, and release software faster and more reliably. The goal is to shorten the SDLC and improve reliability while delivering features, fixes, and updates frequently in close alignment with business objectives.”¹⁹⁷ DevOps is used to promote coordination and communication between development and operations teams (e.g., developers, testers, or operations personnel). For example, a group of developers can be embedded with the operations team to acquire domain-specific expertise, allowing them to better understand applicable business processes in a given area of the entity’s systems. The operations team benefits from having developers readily accessible to help operations personnel better understand the entity’s developed applications and IT infrastructure.

Using DevOps practices, personnel can automate tasks that were previously performed manually. For example, a DevOps team can automate configuration management processes (e.g., firewall rules, server hardening, and mobile device management). DevOps practices often include containerization, which allows applications to be implemented as microservices. For more information on containers and microservices, refer to the “[Common Development, Acquisition, and Maintenance Risk Topics](#)” section of this booklet.

Automation and orchestration give the DevOps approach several benefits including shorter development cycles, increased deployment frequency, faster time to market, and more stable operating environments. In the past, entities may have had changes that took place on a weekly basis; however, in a DevOps environment, the same number and type of changes can be made daily or even hourly. However, automation of previously manual activities, combined with frequent and rapid release cycles, may result in perpetuation of errors or invalid code. Management should assess the risks involved in using a DevOps approach and implement appropriate controls. Potential risks include the following:

- Misconfigured process automation (e.g., quality and release management).
- Unclear governance practices, such as inadequate development standards and procedures and a lack of validation of effectiveness.
- Inappropriate metrics or tracking measures.
- Unauthorized code access and modification via unsecured code repositories (e.g., GitHub).
- Lack of cyber hygiene (e.g., inappropriate configurations or unscanned and vulnerable systems are released).
- Developers being able to use uncontrolled and insecure system images.
- Inadequate controls over code implemented in production (e.g., bypassing the entity’s coding standards).

V.D.2 DevSecOps

DevSecOps is the evolutionary progression from DevOps that integrates security objectives and controls (e.g., metrics and compliance reports) into the development process. The main

¹⁹⁷ Refer to NIST SP 1800-16, [Securing Web Transactions: TLS Server Certificate Management](#).

characteristics of this practice are to automate, monitor, and apply security at all phases of the SDLC. Automation of the workflows and integrated security testing is a key attribute of DevSecOps. Additionally, automation of testing (e.g., unit testing, code analysis, and image scanning) provides timely feedback to DevSecOps teams while not obstructing productivity. Cybersecurity and design have the same priority as they would in traditional system and component development. Security resources are integrated at the outset of the development process. DevSecOps is a key approach used in cloud development environments. Cloud-native applications require updates and deployment techniques to be flexible and secure for business reasons, as well as resilient to respond to cybersecurity events.¹⁹⁸

Coding services and tools can be used to automate and implement security faster in the development process, allowing for quicker implementation. NIST notes that DevSecOps can be used with the following types of coding and coding services:¹⁹⁹

- **Application code:** Code used for one or more business functions, made up of code describing the business transactions and any database access.
- **Application services code (e.g., service mesh code):** Provides various services for the application, such as service discovery, establishing network routes, network resiliency services (e.g., load balancing, retries), and security services (e.g., enforcing authentication and authorization based on policies).
- **Infrastructure as code:** Expresses the computing, networking, and storage resources needed to run the application in the form of declarative code.
- **Policy as code:** Contains declarative code for generating the rules and configuration parameters for realizing security objectives through security controls (e.g., authentication and authorization) during runtime.
- **Observability as code:** Code that triggers automation of software related to logging all transactions, tracing communication pathways involved in executing application requests, and monitoring applications during runtime.

As infrastructure and development activities have moved to a cloud-based environment, the use of the term “as code” is often added to the type of technique. Further, “when using ‘as code’ techniques, the code that is written (e.g., for provisioning a resource) is managed like application source code. This implies that it is versioned, documented, and has access controls defined similarly to what is done for an application source code repository.”²⁰⁰ In addition, some on-premises hardware components may be replaced and deployed as software in cloud-based environments.

¹⁹⁸ Refer to NIST SP 800-204C, [Implementation of DevSecOps for a Microservices-Based Application With Service Mesh](#).

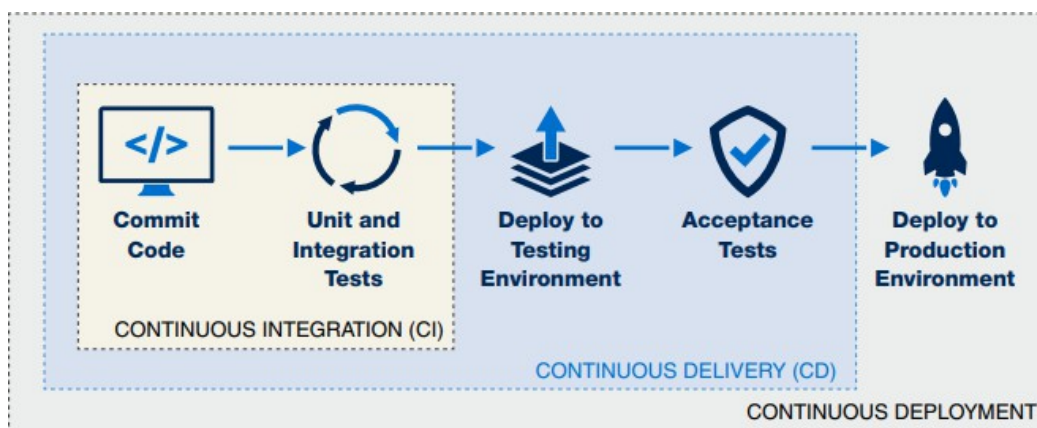
¹⁹⁹ [Ibid.](#)

²⁰⁰ [Ibid.](#)

DevSecOps makes use of the continuous integration (CI)²⁰¹ and continuous delivery (CD)²⁰² or continuous deployment²⁰³ pipeline (see figure 6) during the SDLC, depending on whether the entity uses automation to move code into production. The U.S. Department of Defense (DOD) defines this CI/CD pipeline as “the set of tools and the associated process workflows to achieve CI/CD or continuous deployment with build, test, security, and release delivery activities, which are steered by a CI/CD orchestrator and automated as much as practice allows.”²⁰⁴

Developers digitally sign code in the CI/CD pipeline process. This helps with determining code integrity. For example, downstream evaluations can compare the expected code author’s name to the name of the person who last changed the code and take appropriate action if they do not match.

Figure 6: CI/CD Pipeline Process Workflow



During CI (as illustrated above), developers frequently merge code changes into a central repository where automated builds and tests run.²⁰⁵ CI activities include committing code (i.e., establishing

²⁰¹ Continuous integration (CI) involves developers frequently merging code changes into a central repository where automated builds and tests run. Build is the process of converting the source code to executable code for the platform on which it is intended to run. When developers use CI to deploy new software, the developer’s changes are validated by creating a build and running automated tests against the build. This process avoids the integration challenges that can happen when waiting for release day to merge changes into the release branch. For more information, refer to NIST SP 800-204C, [Implementation of DevSecOps for a Microservices-Based Application With Service Mesh](#).

²⁰² NIST defines “continuous delivery” as “the stage after CI when code changes are deployed to a testing or staging environment after the build stage.” For more information, refer to NIST SP 800-204C, [Implementation of DevSecOps for a Microservices-Based Application With Service Mesh](#).

²⁰³ NIST defines “continuous deployment” as “similar to continuous delivery except that the releases happen automatically, and changes to code are available to customers immediately after they are made.” For more information, refer to NIST SP 800-204C, [Implementation of DevSecOps for a Microservices-Based Application With Service Mesh](#).

²⁰⁴ Refer to DOD’s [DoD Enterprise DevSecOps Reference Design: Version 1.0](#).

²⁰⁵ For a definition of CI, refer to NIST SP 800-204C, [Implementation of DevSecOps for a Microservices-Based Application With Service Mesh](#).

version control, in which a snapshot is taken of the current code changes and saved to a repository), developers packaging up code (i.e., bundling of related code) or revisions to code, and automated initial code testing (such as unit and integration testing).

Management often uses CI processes to put the entity's apps into containers directly in the build process itself. Also, during CI, code is uploaded into a central repository where automated tools validate and initially test the code. The purpose is to avoid inconsistency from the very beginning of an app's life cycle to help ensure consistency in the app's runtime environment (i.e., the environment in which a program is executed). Many organizations may see developers build in one environment, test in another, and deploy in a third, so having consistency in assessment and enforcement across these environments is key.²⁰⁶

Once the code is initially validated and tested, CD automatically deploys code to the formal testing environment for acceptance testing. Within the CD segment illustrated above, code is deployed to production manually, using scripts to assist in the configuration. In continuous deployment, rather than manually, deployment occurs when the entity automates the deployment process, and code is available to users immediately.

NIST documents the following resources and tools used in the CI/CD pipeline process:²⁰⁷

- **Pipeline software.**
 - CI software: Pulls code from a code repository for building the software, facilitates initial testing tools, and saves tested artifacts to an image registry (i.e., repository for copies of code to maintain coding integrity).
 - CD or continuous deployment software: Pulls artifacts from the repository and deploys the package.
- **Development software.**
 - Build tools: Used for constructing software (e.g., for integrated development environments).
 - Testing tools (e.g., software application security testing, dynamic application security testing, or software composition analysis).
- **Repositories.**
 - Source code repositories (e.g., GitHub).
 - Container image repositories or registries.
- **Observability or monitoring tools.**
 - Logging and log aggregation tools.
 - Tools that generate metrics.
 - Tracing tools (e.g., sequence of application calls).

²⁰⁶ Refer to NIST SP 800-190, [Application Container Security Guide](#).

²⁰⁷ For more information, refer to NIST 800-204C, [Implementation of DevSecOps for a Microservices-Based Application With Service Mesh](#).

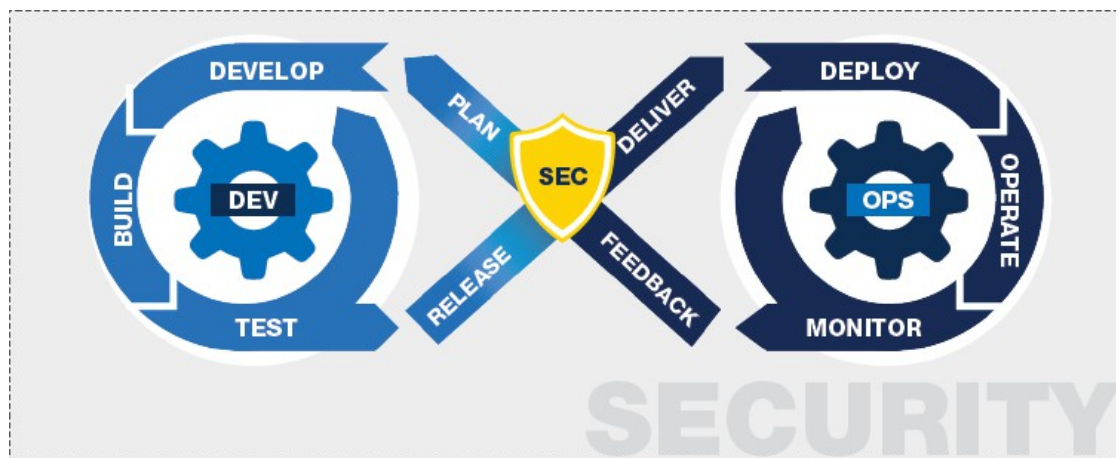
- Visualization tools (e.g., used to combine data from all development activities to generate dashboard/alerts).

NIST recommends the following controls to secure the CI/CD pipeline process:²⁰⁸

- Harden servers hosting code and artifact repositories.
- Secure credentials (e.g., authorization tokens) used for accessing repositories.
- Implement controls on who can check in and check out artifacts in container image registries. These registries store artifacts produced by the CI pipeline and serve as bridges between the CI and CD pipelines.
- Log all code and build update activities.
- Send build reports to developers and stop further pipeline tasks when a build or test fails in the CI pipeline. Code repositories should be configured to automatically block all subsequent pull requests from the continuous deployment stage of the pipeline until issues are resolved.
- Send build reports to the security team and stop further pipeline tasks when an audit fails.
- Ensure that developers can only access the application code.
- Digitally sign (preferably multiparty digital signing) the release artifact during each required CI/CD stage during the build and release process.
- Verify that all required digital signatures are present during production release to ensure that no one bypasses the pipeline.

Figure 7 provides an overview of the CI/CD pipeline. Automated security testing is performed throughout development phases and throughout production.

Figure 7: CI/CD Pipeline Architecture²⁰⁹



²⁰⁸ Refer to NIST SP 800-204C, [Implementation of DevSecOps for a Microservices-Based Application With Service Mesh](#).

²⁰⁹ Refer to DOD's [DoD Enterprise DevSecOps Reference Design: Version 1.0](#).

V.E Functional Development Types

Functional development types include hardware, software, front end, and backend. Examples of hardware developed for the financial sector are point-of-sale terminals, mobile card readers, credit cards, and managed security devices. Examples of software developed for the financial sector are mobile banking apps, online banking systems, loan estimators, core banking systems, transaction monitoring systems, and imaging systems. Development of either hardware or software may include a combination of backend and front-end development types. Backend refers to the parts of systems that are not seen by the end user. Front end refers to the parts of systems that the end user sees and uses. Understanding that there are different functional development types is important for development teams as each development type may have unique procedures (e.g., steps and timing), include various reporting lines (e.g., internal and external stakeholders, including management), and address different risks (e.g., physical and virtual) depending on the project.

Functional development types can include the following:

- **Hardware development:** Hardware development includes integrating hardware with software to provide a user experience that supports the business use cases. This includes designing and building the physical aspects of a hardware component. Hardware may include servers, circuit boards, credit cards, ATMs, point-of-sale terminals, and mobile reader devices. The hardware developer designs the system, selects components, builds prototypes, and coordinates testing. The developer generally has in-depth knowledge of software development because developing hardware requires using complex design tools and programming skills. Hardware development includes incorporating firmware and producing circuitry concepts and circuit diagrams, which are then put into operation. The developer designs circuit board layouts and programs microchips and microcontrollers. They develop and simulate digital signal and image processing. They are responsible for maintenance and testing as well as preparing manufacturing documents and product documentation. Hardware developers are sometimes referred to as electronics developers or hardware designers.
- **Front-end (or client-side) development:** Front-end²¹⁰ development can be facilitated through hardware or software-based solutions. A front-end developer works toward providing an effective end-user experience. This includes anything (e.g., text and layout, touchscreen, and icons) the user interacts with on their devices (e.g., PCs, tablets, mobile phones, and ATMs). Developers combine design, technology, and programming to create user interfaces that provide clear and understandable products with end-user appeal. Another front-end consideration is the importance of integrating the business line product rules (e.g., rules for negative interest rate changes or loan-to-value limitations) into the user interface. Front-end development may include web development, desktop development, mobile development, and graphics development.

²¹⁰ Merriam-Webster defines “[front end](#)” as “a software interface (such as a graphical user interface) designed to enable user-friendly interaction with a computer.”

- **Backend development (or server-side development):** Backend²¹¹ development can be facilitated through hardware or software-based solutions. Backend development includes developing databases, internal APIs, business logic, microservices, web integration, servers, and server-based utilities. Users interact directly with the front end to communicate and engage with the backend, which is not visible to end users. Backend developers should understand front-end development and vice versa. Without that understanding, the risk of noncompliance with laws and regulation increases. For example, financial institution customers rely on loan calculators to provide accurate results relevant to their input scenario. Visible and correct results are only possible if the user interface is clear (front-end development) and the calculations are accurate (backend development).
- **Big data development:** Big data development focuses on using, organizing, and maintaining large amounts of data that may originate from many sources. Big data development includes building data mining, data visualization, and quantitative analysis tools. In addition to developing specific tools, big data developers work with analysts to help them decide whether a set of data are appropriate for their analytics. Big data development can result in maintaining petabytes of complex unstructured, semi-structured, and structured data without rigid schemas. When appropriately controlled, big data can enable cost-effective processing of massive volumes of data, support multiple concurrent queries and other analytics tasks, and rapidly generate results. However, if big data environments are not adequately controlled, costs may increase rapidly, and the examined entity may rely on inaccurate information for business decisions. For additional information on big data, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" booklet.

The following subsections of this booklet provide more information on additional development types, including model development and database development.

V.E.2 Model Development

For purposes of this discussion, “model” refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.²¹² A model consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information. Models meeting this definition may be used in the following:

- Analyzing business strategies.
- Informing business decisions.
- Identifying and measuring risks.
- Valuing exposures, instruments, or positions.
- Stress testing.

²¹¹ *Merriam-Webster* defines “[backend](#)” as “the part of a software system that is not usually visible or accessible to a user of that system.”

²¹² For purposes of this discussion, the term “model,” is used as described in joint agency guidance, FRB SR Letter 11-7, “[Guidance on Model Risk Management](#),” and OCC Bulletin 2011-12, “[Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management](#).”

- Assessing capital adequacy.
- Managing client assets.
- Measuring compliance.
- Maintaining the formal control apparatus of the bank.
- Meeting financial or regulatory reporting requirements.
- Issuing public disclosures.

V.E.3 Database Development

Databases are digital repositories of data designed to be accessed, managed, and updated. They can be internally developed or purchased from third parties. Commonly used database models include hierarchical, networked, relational, object-relational, and nonrelational. Developers should understand the different types, structures, and uses of databases to effectively mitigate database development risks. To do this, it is important to understand the benefits, limitations, and appropriate controls for the type of database used. Examples of risks developers of databases should consider include the following:

- Data errors and omissions.
- Inappropriate database access privileges.
- Misuse of legitimate privileges.
- Database injection attacks (e.g., SQL injection).
- Malware.
- Storage media exposure (e.g., backups).
- Exploitation of vulnerable databases (e.g., failure to patch and maintain the database).
- Unmanaged sensitive data (e.g., failure to maintain an accurate database inventory that includes each database's content and the content's sensitivity).
- Human error (e.g., failure to apply security controls, enforce policies, or implement appropriate incident response processes).

Potential mitigation strategies include the following:

- Maintaining a database inventory that includes the database location(s), contents, and sensitivity.
- Assessing databases for any vulnerabilities.
- Managing user access rights (e.g., removing user access and privileges when access is no longer required for business purposes).
- Logging and monitoring database access and usage to identify patterns and help detect data leakage, unauthorized or significant activity, and system and component attacks in real time.
- Blocking inappropriate web requests.
- Backing up the databases.
- Encrypting databases.
- Training database developers on their security-related development responsibilities, including identification of potential information security risks and appropriate mitigation practices.

Prudent practices include choosing databases that meet business and other stakeholder objectives and implementing controls, including access controls, to protect the data consistent with their criticality and sensitivity. Additional database design and selection considerations are flexibility, scalability, data integrity, and retrieval efficiency.

VI ACQUISITION

Action Summary

Management should establish acquisition processes that are commensurate with the entity's business and procurement needs. Management should also assess and mitigate procurement risks associated with an entity's overall strategic, regulatory, and operational risks.

Examiners should review the following:

- Project requests and plans for one or more recent acquisitions.
- Strategic and business plans, risk assessments, due diligence activities, and acquisition-related meetings with minutes.
- Contracts and licensing agreements.
- Acquisition policies, standards, and procedures, including evaluation criteria and documentation maintenance practices.
- Acquisition training and entity guidance for stakeholders.
- Acquisition and procurement-related audits.

NIST defines “acquisition” as “all stages of the process of acquiring a system, product, or service, beginning with the process for determining the need for that system, component, product, or service and ending with contract completion and closeout.”²¹³ While acquisition and procurement are terms often used interchangeably, for purposes of this booklet acquisition refers to the overarching process and procurement refers to the specific steps to obtain the system, product, or service. To effectively manage the risks inherent in acquired systems, components, products, or services, entity personnel identify key roles and responsibilities. For example, once management completes contract negotiation and takes control of the system, component, product, or service, management determines the activities related to and responsibilities for oversight (e.g., entity's third-party or enterprise risk management office).

An entity may acquire technology or technology services from a third party, rather than developing it in-house. An entity may use or acquire systems, components, products, and services from various sources, including internal development teams, technology and software development firms, co-sourced arrangements, open-source repositories, and commercial sources. When an entity purchases systems, components, products, or services, effective management ascertains whether the product specifications are “fit for purpose” and meet the entity's requirements, whether purchasing directly from the OEM partners or a secondary market. This should be addressed in agreements with supply chain partners.

The acquisition of system, components, products, and services (versus in-house development) poses certain risks at each step of the acquisition process that should be assessed and mitigated. Risks associated with the third-party product or service may vary depending upon the specific

²¹³ Refer to [NIST Glossary](#).

situation. These may include strategic (e.g., the system does not align with business needs), regulatory (e.g., the solution does not consider GLBA), and operational risks (e.g., the provider does not have an adequate testing environment or sufficient resources to maintain the solution). In addition, there may be third-party risk management concerns,²¹⁴ weaknesses in security controls, or other operational weaknesses at the third-party provider.

An entity may mitigate the risks associated with acquisition in several ways. The following are examples of effective risk mitigation:

- Develop policies, standards, and procedures to effectively carry out the entity's procurement processes aligned with the entity's acquisition activities.
- Perform potential supplier due diligence reviews.²¹⁵ Due diligence rigor should align with a risk assessment that identifies the criticality of the business function supported, the information sensitivity the system or component stores or processes, business function complexity, and external factors such as the supplier's location and ownership.
- Implement contract and licensing processes for all acquisitions, particularly for more complex relationships. An entity's processes should include contract and license review to help ensure that the rights, responsibilities, and accountability of each party are clear.

A structured procurement process (such as the procurement steps in figure 8) is likely to produce more consistent and sustainable results across an entity over time. The more critical the system, component, and service being procured the more important that each procurement step is successfully completed.

In the example in figure 8 below, the procurement process begins with the identification of an entity's business need for procuring a system, component, or service. Then management may engage in the following:

- **Planning.** Planning what information will be needed to procure the best system, component, or service, and requesting information from the project team and key stakeholders.
- **Defining requirements.** From planning and information provided, clearly defining what requirements are necessary.
- **Solicitation.** Requesting quotes or proposals.
- **Evaluation and selection.** Evaluating proposals and determining the best choice.
- **Contract negotiation and award.** Determining contract requirements and responsibilities, and which risks will not be covered in contract.

²¹⁴ Refer to the following guidance: [Interagency Guidance on Third-Party Relationships: Risk Management](#), also noted in OCC Bulletin 2023-17, "[Third-Party Relationships: Interagency Guidance on Risk Management](#)"; FDIC FIL-29-2023, "[Interagency Guidance on Third-Party Relationships: Risk Management](#)"; and FRB SR Letter 23-4, "[Interagency Guidance on Third-Party Relationships: Risk Management](#)." Also see CFPB Compliance Bulletin and Policy Guidance 2016-02, "[Service Providers](#)."

²¹⁵ Refer to NIST SP 800-53, rev. 5, SR-3, [Supply Chain Controls and Processes](#), notes that rigorous due diligence includes research on potential suppliers or products, as well as their upstream dependencies (e.g., fourth- and other parties beyond third-party suppliers), which can help enterprises avoid single points of failure in their supply chains. The results of this research can be helpful in shaping the sourcing approach and refining requirements.

- **Vendor management and ongoing administration.** Oversight and maintenance of the relationship, if ongoing.
- **Preparing for the off-ramp.** EOL or upgrade of system, component, or service.

Figure 8: Procurement Steps: Example



An effective procurement process helps management and personnel to address each step in the process, communicate and meet combined stakeholder requirements, select appropriate systems and components, and support the entity's overall business objectives. Additionally, an effective process helps minimize confusion (e.g., by identifying minimum requirements) and promotes coordination in the supply chain (e.g., by achieving efficiencies using one OEM for multiple products).

Specific procurement risks to address include the following:

- Actual costs being materially higher than budget.
- Procured system, component, or service does not meet all stakeholder's requirements.
- Due diligence does not reveal a material third-party deficiency.
- Procured system does not interoperate with existing systems.
- Procurement process informality leads to inconsistent system, component, and service selection over time.
- Contract or license does not specify characteristics critical to system, component, and service success.
- Lack of visibility into supply chain partners for identification of weaknesses (e.g., security, interoperability, or incident response).

VI.A Acquisition Policies, Standards, and Procedures

Acquisition policies, standards, and procedures that are enforced create acquisition consistency across the entity. Well-communicated and enforced policies, standards, and procedures are important for the acquisition process to help determine the appropriate technology for new IT

procurement requests or requests for significant updates to current systems and components. Without adequate policies, standards, and procedures, management may expose the entity to the following:

- Procurement of a system or component that does not address the business need.
- Products or services that fail to protect the confidentiality, integrity, availability, and resilience of the entity's systems and components, which may adversely affect other systems in the entity's supply chain.
- Noncompliance with legal and regulatory requirements (e.g., Information Security Standards, Bank Service Company Act).
- Inadequate contracts and licensing agreements, due to failure to communicate and involve key stakeholders (e.g., IT, information security, privacy, legal, and compliance personnel).

An effective entity's acquisition policies, standards, and procedures address the following:

- Information requests, such as requests for information (RFI) and requests for proposals (RFP) to third parties. Responses to these requests provide the entity with vital information for identifying the best provider solution. Requests for quotes (RFQ) are also used before final selection to obtain the best pricing. For additional information on RFIs, RFPs, and RFQs, refer to the "[Solicitation](#)" section in this booklet.
- Third-party due diligence²¹⁶ includes the following:
 - Comprehensively assessing risks associated with third-party relationships.²¹⁷
 - Reviewing system, component, and service operational and internal controls (e.g., security and resilience controls).
 - Evaluating and selecting (including criteria for selection) a third party.
 - Checking references (e.g., through external user groups or banking association members) to ascertain current and past customer views on product and service quality.
- Specialist stakeholders' (e.g., subject matter, legal, and compliance experts) review of proposal.
- Contract negotiation to ensure that the contract contains terms amenable to the entity.
- Transferability or portability of systems, components, products, and services if a third-party relationship is discontinued.
- Contract signature authority.
- System, component, and service validation to ensure that user requirements are met before acceptance.

In some cases, management may acquire systems, components, or services from foreign-based third parties. In addition to information security risks, there are several unique risk considerations in these relationships, including the following:

²¹⁶ Refer to the following guidance: [Interagency Guidance on Third-Party Relationships: Risk Management](#).

²¹⁷ The risk assessment typically includes a third party's personnel background checks, customer service issues, financial condition, stability, and fourth-party products or services.

- **Legal.** Confusion over which country's laws will control the relationship. Additionally, it is important to consider that there may be specific U.S. laws with which the entity and its third-party service providers may need to comply (e.g., the restriction on the export of software applications employing encryption techniques).
- **Country.** The possibility that economic, social, or political conditions and events in a foreign country will adversely affect an entity's financial and business interests (e.g., financial defaults by obligors in a foreign country, nationalization of private assets, government repudiation of external indebtedness, exchange controls, or significant currency devaluations).
- **Currency (or exchange rate).** The risk that arises from the change in price of one currency in relation to another. Assets or business operations located across national borders are exposed to and affected by currency risk, creating unpredictable profits and losses, currency devaluations, and foreign exchange controls.
- **Geopolitical.** Risk associated with wars, terrorist acts, and tensions between states that affect the normal and peaceful course of international relations. For example, regime change in the country of operations may result in a loss of control over the entity's data stored in that country.
- **Resilience.** The risk that operations and assets may be undermined or destroyed by crises. This includes the capacities and resources of business systems affected by risks, stresses, and shocks. For example, if there is a disruption of utilities in a country, it may disrupt data center operations.

Management should be knowledgeable of these risks and their effects on the business before entering foreign-based third-party relationships. Therefore, effective management identifies, plans, and addresses the root causes of foreign-based risks or crises to minimize their effects on the entity's operations.

VI.B Acquisition Projects

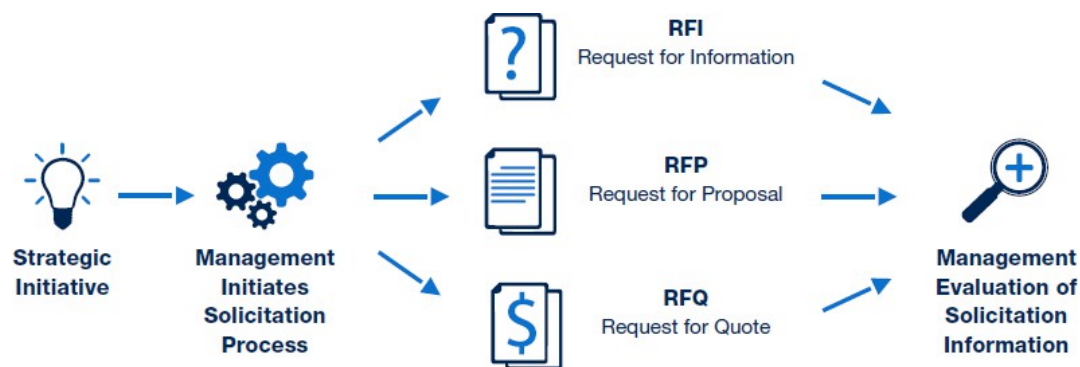
If an entity has a PMO, acquisition projects may be managed according to established entity PMO processes. Smaller or less complex entities may not have the same formality or rigor in their acquisition project processes. However, it is still important to have project guidance and procedures for the management of acquisition projects. If a procurement project request is approved, the feasibility study should clearly define the IT, information security, functional, legal, and regulatory requirements in the RFIs and RFPs that management distributes to third parties in the solicitation process for bids, including RFQs. Acquisition projects should follow the same principles as noted above throughout section IV.N. "[IT Project Management](#)."

VI.C Solicitation

For procurement projects, management follows the entity's requirements definition with solicitation for information and evaluation. These solicitations do not represent binding agreements between the entity and a third party. An entity's solicitation process generally is initiated when it has a business need or problem to solve. Management may issue RFIs to determine potential third parties with solutions available to address the business need or problem and gather information. When the entity has gathered the appropriate information and narrowed

down the number of potential third parties, management may issue an RFP to ask those third parties to propose specific solutions. This helps management evaluate and prioritize third parties and their solutions. When management has identified the third parties that can meet the business needs, it uses the RFQ to validate specific requirements and ask whether the third party is able to meet those requirements, and if so, to list all associated costs to help management determine its final selection. For smaller or less complex entities, these terms and steps may not be as clearly delineated or defined; however, management should still have a process that considers business needs, third-party solutions, specifications, and costs. A solicitation to a potential third party may involve an RFI, RFP, or RFQ, or a combination of the three if the entity chooses to move forward with a particular third party on a project, as shown in figure 9 and described in more detail below.

Figure 9: Third-Party Solicitation Types and Inputs



- RFI:** A request for information is a market research tool also referred to as a sources-sought notice that is used to obtain, for example, price, delivery, capabilities, and interest for planning purposes.²¹⁸ Management may use an RFI to identify third parties that should be targeted for more specific information or further requests. The RFI includes the entity's requirements and appropriate questions that will allow respondents to provide necessary information for stakeholders to make acquisition decisions. Third parties receive requests and provide information about their capabilities, including products or services they offer, and interest in establishing a relationship. There is no standard format for an RFI; however, a formal, well-crafted RFI may facilitate faster responses from potential third parties by providing an overview of the entity's requirements, including any specific questions for the third party. The RFI should clearly identify the entity's needs to avoid a third party's confusion with the request and omission of critical information needed for decision-making. When management receives information from the third parties, assumptions should not be made based on the responses. Instead, if appropriate, management should consider asking follow-up questions to clarify concerns or solicit more information. Additional considerations when reviewing third parties' RFI responses include the following:

- RFI format: Whether the provider followed the format specified in the RFI.

²¹⁸ For more information, refer to U.S. General Services Administration's (GSA), "[RFP, RFI, and RFQ: Understanding the Difference](#)."

- Third-party interest: Whether the third party is interested in forming a relationship.
 - Business size: Whether the third party has the resources (e.g., personnel and infrastructure) to support or provide resilience for the suggested solution.
 - Location: Proximity of the third party's location to entity locations and effect on resilience.
 - Qualifications: Whether the third party's personnel have appropriate knowledge and experience, as well as whether the entity has the personnel and training to operate the solution.
 - Subcontractor involvement: Third-party standards for subcontracted work, responsibilities and liabilities for subcontractors, third-party due diligence on subcontractors, and percentage of work to be performed by subcontractors.
 - Conflicts of interest: Whether doing business with this provider causes conflicts with other entity third-party providers, internal conflicts of interest at the entity (e.g., a relative of entity personnel works at the third party), or anticipated conflicts of interest with the third parties.
- **RFP:** A request for proposal is a solicitation method that communicates the entity's requirements and requests proposals.²¹⁹ An RFP is a formal procurement activity to solicit bids. When drafting an RFP, it is critical to communicate an entity's key system and component requirements, especially those that may incur significant costs to implement. An RFP can include a solicitation for quotes. Bids in response to an RFP provide information needed to select a provider. Information such as the description of the bidder's approach, price, and personnel expertise are helpful in differentiating between bidders to make a final selection.

Additional considerations when reviewing third parties' RFP responses include the following:

- Terms and conditions that can help management identify limitations (e.g., length of agreement, resource ceilings, and potential interruptions in service) that the third party may have.
 - Whether a third party follows the RFP format and provides the required information (e.g., cost, experience of the third party, and resilience), which indicates the third party's attention to RFP requirements.
 - Whether the third party's responses are detailed, specific, and responsive (e.g., timely and with no exceptions to the solicitation).
- **RFQ:** A request for quote is a solicitation method used to obtain price, cost, delivery, and related information from suppliers.²²⁰ An RFQ can provide more precise information for bidder comparison and budgeting. There is a potential risk in the RFQ process that bidders misunderstand when an entity is bound by an agreement and a contract is created. To

²¹⁹ For more information, refer to GSA, "[RFP, RFI, and RFQ: Understanding the Difference.](#)"

²²⁰ [Ibid.](#)

mitigate this risk, an entity should include legal counsel to help guide the engagement and help avoid potential contractual issues. For additional information on contracting,²²¹ refer to the [“Contracts and Other Agreements”](#) section of this booklet.

For more information on third-party risk management, refer to the *FFIEC IT Handbook’s* [“Outsourcing Technology Services”](#) booklet.

VI.D Evaluation

A formal process for evaluating RFI, RFP, and RFQ responses produces higher quality selections of third parties across the entity and reduces legal risk. The process goal should be a fair and consistent approach to evaluating and eventually selecting a third-party provider. The process should include procedures to compare each proposal or quote to the entity’s defined requirements for the systems, components, or services needed. Then, the entity can compare all the proposals or quotes that meet those requirements. When the process includes pre-determined evaluation criteria, the process is more equitable and legal risk is reduced. Careful consideration helps management determine appropriate evaluation criteria that assists in the review of the widely varying proposals (e.g., bidders proposing either SaaS, infrastructure-as-a-service [IaaS], or platform-as-a-service [PaaS])²²² to meet the basic requirements. Table 3 lists evaluation criteria examples.

Table 3: Evaluation Criteria Examples for Third-Party Solicitations

General criteria for all products and services:

• Ability to audit or receive independent audit reports. • Confidentiality and privacy standards. • Copyright standards. • Delivery dates. • Liability limitations. • Licensing restrictions. • Maintenance procedures. • Financial performance and condition. • Information security requirements set by the entity. • Backup and resilience options. • Costs, fees, and discounts.	• Operations and internal controls. • End-of-service or EOL. • Legal and regulatory requirements. • Subcontractor details. • Testing standards. • Third-party service provider customer reference. • Training provided. • Warranty specifications. • Event or incident response roles and responsibilities. • Insurance considerations.

Software products and services:

• Compatibility of Oss. • Escrow criteria.	• Next release date. • Programming language.

²²¹ Refer to the following guidance: [Interagency Guidance on Third-Party Relationships: Risk Management](#), as noted in OCC Bulletin 2023-17, [“Third-Party Relationships: Interagency Guide on Risk Management”](#); FDIC FIL-29-2023, [“Interagency Guidance on Third-Party Relationships: Risk Management”](#); and FRB SR Letter 23-4, [“Interagency Guidance on Third-Party Relationships: Risk Management”](#). Also see CFPB Compliance Bulletin and Policy Guidance; 2016-02, [“Service Providers.”](#)

²²² Refer to the *FFIEC IT Handbook’s* [“Architecture, Infrastructure, and Operations”](#) booklet for more information on SaaS, IaaS, and PaaS.

Hardware products and services:

• Maintenance requirements (for the entity and the third party). • Capacity (e.g., memory, bandwidth, storage, power).	• Servicing options. • Performance capabilities.

For more information on evaluation considerations, refer to the *FFIEC IT Handbook's* [“Outsourcing Technology Services,”](#) [“Architecture, Infrastructure, and Operations,”](#) [“Information Security,”](#) and [“Management”](#) booklets.

VI.E Contracts and Other Agreements

Contracts and other types of agreements are used to document the terms and conditions under which systems, components, and services are provided. Acquisition policies, standards, and procedures specify how contracts and other agreements are documented, reviewed, and approved. Agreements²²³ take many forms and may be included in a contract by reference. Agreement examples are statements of work (SOW), master services agreements (MSA), SLAs, and escrow agreements. To ensure that contracts and other agreements are legally enforceable, legal counsel should be involved in the acquisition process before finalization. Contracts are intended to be legally binding agreements between two or more parties. They generally identify the goods and services to be provided, the time frame for provision, and the associated costs and fees. There may be several documents involved in the procurement process; therefore, it is helpful to identify each of the agreements and contracts, which will assist management in completing the evaluation and selection steps. These documents may be useful to management in its effective oversight of the performance of the entity's supply chain partners. The following subsections describe several agreements and contracts commonly encountered during examinations.

VI.E.1 Statement of Work

An SOW is one supporting document for contracts, detailing the activities to be performed and the activity output in system and component development (e.g., performance level, operating reports, developer documentation, and user manuals). This documentation is critical to system and component maintenance because it details maintenance standards for operations. SOWs can also specify the security assurance requirements (e.g., code reviews, penetration tests, and SOC reports). The security assurance requirements should include the processes that the developer and other staff will follow. Additionally, the SOW may specify the verification process for delivery of products and services, including what task completion evidence is required for payment. SOWs often become part of a binding agreement, such as a contract.

While the contract defines the legal aspects of the relationship, the SOW generally contains elements, such as the following:

- Purpose of the relationship.

²²³ For purposes of this booklet, *Black's Law Dictionary* defines [“agreement”](#) as “the consent of two or more persons concurring, the one in parting with, the other in receiving, some property, right, or benefit.”

- Project objectives.
- Services and products to be provided (i.e., scope of work).
- Schedule, including deliverables and delivery deadlines.
- Requirements for providing the desired services and products, including potential penalties or payment retention for unsatisfactory work.
- Objective measure of satisfactory completion of work.
- Payment due date and method.
- Legal and regulatory requirements.
- Location and duration of the work.
- Acceptance criteria.

There is no standard SOW format across entities and industries. It is up to appropriate stakeholders at the examined entity to determine the format according to the entity's needs. Effective entities provide guidance to relevant personnel in support of a structured approach to SOW development to promote consistent and positive acquisition results, often achieved through SOW training. Similarly, involving all stakeholders in SOW development and establishing an appropriate management review and approval process are both effective practices in achieving positive acquisition results consistently across an entity.

SOW details are important because the type, duration, and complexity of work varies significantly. Clear and specific SOWs help increase the likelihood that bids are comparable, that selection decisions are made quickly, and that miscommunication and misunderstanding are avoided. For example, the SOW should identify the responsibilities of all parties involved. One risk is that service and outsourcing providers can become so focused on the customer entity's needs and requirements that they overlook their own. In order to meet requirements and provide for delivery of a quality product or service, it is important that the provider's needs and requirements (e.g., price, security, and interoperability) also be specified and met. Another example of effective SOW details includes the documentation required from supply chain partners.²²⁴ When an SOW is specific, it can be used to measure whether requirements have been met to an acceptable level.

An SOW may include elements, such as the following:

- Statement of confidentiality.
- Description of work with assumptions and constraints.
- Services to be provided.
- Facility and security requirements.
- Marketing requirements.
- Transition requirements.
- Training and reporting requirements.
- Roles and responsibilities.
- Schedule.

²²⁴ Refer to NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#), and NIST's Response to Executive Order 14028, [Software Supply Chain Guidance: Software Security in Supply Chains](#).

- Pricing.
- Approvals.
- Glossary.
- Appendix (e.g., containing an incident response plan with contractor responsibilities).

In addition to SOWs, there are alternative methods²²⁵ to document details for proposals (e.g., RFI, RFP, and RFQ), which support the contract or other agreements. One example of these alternatives includes a statement of objectives (SOO), which identifies the broad business outcomes and objectives for performance.²²⁶ An entity makes a request for detailed proposals (i.e., an SOO), which are provided in response. Another alternative is a performance work statement (PWS),²²⁷ which emphasizes outcomes, desired results, and objectives at a more detailed and measurable level. An appropriate response is furnished by prospective providers. These alternative methods may be used in conjunction with the other documents noted above (e.g., RFI, RFP, and RFQ). Information from the SOO or PWS may then be included into the contract to produce a more effective engagement.

VI.E.2 Master Services Agreement

MSAs are “master” documents that govern multiple agreements or transactions between entities. The MSA often sets forth the principal legal terms that govern the parties’ relationship and are usually drafted by the service provider. An MSA usually governs or incorporates additional contract documents, such as software license agreements, policies and procedures, terms and conditions, data protection agreements, end-user license agreements, and SOWs. These additional contract documents provide important information to operations personnel.

An MSA helps the parties change contracted services more quickly than without an MSA, because services do not have to be renegotiated each time there is a mutually agreed-upon change to underlying services. For example, a financial institution and a third-party core banking platform product or service provider may enter into an MSA that covers the core banking platform and the possible use of related software and services (e.g., payments software, consulting services, and cloud storage platform). Therefore, changes to the listed services noted in the MSA could occur without creating a new agreement.

MSAs typically include items such as the following:

- Service overview.
- Terms of agreement (e.g., payment, audit, subcontracting, or confidentiality).
- Proprietary rights.
- Intellectual property rights.
- Insurance and taxes.
- Representations and warranties (e.g., patents and trade secrets).

²²⁵ Refer to GSA, “[PWS, SOO, SOW - Finding the Best Fit](#),” for more information.

²²⁶ Refer to GSA, “[Respond to a Solicitation](#),” for more information.

²²⁷ Refer to GSA, “[Performance Work Statement](#),” for more information.

- Limitation of liabilities (e.g., a force majeure clause).²²⁸
- Dispute resolution process.
- Agreement termination process.
- Legal jurisdiction (e.g., country, state, federal, or local).

VI.E.3 Service Level Agreement

An SLA is a formal agreement between two parties that records a common understanding about products or services to be delivered and how they will be delivered, including the following:

- Priorities, responsibilities, guarantees, and warranties between the parties.
- Nature, quality, security, availability, and scope.
- Timeliness of delivery and response of the parties.
- Point(s) of contact for end-user problems.
- Metrics to monitor the effectiveness of the process.
- Approvals.
- Other measurable objectives.
- Expected day-to-day situations and unexpected or adverse events.

An SLA represents a commitment between a third party and one or more customers and addresses specific aspects of the service, such as responsibilities, details on the type of service, expected performance level (e.g., reliability, acceptable quality, and response times), and requirements for reporting, resolution, and termination.²²⁹

SLAs are an effective practice to mitigate the risk of differing performance expectations. When procuring services related to a system or component, agreements should have clear and measurable expectations for the services provided, recourse when expectations are not met, and accountability for both parties. SLAs generally include how the third party expects to meet the SLA requirements and establishes incentives for the third party to meet, or penalties for failing to meet, those requirements. The SLA should be linked to clauses in the contract regarding incentives, penalties, and contract termination to protect the entity in the event of third-party performance failures. For more information, refer to the *FFIEC IT Handbook's* "[Outsourcing Technology Services](#)," "[Management](#)," and "[Information Security](#)" booklets.

VI.E.4 Contracts

Contracts between an entity and its third parties should clearly describe the rights and responsibilities of the respective parties. Contracts are formal binding documents, usually preferable to agreements, which can be informal and may not be enforceable in a court of law.

²²⁸ A contract or agreement clause pertaining to "[force majeure](#)" (i.e., "act of God") risk, irresistible force, or uncontrollable event (e.g., war or civil unrest) that refers to an event or circumstances "when business is disrupted due to a factor beyond control." This type of clause allocates the risk of loss if performance is hindered, delayed, or prevented because of an event that the parties could not have anticipated or controlled. It helps provide a contractual defense, the scope and effect of which depends on the express terms of a particular contract.

²²⁹ Refer to NIST SP 800-47, rev. 1, [Managing the Security of Information Exchanges](#).

An example of important rights to specify are license rights²³⁰ when the entity is using systems and components developed by third parties. Another example is rights and liabilities relating to leased hardware necessary to operate related software. The consequences for failure to meet contractual obligations should also be specified. Examples of software development and maintenance-related contract clauses may include the following:

- Software functional and performance specifications.
- Development process milestones and associated payments.
- Development roles and responsibilities for the third party and the entity.
- SLA information and pricing methods.
- Controls over foreign based third-party activities (i.e., activities performed by entities subject to international laws and regulations).
- Software modification restrictions.
- Objective pre-acceptance performance standards to measure the software's functionality. For example, the contract may identify particular tests that will be used to determine whether the software complies with the contract's performance and security standards.
- Training specifications.

Examples of hardware development or maintenance-related contract clauses may include the following:

- Hardware may not be altered from OEM status, as-delivered (i.e., alterations may void the contract or warranty).
- Proprietary hardware remains the property of the vendor or service provider, and access to it is limited.

A third-party's contributions to the mitigation of major risks are particularly important to specify in contract clauses. For example, security and privacy standards to be followed by third-party service providers or vendors that process, store, or transmit sensitive customer data should be specified in the contract. Table 4 has additional examples of contract clauses.

Table 4: Contract Clause Examples

Clause	Considerations
Legal and regulatory requirements	Outlines responsibility for maintaining software so functionality complies with applicable laws and regulations.
Representations, warranties, and indemnifications	Express representations, warranties, and indemnifications including provisions such as: • Licensed software does not infringe on the intellectual property rights of any third parties worldwide.²³¹

²³⁰ Typically, the developing entity provides licenses to the entity that is using the systems or components, granting it certain rights for their use.

²³¹ Under some state laws, noninfringement warranties are limited to the United States unless otherwise specifically stated.

Clause	Considerations
	- Warranties²³² that software performs according to specifications and how a third party responds in the event of problems. - Specifications for the length of the warranty and how the warranty relates to maintenance obligations and agreements. - Representations that software does not contain undisclosed restrictive code or automatic restraints not specifically authorized in the agreement.
Third-party liability limitations	Proposed limitations of liability in the contract should be reasonable based on the amount of loss or disruption the entity might experience. For mission-critical systems or components, broad exculpatory (i.e., cleared from fault) clauses limiting a third party's liability could adversely affect the safety and soundness of an entity (e.g., excessive force majeure clauses and nested third-party activity exclusions that exceed the entity's capital risk parameters).
Payments	Payment schedule and expense details (e.g., installation, conversion, maintenance, and travel). A payments clause may include provisions such as: - Partial payments at specified development milestones, with final payment due after successful system and component acceptance tests. Properly defined milestones can break development projects into segments with deliverables, allowing management to monitor developer progress and identify any potential problems. - Determination of compensation (e.g., based on the developer's time and materials versus a fixed-price agreement with specific payment milestones). Clearly defined compensation information allows for management control over the development process and total project costs. - Consequences if the third party fails to meet any of the requirements stipulated in the contract, such as failure to deliver system or component features and functions. The contract should allow for the right to reject the deliverable and withhold payment until the third party meets all contractual requirements.
Dispute resolution	Dispute resolution clauses specify the process to be used to resolve problems in a timely manner. Dispute resolution clauses may specify that system and component development will continue during a dispute resolution process.
Agreement modifications	These clauses mitigate the risk that the agreement is not modified without appropriate approval because agreement modification may affect pricing or result in necessary modification to systems and components.
Bankruptcy²³³	Clauses that protect the examined entity in the event of third-party bankruptcy. For example, a clause may specify a software code escrow process that would provide the entity access to the code (that is ordinarily accessed only by the third party) in the event of the third party's insolvency. A second example is a clause specifying that the entity will have direct access to cloud-based services and production data used by the third party for the entity's benefit in the case of the third party's bankruptcy.
Information security	Clauses that identify the information security requirements (e.g., compliance or performance standards) and align with the entity's information security program. Refer to the <i>FFIEC IT Handbook's</i> "Information Security" booklet. Examples are: - Clauses that specify the third party's ongoing responsibilities for maintaining the information security and confidentiality of an entity's resources and data. Provisions should address prohibitions on the third party and its contractors or agents using or disclosing an entity's information, except as necessary to provide contracted services. - Clauses guaranteeing that third party-developed systems and components do not and will not permit unauthorized or unknown access (e.g., "backdoors") to the system, component, or the entity's systems or data.

²³² Warranties generally address events and distinguish between mission-critical failures, which should receive an expedited response, and noncritical failures, which management can resolve in a routine manner. It is helpful to review warranties compared to the latest independent certification report demonstrating the software's capabilities.

²³³ Refer to relevant provisions of the [U.S. Bankruptcy Code](#).

Clause	Considerations
	- Clauses that specify the third party's actions in a breach, such as reporting requirements regarding the incident, its resolution, and communication timeliness. For more information on incident response, refer to the <i>FFIEC IT Handbook's</i> "Information Security," "Outsourcing Technology Services," and "Business Continuity Management" booklets. - Legal, regulatory, and entity standards. For example, applicable regulatory standards include GLBA²³⁴ for financial institutions and the Federal Trade Commission's (FTC) <i>Standards for Safeguarding Customer Information</i> for financial institutions subject to the FTC's enforcement authority.²³⁵
Change in control	Clauses addressing contract revision after third party change of control (e.g., merger, acquisition, or change of ownership). This is important as service quality and support may not be maintained after a change in control.
Subcontracting	- Clauses specifying that the third party is responsible for the performance and security of the systems and components regardless of who designed or developed them. Some third parties may subcontract with other parties (referred to as subcontractors or fourth parties) to develop systems and components for their customers. - Notification and approval requirements regarding changes in subcontractors. Management should consider contract clauses that allow for a contract to be revisited if a key subcontractor changes, which may affect critical entity services. For more information, refer to the <i>FFIEC IT Handbook's</i> "Outsourcing Technology Services" booklet.
Audit	"Right to audit" clause allowing for periodic audits of critical third parties' operations. Periodic audits help validate that third-party service providers comply with the agreement's control terms such as the entity's information security requirements.
Continuing vendor support	Clause regarding system and component support including upgrading, patching, and bug fixing through EOL. The clause should include a minimum time frame for notification of the EOL date.

Appropriate entity personnel should be involved in contract drafting to help ensure that contracts cover all relevant aspects of the development, acquisition, and maintenance of the entity's systems, components, and services, including those that are customized for the examined entity. Contracts should contain such details as performance specifications, source code accessibility, software and data security, and hardware viability and replacement. Contracts should identify the recourse available to the entity if the vendor fails to meet defined requirements and user acceptance criteria. For more information, refer to the *FFIEC IT Handbook's* ["Outsourcing Technology Services"](#) booklet.

Before opening negotiations or issuing an RFP for customized systems and components, management should define objectives and understand the entity's present and planned IT

²³⁴ Refer to [GLBA](#) further implemented by FFIEC members as follows: FDIC: 12 CFR 364, appendix B, ["Interagency Guidelines Establishing Information Security Standards,"](#) and 12 CFR 364, supplement A to appendix B, ["Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice";](#) FRB: Regulation H, 12 CFR 208, appendix D-2, ["Interagency Guidelines Establishing Information Security Standards,"](#) and Regulation Y, 12 CFR 225, appendix F, ["Interagency Guidelines Establishing Information Security Standards";](#) NCUA: 12 CFR 748, appendix A, ["Guidelines for Safeguarding Member Information";](#) OCC: 12 CFR 30, appendix B, ["Interagency Guidelines Establishing Information Security Standards,"](#) (especially the requirement under Section III, D.2, for national banks and federal savings associations to "[r]equire its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines").

²³⁵ Refer to FTC 16 CFR 314, ["Standards for Safeguarding Customer Information."](#)

architecture, infrastructure, and operations. During contract negotiation, entity management may encounter situations in which third parties cannot or will not agree to the terms an entity sets out in the draft contract. Under such circumstances, management should determine whether it is willing to accept or can mitigate the risks related to systems or components without the requested terms. Any accepted risk or compensating control factors should be clearly documented with appropriate approval consistent with the entity's policies and governance structure. If management cannot accept or mitigate the risk, it is important to consider alternative solutions. After contract negotiation or agreement execution, periodic audits help to verify that the third party is meeting its contractual responsibilities, such as agreed-on security controls and compliance with laws and regulations.

When negotiating contracts or agreements, management should anticipate that it may decide to convert to different products or providers in the future. Contracts or agreements should enable and facilitate conversions (e.g., minimize restrictions or provide appropriate assistance) to new systems or components. For example, when converting to a different product at the same provider, management and the provider should facilitate coordination between the old and new product teams and entity personnel should be aware of any differences among the products (e.g., hardware, interfacing software, and storage). Additionally, clauses should provide the ability to convert data to a new format as needed. Finally, if converting to a new provider, clauses that allow the old and new providers to coordinate in the conversion process may mitigate conversion related issues (e.g., incompatibility, integration problems, or lack of data availability).

VI.E.5 Escrowed Source Code Agreements and Documentation

Programs are written using proprietary or open-source code. Proprietary systems and components are normally copyrighted trade secrets of the company that wrote or owns the programs. Generally, to protect the integrity of code and software copyrights, vendors do not release proprietary code to the entities that buy or lease the products. Typically, an independent third-party escrow agent retains the source code and related documentation in escrow;²³⁶ however, entity management is responsible for verifying annually that the third party maintains a current version of the source code in escrow. Some escrow agents provide services for reviewing and confirming source code version numbers and dates. Some agents perform automated code reviews to confirm integrity of the escrowed code.

The documentation held by the escrow agent should include system narratives, system flowcharts, program source listings, program narratives, file and record layouts, descriptions of individual fields in the records, and calculation routines. Portions of this documentation may be included with the user guides that are provided to the entity. These documents should cover transaction codes and descriptions of input forms and output reports. In addition, management should consider protecting the entity's escrow rights by contractually requiring third parties to inform the entity if the software vendor pledges the software as loan collateral. It is important to consider the risks associated with a foreign-based escrow agreement.

²³⁶ *Merriam-Webster* defines "[escrow](#)" as "a deed, a bond, money, or a piece of property held in trust by a third party to be turned over to the grantee only on fulfillment of a condition." For purposes of this booklet, the code in escrow is held by a third party and provided to the entity only on the fulfillment of some condition.

Effective escrow agreement provisions may include the following:

- Requirements to include minimum code documentation with the code in escrow.
- System and component maintenance procedure documentation to be escrowed.
- Conditions that should be present before an entity can access the source code and related documentation.
- Assurances that the escrow agent will hold current versions of the source code and related documentation to validate that escrowed information is updated whenever significant program changes are made.
- Arrangements for auditing or testing escrowed code integrity.
- Source code descriptions and related documentation including the storage type and location (e.g., magnetic tape or cloud).
- Assurances that the source code storage type and location and related documentation is accessible, operable, and compatible with an entity's existing IT environment.
- Assurances that the source code can be compiled into executable code.
- If the escrow agent is based outside the United States, consideration of the practical and legal implications of establishing foreign-based escrow arrangements.

VI.E.6 Exit Strategy

An exit strategy is an entity's plan for transitioning to a replacement system, component, or service, or for terminating a system, component, or service. Entities design exit strategies to minimize disruption. Having a well-defined exit strategy is part of ongoing, effective strategic planning. During the procurement process, management should develop an exit strategy that at a minimum addresses the third party not meeting the contract terms.

To have the most leverage, entity personnel should negotiate default and termination language in the initial contract. The default and termination language may provide opportunities or methods to remedy contract defaults. Contract clauses should define termination rights; document time frames for transferring services to another third party or bringing the service in-house; and provide for how data, records, and IT assets are preserved, transferred, or destroyed.

Default and termination language may provide for the initial steps in executing an exit strategy, but it is important to consider identifying alternative third parties that provide similar products and services at the onset of the relationship. This could provide management with an initial plan to execute a transition between third parties. For more information on exit strategy planning, refer to the *FFIEC IT Handbook's* "[Management](#)," "[Outsourcing Technology Services](#)," and "[Business Continuity Management](#)" booklets.

VII MAINTENANCE

Action Summary

Management should establish policies, standards, and procedures for maintaining systems and components that include detailed roles and responsibilities. It is important that policies and procedures effectively ensure the availability and continued operability of systems and components.

Examiners should review the following:

- System and component inventory adequacy for key information (e.g., to facilitate the entity identifying and addressing vulnerabilities).
- Maintenance plans, including maintenance schedules and logs, vendor and developer recommendations, cost-benefit analyses, operational risk assessments, and qualified staffing adequacy.
- Change management processes, including change types, authorizations, and related risk assessments.
- Security monitoring reports (e.g., anomalous activity).
- Configuration management practices to validate appropriate implementation and enforcement of established change processes.
- Vulnerability and threat identification processes, including remediation plans.
- Any maintenance-related reports to the board of directors and senior management.
- IT asset inventory, including considerations for EOL, such as planned obsolescence and planning for upgrades to legacy systems and components.
- Termination, disposal, and off-boarding processes of systems, components, and change in third-party relationships.
- Maintenance documentation for any system, component, and configuration updates.

The maintenance²³⁷ and operations²³⁸ SDLC activities are necessary whether systems and components have been developed internally or by a third party. They include the routine servicing and periodic modification of everything needed for a system or component to run correctly including the network, hardware, system software, databases, and the related documentation. An entity's maintenance policies and procedures should include maintenance roles and responsibilities (which may include third-party roles and responsibilities), maintenance access policy (internal and remote), and maintenance monitoring and auditing mechanisms.

²³⁷ As noted in the FFIEC Glossary, "[maintenance](#)" is "any act that either prevents the failure or malfunction of equipment or restores its operating capability."

²³⁸ As noted in the FFIEC Glossary, "[operations](#)" are "the performance of activities comprising methods, principles, processes, procedures, and services that support business functions." IT operations include the tactical management of technology assets and daily delivery of services to capture, transmit, process, and store transactions and information that support the entity's overall business processes.

Well-managed modifications can improve a system's or component's functionality, confidentiality, integrity, availability, and resilience. Periodic modifications may address user functional requirements, correct security vulnerabilities, enhance performance, or increase storage.

An accurate and complete IT asset inventory, including system and component maintenance, is central to ITAM. For example, an inventory that contains system and component versions and patch levels allows an entity to quickly determine how a newly discovered vulnerability affects the organization. Another use of the IT asset inventory is to determine which systems are affected by components reaching their EOL. IT asset inventories should include IoT products.²³⁹ For more information on ITAM, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" booklet.

VII.A Preventive Maintenance

Preventive maintenance is the activity to proactively address situations that may cause issues or disruptions. For example, an entity may review a system's storage utilization periodically to determine whether storage is adequate to prevent related outages.

Management should establish a preventive maintenance plan, especially for mission-critical systems and components. When developing the preventive maintenance schedule, it is important to consider system or component criticality, developer maintenance recommendations, operational risks, and other relevant factors (e.g., emerging technologies and threats). These maintenance plans should be aligned with business plans. Appropriate entity personnel schedule maintenance activities during time frames that minimize the risk of interruption to business processes such as after business hours, during weekends, and during holidays.

System and component access for maintenance activities should be limited to only that part of the system needed to perform the maintenance and only for the time necessary to conduct the maintenance activity. Capturing and reviewing maintenance activity logs minimizes the risk that malicious activity occurs during a maintenance window.

For more information, refer to the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)" booklet.

VII.B Change Management

Change management encompasses the planning, governance (including approvals), testing, and implementation of any form of change. Examples of changes that are important to manage are configuration changes, software patches, and functional changes.

A key piece of change management is change control, further explained in the "[Implementing Changes](#)" section of this booklet. Changes may be necessary for a variety of reasons, including

²³⁹ For more information, refer to NIST IR 8425, [Profile of the IoT Core Baseline for Consumer IoT Products](#), and NIST IR 8259A, [IoT Device Cybersecurity Capability Core Baseline](#).

updates or modifications to systems or components, requests from users, and results from vulnerability scans or penetration tests. The speed with which these changes should be implemented varies. For example, configuration changes or software patches that address a newly discovered vulnerability in a critical system should be completed quickly, while changes to improve user functionality in a low criticality system may have a slower implementation time frame.

The complexity and, in some cases, the system's or component's age may determine the type and frequency of changes needed to maintain the system or component. A system that is complex and contains multiple components may need to be changed more frequently than a simple system that is less reliant on multiple components. Similarly, a system or component that is new may experience more changes when it is initially placed into a production environment versus a system or component that has existed in a production environment for many years. Additionally, systems and components used by large groups may involve more frequent changes to meet the needs of a greater number of users.

Management should be aware of and manage the risks associated with unauthorized, untested, and unplanned changes. These risks include breach of confidentiality, breach of integrity (e.g., accidental configuration errors), lack of availability (e.g., system failure resulting from an inappropriate change or not implementing a change), or lack of resilience. Appropriate processes should be followed to manage changes (e.g., configuration management, vulnerability management, and patch management) regardless of whether the system or component was developed internally.

- Configuration management:** Configuration management policies, standards, and procedures for developed and procured systems and components should be established, and validation performed to ensure that they are followed. The policies, standards, and procedures should include the identification and the use of system and component baseline configurations²⁴⁰ (or original versions). The policies, standards, and procedures should specify that management evaluates, approves, documents, and disseminates changes to baseline configurations. Automated tools may simplify and promote consistency throughout the process. As previously stated, effective management helps ensure that changes to the configuration follow an established change management process. For more information, refer to the *FFIEC IT Handbook's* "[Information Security](#)" and "[Architecture, Infrastructure, and Operations](#)" booklets.
- Vulnerability management:** Sources of vulnerability information (e.g., including threat intelligence) for the entity's systems and components should be identified. These sources may include the vendor, supplier, or developer, public-private information-sharing partnerships (e.g., the Financial Services Information Sharing and Analysis Center [FS-

²⁴⁰ NIST defines "[baseline configuration](#)" as "the documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures."

ISAC]²⁴¹ and NIST National Vulnerability Database²⁴²), and internal and external testing. Entity personnel should remediate relevant vulnerabilities and address threats continually and efficiently. The criticality of the identified vulnerability and the affected system or component can dictate the timing of the remediation. Appropriate senior leadership should review vulnerability management results, such as whether the most severe vulnerabilities are remediated within appropriate time frames, as specified in policy. Open or unresolved vulnerabilities in an entity's systems and components could result in loss of confidentiality, integrity, availability, and resilience.

- **Patch management:** Patch management processes are a critical part of an entity's effective change management practices. The entity's patch management processes should include procedures for identifying, evaluating, approving, testing, installing, and documenting patches or updates for systems and components. Regardless of whether the systems or components are developed internally or by a third party, it is critical to have a process for the timing, prioritization, testing, and deployment of patches to minimize the potential of vulnerability exploits that may result in system compromise or service disruption. Reasons for not applying patches should be documented and periodically reviewed by appropriate personnel, independent of the decision to not apply the patch. These processes help mitigate the risk that unaddressed vulnerabilities exist in systems and components and lead to system compromise. For more information, refer to the *FFIEC IT Handbook's* "[Information Security](#)," "[Architecture, Infrastructure, and Operations](#)," and "[Audit](#)" booklets.

VII.B.2 Implementing Changes

Action Summary

Management should have a process for the request, decision, approval or rejection, test, and implementation of changes. The goal of the change process should always be system or component confidentiality, integrity, availability, and resilience.

Examiners should review the following:

- Change management policies and procedures.
- Change logs.
- Relevant access controls.
- Processes for controlling system and software versions.
- Sample change documentation (e.g., change requests and approvals), including risk assessments.
- Change management program training.
- Conversion plans and coordination with conversion partners and stakeholders.

²⁴¹ FS-ISAC is an industry consortium dedicated to reducing cyber risk in the global financial system.

²⁴² NIST's [National Vulnerability Database](#) is the U.S. government's repository of standards-based vulnerability management data represented using the Security Content Automation Protocol. These data enable automation of vulnerability management, security measurement, and compliance. The database includes security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

The process of implementing changes is sometimes referred to as change control. This process helps ensure that IT-related modifications are appropriately authorized, tested, documented, implemented, and monitored. Effective change control processes help management ensure that patches, updates, and configuration changes will not adversely affect a system, component, or application on the network. The characteristics and risks of a system, activity, or change should dictate the formality of the change control process. Management should maintain policies, standards, and procedures that specify the change control process, including defined roles and responsibilities. Examples of key roles with associated responsibilities are the project sponsor, change manager, quality manager, information security manager, auditor, network and system administrators, user support, and users.

A change manager is responsible for managing all changes affecting the entity to realize the intended improvements with minimal or no disruptions to operations. A group of stakeholders can aid the change manager in the assessment, prioritization, and scheduling of changes. Examples of this type of group include change advisory boards and change control review boards, which often consist of representatives from all areas in the entity's IT department, affected business lines, and third parties. This individual or group should develop communication protocols to ensure that all affected stakeholders are notified of changes.

Management should prioritize and categorize changes. Changes may be prioritized based on entity requirements (e.g., IT and information security); resources required; and legal, regulatory, and contractual reasons for the change. Change requests may be categorized as rejected, approved, or closed. Prioritizing focuses the organization on completion of the most important changes first. Categorizing changes helps the entity monitor change management performance. Therefore, appropriate change performance metrics and reports should be established.

Effective management has a method to track and report changes (e.g., standard change request forms, library and version controls, and spreadsheets or automated change logs). A change control tracking and reporting process, which may be manual or automated, gives management information about the number, priority, and status of change requests, allowing management to make informed decisions and adjustments as necessary. Maintaining and reviewing detailed change logs is critical for any change control processes. The absence of sound controls and adequate documentation of implemented changes can cause problems when designated personnel install subsequent system changes. Without adequate documentation and controls, personnel will not have the necessary information and may make a change that has an adverse effect on operations.

Effective management follows a defined change control process to make routine and planned changes to systems or components, adjust configuration settings, and make changes to remediate flaws. Management should also account for emergency and unscheduled changes in the change control process. When planning the change, effective management prepares for unexpected problems or failures with the change by creating a back-out plan and documenting the steps taken during the change in the order they occurred. This allows management to back out of a change partially if not all systems and components are affected. Generally, a change control process consists of defined steps, which may address the following:

- **Request:** The change request should include details of the change (e.g., system or component to be changed, description of the change, and justification); impact analysis to identify security needs, risks, and affected systems; change time frame; and back-out plan.
- **Review:** Stakeholders review change requests to determine their viability and business practicality.²⁴³ If reviewers approve a change request, they also prioritize it based on the system's criticality, type of change, interdependencies and interconnections with the involved system, and duration of the change (i.e., time the involved system may be offline or degraded).
- **Approval:** An appropriate level of management, sometimes in collaboration with personnel or a committee, should determine approval of change decisions. Documentation of the decision and approval depends on the type of change initiated. Entity personnel should decide on changes in a timely manner (i.e., in advance of the change). Standard processes may not be followed in emergency situations. However, emergency changes should still be documented, even if after the fact. Emergency change processes should include a list of personnel approved to authorize emergency changes. All changes should be captured through the change control tracking and reporting process.
- **Design and build:** The developer (both internal and external) designs and builds the change to fulfill a request. When completed, the developer provides the requested change to the team or individual responsible for testing.
- **Test:** The team tests the proposed change independently for security, functionality, and any potential adverse effects of the change. Testing should verify that the change performs as intended, identifies any flaws (e.g., integrity issues), and that the change integrates with other systems as intended. Patches and updates that are deployed without testing may have unintended consequences (e.g., deployment delays and operational disruptions) and result in change rollback. Testing should be documented so that testing policy and procedure implementation may be audited.
- **Implementation:** Before deploying a change, an implementation plan (i.e., steps to deploy the change) should be created, full copy of the current production version backed up, and the back-out plan finalized. The team should deploy the approved change according to the implementation plan, preferably during off-peak hours or planned system downtime to minimize the system's or component's time offline.
- **Verify and close:** After implementation, management should perform a post-implementation review to verify that the change was deployed according to the implementation plan and functions appropriately. A comparison of modified programs with change authorization documents serves to validate that only approved changes were implemented. After verification, effective management follows processes to document completion of the change and close the change request. After closing, management should report on the status of the change and monitor the implemented change for unintended issues.

Security is critical when implementing changes for different systems or functions, such as network and client-server environments, mainframes, operating and application programs, and development and procurement projects. To help ensure that modifications do not adversely affect the security posture of varying systems, effective management integrates security into its change

²⁴³ The review may be performed by IT management and stakeholders (e.g., system owner, technical staff, or financial personnel). The reviewers may form a formal committee (e.g., IT steering or operations) depending on the proposed change's scope, costs, risks, impact, and implementation time frame.

control processes. Failure to include information security considerations when implementing changes can result in operational disruptions, degradation in a system's performance, or inappropriate security controls in the system. A change impact analysis can help entity personnel determine the extent to which a change to a system or component may affect its operational, security, and compliance posture. Inaccurately assessing a change's effect could increase the likelihood of an operational disruption or a threat exploiting a vulnerability at the entity.

An impact analysis is completed before the entity makes a final decision regarding the change in the case of a planned change, or after implementation in the case of emergency changes. For a significant change, post-implementation reviews should identify any material impacts that were not anticipated, especially if there were any adverse effects on confidentiality, integrity, availability, resilience, or compliance.

VII.B.3 Additional Control Considerations in Change Management

VII.B.2(a) *Data Controls in the Testing Environment*

Use of production data in test environments should be accompanied by appropriate controls. Some entities have a testing environment that allows the testing of patches, updates, and fixes in a nonproduction environment that is similar or identical to the production environment, including the same configurations and data sets. Use of a test environment that matches the production environment raises the probability that testing will be effective in identifying flaws. If production data is copied into the test environment, it should be protected as if it were in the production environment. Another option is for an entity to generate synthetic data²⁴⁴ for use in the test environment instead of using production data. Additionally, the testing environment should be isolated and otherwise protected to avoid it being a vulnerable exploit vector.

VII.B.2(b) *Library Controls*

Effective management strictly controls the movement of programs and files among development, quality management, and production libraries²⁴⁵ for purposes of change control. Libraries allow programmers to access frequently used routines²⁴⁶ and add them to programs without having to rewrite code. Libraries include executable code modules that run as part of larger applications. Inappropriate segregation of duties between development staff and non-development staff who manage the libraries can lead to production system defects, or the introduction of malicious programs, which in turn can negatively affect system confidentiality, integrity, availability, or resilience.

²⁴⁴ According to NIST Glossary, "[synthetic data generation](#)" is "a process in which seed data are used to create artificial data that have some of the statistical characteristics of the seed data."

²⁴⁵ In computing, the term "libraries" refers to collections of stored documentation, programs, and data typically segregated by the type of stored information, such as development, testing, and production-related programs, data, or documentation, and arranged for quick identification and reuse. Program libraries include reusable program routines or modules stored in source or object code formats.

²⁴⁶ For purposes of this discussion, a "[routine](#)" is defined as "a sequence of computer instructions for performing a particular task."

Assigning librarian functions to independent personnel (e.g., quality management personnel in more complex entities or non-operations personnel in less complex entities) reduces the risk of errant or malicious code being moved to production environments. Additionally, independent program integrity verification, library activity logs, and documented approval processes also mitigate this risk. These controls should ensure that code in libraries is not altered or deleted. Additional library controls, to mitigate these risks include the following:

- **Object grouping and associated access controls:** Rather than establishing controls on individual objects in libraries, which can create security administration burden, entity personnel or automated programs group similar objects (e.g., executable and nonexecutable routines, test data, and production data) into libraries based on object type. Access can then be granted at library levels.
- **Role-based, automated library applications:** When feasible, the implementation of role-based, automated library applications can help management by restricting access at library or object levels. Additionally, such applications can produce reports that identify who accessed a library and what, if any, changes were made.

Effective management considers using these automated change controls commensurate with the complexity of the entity's IT environment and the number, types, and complexities of changes in that environment. Regardless of whether the entity has automated change control tools, management should strictly control access to production software libraries, particularly in distributed environments.

VII.B.2(c) *Code Repository Controls*

Code²⁴⁷ can be stored in repositories.²⁴⁸ They are used in the process of development and configuration management. Through version-control features, code repositories help management track and control different versions of developed source code and program documentation during development, as well as deployment scripts and configuration files. Code repositories may be hosted in-house, on third-party platforms, or on publicly available collaboration venues.

Management should establish code repository use policies. The policies should specify which code repositories the entity uses and where code repository data actually resides, especially for any cloud-based repositories (e.g., public, private, and community clouds). Effective policies and practices include the following actions:

- Prohibiting, when appropriate, the use of any public-based forums, especially if using a private account for entity business or data use.
- Establishing source code ownership.

²⁴⁷ Code types include source code, executable code, and configuration-as-code.

²⁴⁸ Repositories are locations where assets may be stored in no certain order. Repositories may contain assets such as libraries, data, and code.

- Requiring business account use to manage entity repository data and correspondingly prohibiting personal account use.
- Prohibiting entity credential use (e.g., email address, password) when creating personal repository accounts.
- Controlling and tracking entity accounts for personnel if cloud repositories are authorized.
- Prohibiting posting entity-owned code in open (i.e., public) forums.
- Evaluating security and other repository risks before using them.
 - Using available security measures, such as MFA.
 - Auditing to determine that all repository-suggested practices, including security measures, are appropriately adopted.
 - Ensuring sanitization of data, if applicable.
 - Restricting exfiltration of code to personal accounts.
- Implementing technical or logical controls (e.g., data loss prevention filters) to block sensitive data from being published to unapproved repositories.
- Searching open (i.e., public) code repositories for entity-owned source code for unauthorized posting of company-owned source code.

Code repositories can be used to manage software changes. For example, code repositories often have built-in version control functionality. Version control tools can be used to manage both software code and associated documentation. Lack of version control can result in updates to the wrong code version and inappropriate access to code. Additionally, inconsistency in code location and naming convention can result in development and maintenance inefficiency. Therefore, available version control features should be used to track changes made to the code and to increase individual accountability for changes.²⁴⁹

Another important security control for code repositories is access control. To prevent unauthorized access to or modification of code, access to code repositories should be role-based, follow the principle of least privilege, and limit access to authorized personnel, tools, and services. Management may consider authorization strategies (e.g., zero trust) to mitigate risk. The following are examples of effective access controls:

- Request and approval processes for access to code repositories (e.g., development, staging, or production).
- MFA requirement for access to all (internal and cloud-based) code repositories.
- Appropriate segregation of duties to prevent developer access to the staging and production code repositories, prevent quality management personnel from having access to production code repositories, and grant access to production code repositories only to release management personnel.
- Periodic review processes for access roles and repository logs.

²⁴⁹ Refer to NIST SP 800-218, [*Secure Software Development Framework \(SSDF\) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*](#).

The entity's continuity planning should include code repository backup to facilitate recovery when the development, staging, or production environments are disrupted. Additional information related to the principles and concepts discussed in this section is available in the *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)," "[Information Security](#)," "[Management](#)," and "[Audit](#)" booklets.

VII.B.4 Change Types

There are several change or modification types that can be controlled through use of a defined change process. The change types are routine or planned modifications, major modifications, and emergency modifications. Effective management has procedures for changes that include change request, review, and approval that direct management to plan, test, and document changes before implementation. Regardless of the change type, management should ensure that changes to any IT system, component, or service are supported by an orderly, adaptable, documented, and measurable process to promote the consistent implementation of changes as well as provide an audit trail for changes. This gives management the necessary information for resilience purposes (e.g., specific rebuild point) or if there are problems when implementing the change (e.g., specific back-out procedures).

VII.B.3(a) *Routine Modifications*

Routine or planned modifications include changes to systems or components to improve performance, add functionality, enhance usability, address defects, improve security, or comply with a new law or regulation. Sometimes referred to as standard changes, routine modifications can be simple or complex but are not considered major and generally can be implemented during the normal course of business. Routine modifications follow repeatable procedures and are often implemented with automation. They include patches, version updates, and firewall changes. They also may include replacing or upgrading network hardware (e.g., printers, user computers, and networking devices). Defined implementation plans, which often include using automated deployment tools to deploy the modifications, are important especially when changes are implemented over numerous systems or components, or across widely dispersed networks.

Effective management plans and coordinates routine modifications because IT changes often affect multiple business lines. Change management discussions should involve sufficient representation from lines of business, IT, information security, quality management, and audit. It is important for involved personnel to receive training to ensure that changes support entity objectives and do not adversely affect confidentiality, integrity, availability, and resilience. Centralized oversight (e.g., through a committee) helps to manage the interdependencies of the entity's systems and operations. Committees providing oversight help clarify request requirements set by the entity and help ensure that all departments are aware of pending changes. Change management discussions to coordinate change activities may happen using specialized change control committees (e.g., CCB) or less formally through management discussions (e.g., during IT steering committee meetings).

After completing a routine modification, all systems and components should be backed up to an off-site location, secured, and maintained to ensure adequate confidentiality, integrity,

availability, and resilience. Management should have an inventory of changes, including routine modifications, for back-out, resilience, and tracking purposes.

VII.B.3(b) *Major Modifications*

Major modifications include significant functional modifications to an existing system, conversion to a new system, or introduction of new systems, components, or data because of corporate mergers or acquisitions. In some cases, these may be referred to as “normal” changes as they are common but more complex than routine changes. These changes rely on extensive planning and additional management oversight as they often are longer-term; affect more of the entity’s systems, components, departments, and personnel; and incur higher cost. Major modifications should be implemented by adhering to a structured change management process, as noted in the “[Implementing Changes](#)” section of this booklet; however, some changes may need to go through the SDLC, particularly if there is any significant development activity. The goal of this process is to minimize risk, promote integrity and security, and maintain uninterrupted delivery of the service during and after a significant modification is implemented.

Entity personnel should assess risks related to major modification and all security-related changes. Key stakeholders should formally discuss these major modification requests and associated risks identified before approving the requests. Major modification policies and procedures should specify the decision criteria, accounting for requirements, feasibility, cost, project planning, software design, programming, testing, and implementation.

Entity personnel should determine the training required to make the conversion or major hardware and software upgrade successful. Training may start with ensuring that the major modification is adequately documented (e.g., new system information, user manuals, updates made to the system, and training information). Users affected by the changes should receive appropriate communication and training. Additionally, evaluation of the type, volume, and timing of training needs for each affected line of business and coordinate training programs with applicable third parties should be performed.

System conversions (and associated deconversions) are a major modification subset. A system conversion is a major change to an existing system and may involve migrating the system from one platform type to another (e.g., from on-premises to a cloud environment, or from one core provider to another). System conversions occur because of the introduction of new systems or corporate mergers and acquisitions. Changes to the foundation of the core platform may have additional effects throughout an entity’s operations, resulting in increased risk. Therefore, strong conversion controls (including documented conversion plans, adherence to entity change management processes, and comprehensive management oversight) are critical to prevent data corruption, performance degradation, and operational disruption. An improperly planned and executed conversion can disrupt the business and create inefficiencies, internal and external user dissatisfaction, and accounting problems, resulting in customer dissatisfaction and customer loss.

Successful conversions rely on a comprehensive analysis of a conversion’s impact on existing operations (e.g., business processes and associated data processing, storage, and communication requirements), while accounting for interdependencies. Effective conversion policies, standards,

and procedures should include provisions for internal and external communication channels, appropriate reporting, and lines of authority for timely decision-making and issue resolution. Elements such as the following should be considered when planning a conversion:

- **Conversion team:** The conversion team should include stakeholders with knowledge of the interdependencies of the system being converted and ability to articulate how the new system solves issues or improves outcomes.
- **Strategic fit:** The new system should meet as many of the entity's strategic and business objectives as possible (to limit the need for additional products or add-ons).
- **Integration:** The new system should integrate with existing systems and components. This often involves using internal APIs to securely connect to internal systems across lines of business and using external APIs to securely connect with the entity's third parties (e.g., cloud providers, fintechs,²⁵⁰ third-party developers, partners, and customers).
- **Business intelligence:** The new system should enable comprehensive data analysis to support daily business activities and customer relationship management.
- **Ease of use:** The new system should be easily navigable and intuitive for entity personnel, which can improve workflow efficiency even if workflow efficiency was not an objective.
- **Evolution:** The new system should efficiently support evolving functional needs, changing technologies (e.g., evolution from on-premises to a cloud environment, artificial intelligence [AI], and quantum computing), and increasing capacity needs.
- **Compliance:** The new system should meet the entity's regulatory and internal policy requirements.
- **Security:** The new system should meet the entity's enterprise-wide information and cybersecurity requirements (e.g., security protocols, cyberattack monitoring, and resilience).
- **Training:** New system training should be available in a variety of formats (e.g., prerecorded, in-person, and virtual) and for a variety of users (e.g., end users and administrators).
- **Remote work flexibility:** An important variable to consider is whether the solution supports entity personnel remote work.
- **Conversion plans:** A key factor in conversion plans is ensuring the capability of personnel to map existing entity systems and components to the new system, to identify interdependencies, and to transfer data to the new systems. Additionally, an after-action review of the conversion can be useful for minimizing potential issues in future conversions.
- **Support:** Third parties should be able to support the conversion and provide ongoing support to the entity after the conversion.
- **Cloud:** Cloud-based solutions should meet applicable compliance requirements, include technology support, and integrate with the entity's existing systems and components.

Reference checking with a conversion partner's other clients can be helpful to learn the lessons from their conversions and improve the entity's conversion plan.

VII.B.3(c) *Emergency Modifications*

Emergency modifications correct severe and unexpected problems with systems and components

²⁵⁰ As previously stated, for purposes of this booklet, the term "fintech" refers to using technology in novel ways to provide financial services.

and minimize operational disruptions after an incident. Examples of situations that may require emergency modifications include the following:²⁵¹

- Natural disasters (e.g., floods, earthquakes, and storms) that disrupt critical facilities (e.g., data center outages and building evacuations for extended periods).
- Loss of a critical vendor or other supply chain component (e.g., cloud vendor, network vendor, telecom provider, electricity provider, and water system).
- IT incidents (e.g., denial of service attacks, malware, and network cable cuts).
- Emergency security patches released by vendors.
- Zero-day vulnerabilities that require timely configuration or other changes to mitigate risk until a patch can be developed, tested, and installed.

Entities that plan for emergency modifications are better able to limit negative effects on their business when situations like the above occur. To plan for emergency modifications, entities' policies, standards, and procedures should address expected emergency steps, such as the following:

- Specify who can declare an emergency.
- Designate a group (e.g., emergency change control review board) that can meet on extremely short notice to evaluate and approve proposed emergency modifications. The group could include senior leadership, critical line-of-business management, and key IT management.
- Create an emergency modification plan that includes a list of individuals in the emergency group (e.g., emergency change control review board) with contact information, and the procedures that are modified from standard change control and security processes to enable quick action.
- Plan for multiple methods of communication (e.g., in-person, phone, text, email, and collaboration site) in case the emergency occurs outside normal business hours, or a method is unavailable or insecure.
- Identify the responsible parties for enacting emergency changes and plan for their continuity.
- Compress certain phases of the implementation process to save time and still test, model, or simulate²⁵² before releasing the changes into the production environment. Any unwarranted delays in patching increases the risk that malicious actors or malware can exploit unpatched systems. For more information on exploits, refer to the *FFIEC IT Handbook's* "[Information Security](#)" booklet. Methods for reducing deployment time include the following:
 - Reducing the number of use cases addressed in testing and modeling, as well as planning to remediate issues with specific use cases.
 - Performing smaller scale testing in the modeling environment, such as deploying patches to 10 test machines instead of 50 or 500.

²⁵¹ Refer to CISA's [CRR Supplemental Resource Guide, Vol. 3: Configuration and Change Management, Version 1.1](#), and [CRR Supplemental Resource Guide, Vol. 5: Incident Management, Version 1.1](#).

²⁵² In computing, "modeling" or "[simulation](#)" is defined by *Merriam-Webster* as "the imitative representation of the functioning of one system or process by means of the functioning of another."

- Maintaining a list of users who have the authority and access rights to easily acclimate to emergency changes and can communicate temporary remediation tactics to their peers.
- Establish emergency minimum recovery point objectives with stakeholders to reduce the time required to perform system backups.
- Establish emergency downtime procedures (e.g., failover to alternate systems) that allow systems to be taken completely offline in emergencies. This helps minimize the need for outages and reboots in times of heavy use and expedites change completion.
- Perform periodic emergency drills in the test and modeling environment to prepare IT staff to deal with the stress of emergency modifications. Review the results of these drills and adjust emergency modification plans accordingly.

As identified above, testing emergency modifications before deployment is preferable to minimize potential disruptions. Effective management weighs the potential damage from an untested emergency change against the known damage from the subject issue to determine the level of testing required. Because testing is likely to be shortened, it is even more critical in emergency situations to have backup files and programs available and to establish a back-out plan before emergency modifications are implemented. Appropriate backups, established back-out plans and procedures, and detailed documentation provide the ability to reverse a change if it disrupts the system.

The number of emergency modifications should be kept to a minimum, and management should validate every emergency modification after implementation to determine whether it was correctly classified. Control should be maintained over personnel attempting to circumvent routine modification or major modification control processes by incorrectly classifying changes as emergencies to avoid resource constraints (e.g., time, personnel, and cost).

Detailed documentation enhances management's ability to analyze the effect of the emergency modification during a post-implementation review and verify that the change was deployed appropriately. Evaluations and documentation reviews of emergency modifications should be completed as soon as possible after implementation. Findings from these evaluations and reviews are used to improve existing change control policies, standards, and procedures.

For more information, refer to the *FFIEC IT Handbook's* "[Business Continuity Management](#)," "[Architecture, Infrastructure, and Operations](#)," "[Information Security](#)," and "[Management](#)" booklets.

VII.B.5 Change Management Documentation

Documentation related to changes allows management to analyze changes over time, learn lessons from those changes, and the effect of those changes on the entity's systems and components. Documentation of all changes (e.g., configuration changes, patches applied, system conversions, and emergency modifications) and their impact on systems and components should be maintained. Some examples of change-related documentation are covered in the following subsections.

VII.B.4(a) *Change Request Form*

Entities use change request forms to communicate the specifics of the change to all stakeholders for analysis purposes after the change is completed. The forms should provide a clear description of the requested changes as well as sufficient information for affected parties to understand the effect of a change. Change requests typically include elements such as the following:²⁵³

- Change request title.
- Change control identification number.
- Requestor's name.
- Request date.
- Detailed description of the change, including system, component, or configuration item involved.
- Proposed date and time of the change.
- Stakeholder groups affected.
- Business justification for the change.
- Resources (e.g., personnel, expertise, cost, and time) needed to implement the change.
- Expected impact of the change.
- Expected impact on resilience requirements for the asset.
- Backup procedures.
- Rollback (or back-out) procedures.
- Change urgency (e.g., low, medium, high, or emergency; and scheduled, urgent, or unscheduled).
- If the change is an emergency, justification for emergency change.
- Change control review board input, such as the following:
 - Preliminary assessment of change.
 - Decision (e.g., approved, rejected, more information required, or deferred) and further action if not approved.
 - Comments.
 - Authorized approver's signature and date.

VII.B.4(b) *Impact Analysis*

Documented impact analyses assist in communicating the effect of a change on the entity's information security. The impact analysis is generally maintained with and may be presented

²⁵³ Refer to CISA's [CRR Supplemental Resource Guide, Vol. 3: Configuration and Change Management, Version 1.1](#), and [CRR Supplemental Resource Guide, Vol. 5: Incident Management, Version 1.1](#). Also refer to NIST SP 800-128, [Guide for Security-Focused Configuration Management of Information Systems](#).

with the change request to serve as supporting information for decision purposes. The impact analysis typically includes elements such as the following:²⁵⁴

- Change request title.
- Change control identification number.
- Requestor's name.
- Request date.
- Analyst performing the impact analysis.
- Technical implications, such as other systems or components affected by the change or interface and integration issues (including with third parties).
- Functional impact, such as required changes to existing applications.
- Schedule impact.
- Financial impact, such as funding required to implement the change.
- People impact, such as end users, customers, expertise, and training.
- Security impact, including information security, cybersecurity, and physical security.
- Resilience impact.
- Entity risks from this change.
- Rollback (or back-out) implications.
- Alternatives to change and impact of not making the change.
- Authorized approval signature and date of approval.

VII.B.4(c) *Rollback or Back-Out Plan*

When implementing changes, there is always the potential that the deployment does not go as planned. When issues arise after a change, it may be necessary to rollback (or revert) to a prior version or level or back out a change and restore a system to its earlier state. Entity personnel should prepare for the possibility of a failed or incomplete deployment and have a plan with procedures to address the issues. Entity personnel should develop a rollback or back-out plan to reverse a failed deployment.

A rollback or back-out plan identifies the steps necessary for restoration to a previous secure and functional version of the baseline configuration.²⁵⁵ This plan can help an entity recover from a system or component update that is not functioning correctly. The plan can explain what to do (e.g., shut down, failover, or replace) if a service or component fails and how to resume secure operations on a redundant system while still providing uninterrupted service to end users. Entity personnel should consider the time required to perform rollback procedures and when to trigger the rollback plan. Entity personnel should establish rollback plan timing that minimizes business disruption.

Change implementation failures or incomplete changes can cause expensive damage to systems and components. One effective plan step is to minimize damage by identifying a stable recovery

²⁵⁴ Refer to CISA's [CRR Supplemental Resource Guide, Vol. 3: Configuration and Change Management, Version 1.1](#), and [CRR Supplemental Resource Guide, Vol. 5: Incident Management, Version 1.1](#). Also refer to NIST SP 800-128, [Guide for Security-Focused Configuration Management of Information Systems](#).

²⁵⁵ Refer to NIST SP 800-128, [Guide for Security-Focused Configuration Management of Information Systems](#).

point and archiving or imaging the system or component at that point. Entity personnel would develop and test related rollback procedures and identify spare systems and components (e.g., power supplies, system motherboards, hard drives, and communication switchboards) that may be needed, consistent with the criticality of the system or component. The entity documents the stable recovery point so multiple personnel can participate and view the same information during rollback (e.g., hardware, software, firmware, configuration files, and other configuration records).

It is important to control rollback tools because an unauthorized rollback could allow an attacker to restore a system or component to a prior vulnerable image, which in turn could allow the attacker to corrupt the system or component or inject malware. Effective management has appropriate security controls to prevent unauthorized rollback. The entity may have a special update process (e.g., physical presence of personnel) for rolling back the installed systems and components to an earlier version. This mechanism provides a dual control for management to guard against attackers using automation to install old systems and components with known vulnerabilities.

Effective management tracks and reports issues that lead to the use of a back-out plan and the effects of a failed or incomplete change deployment. Documentation of failed or incomplete deployments should include lessons learned for future change implementations.

VII.C End-of-Life

With respect to technology, EOL is a time frame usually defined by a technology vendor to describe when an asset has reached the end of its useful life cycle and when the vendor will no longer maintain and support the asset or continue to sell or license it. This is also applicable to a service provided in support of purchased IT assets. When the vendor no longer updates or plans to sunset services that support the IT asset or discontinues the sale of licensing of support services, this form of EOL is considered “end-of-service.”²⁵⁶ If the IT asset was created in-house, EOL occurs when the entity has decided to no longer update and otherwise maintain it.

A vendor generally determines the useful life of the IT assets it sells. The vendor identifies when it will stop providing updates and communicates a timeline along which it will sunset the systems and components. Entity personnel who purchase IT assets from vendors should evaluate the expected life of the IT asset as part of their due diligence. EOL considerations should occur as part of the initial contract negotiation and at contract renewal and be specified in the resulting contract. For example, the contract should contain a clause specifying the amount of advanced notice the vendor will provide the entity before it discontinues updates and other support of the IT asset. This notification is critical to the entity in planning replacements (including migrations from the legacy system to the replacement), and in planning for the off-boarding of the IT asset. Therefore, management should have a process to determine EOL decisions (e.g., replace, upgrade, or migrate to a new system) before a system’s or component’s EOL.

²⁵⁶ System, component, and service providers sometimes use the term “end-of-service” to indicate when maintenance services and updates will no longer be supported or provided.

If developed internally, the entity should plan for system or component obsolescence. Management, development staff, and users may have input into the system's or component's useful life timeline. If a system or component no longer meets users' needs, or maintenance costs are too high, management may conclude that the system or component has reached EOL and should be replaced.

The entity's IT asset inventory should have information about the useful life of IT assets in order for the entity to plan for orderly transitions from one system or component to another. An effective ITAM process includes monitoring each IT asset's depreciation and obsolescence schedule and planning well in advance for EOL. Items to consider in the process include the party responsible for development, version, patch levels (available and currently deployed), and the system's or component's expected life. An entity may leverage existing tools (e.g., depreciation schedule and IT asset inventory) to facilitate obsolescence planning and ensure that replacement resources have been provided for.

An IT asset that is obsolete and at EOL or end-of-service may be more vulnerable to exploitation; therefore, this risk should be managed to maintain confidentiality, integrity, availability, and resilience. With older and less resilient IT assets, an increased number of security vulnerabilities may result in greater risk of intrusion and exploitation (e.g., malware, ransomware, and data breaches). The potential impacts from these risks increases for interconnected systems and components because of the number and types of access points. These risks also exist for components provided by all parties in the supply chain. Continuously assessing the risks of using aging, outdated, and unsupported systems and components is the foundation for mitigating the risks. Effective risk mitigations include the following:

- Replacing systems and component in a timely manner.
- Establishing processes for vendors to notify the entity of component EOL status changes (e.g., end-of-production, end-of-service).
- Extending support from the vendor.²⁵⁷
- Adding or augmenting system or component controls:
 - Segregating the system or component from the network until it can be replaced or removed.
 - Locking down system or component devices and ports for access.
 - Increasing access controls and monitoring.
 - Minimizing connections to the system or component.

Management should consider EOL risks tied to maintaining legacy systems and components for extended periods of time. When continuing to use legacy systems, management should consider weaknesses related to the design, development, manufacturing, production, shipping and receiving, delivery, and operation of the system and component that can be exploited at EOL by

²⁵⁷ Third-party providers often charge additional fees to continue providing updates after a system's or component's EOL. Extending support beyond EOL may result in risks, such as operating systems and components with compounded vulnerabilities and diminishing availability of expertise.

a threat source.²⁵⁸ These legacy-related risks are two-fold. If management continues to use legacy systems or components, management puts its supply chain partners at risk; and if the entity's supply chain partners continue to operate legacy or unsupported systems or components, the entity may be at risk for EOL or end-of-support vulnerabilities. Effective management addresses EOL and the use of legacy systems and components and time frames for necessary replacement, upgrade, or migration in contracts between the entity and its supply chain partners.

For more information on ITAM and EOL, refer to *FFIEC IT Handbook's* "[Architecture, Infrastructure, and Operations](#)," "[Information Security](#)," "[Outsourcing Technology Services](#)," "[Business Continuity Management](#)," and "[Management](#)" booklets.

VII.D Termination and Disposal

When a system or component becomes obsolete, is no longer supported, no longer meets the users' or entity's needs, or becomes too costly to maintain, management may decide to terminate its use and dispose of the system or component. Effective management has appropriate termination and off-boarding procedures. The procedures should identify who has the responsibility to decide whether to terminate a vendor relationship, as well as an approval and acknowledgment process in which contracted parties agree to the relationship termination. Effective management negotiates contract clauses that specify termination criteria, including related to fourth or nth party relationships (e.g., affiliates, subcontractors) if necessary. It is important that the termination clauses address confidentiality, integrity, availability, and resilience of data and operations throughout the off-boarding process.

There are several important considerations when terminating a system, component, or service including disposing of decommissioned systems and components, and safely migrating and disposing of data and documentation. Data are particularly important when being transferred to a new replacement system to maintain confidentiality, integrity, availability, and resilience. Effective management has procedures for activities such as the following:

- Shutdown (i.e., sunset) of the systems and components.
- Identification of the tasks involved.
- Data identification and preservation (i.e., archival or transfer) or disposal.
- Secure disposal of unnecessary systems and components (e.g., hardware and software).

Effective management validates that appropriate personnel are aware of the procedures to coordinate the orderly disposition of the system, its components, and the data.²⁵⁹ The entity's critical or sensitive data and documents should be removed (e.g., wiped, sanitized, or otherwise destroyed) logically and physically from the system and components before disposal. This extends to any data or documents maintained by the third party on behalf of the entity, and effective management addresses the entity's requirements in the contract termination and disposal clauses.

²⁵⁸ Refer to "[CISA Insights – Cyber: Remediate Vulnerabilities for Internet-Accessible Systems](#)."

²⁵⁹ Refer to U.S. Department of Justice's *Systems Development Life Cycle Guidance Document*, chapter 12, "[Disposition Phase](#)."

VII.E Maintenance Documentation

Maintenance documentation provides valuable descriptions for the upkeep of an entity's systems and components and significantly enhances management's ability to maintain, operate, and administer IT assets. The larger and more dispersed an entity, the greater role documentation plays in effective maintenance across the entity. Advantages of documentation for users include access to operation manuals, training materials, and online application help features.

Documentation enhances IT personnel's ability to maintain and update systems efficiently, track updates to the systems and components, and identify and correct programming defects.

Developing and maintaining current and accurate maintenance documentation can be complicated, time-consuming, and expensive. However, maintaining standardized documentation and indexing procedures are important to help ensure the uniform accessibility of existing maintenance documentation. Authorized personnel should update the documentation with system, component, and configuration updates according to the entity's or third party's prescribed standards, as applicable. Effective management works with third parties to help ensure that the entity receives current system, component, and user maintenance documentation.

APPENDIX A: EXAMINATION PROCEDURES

Examination Objectives

Examiners should use these procedures (also referred to as the work program) intended to help them determine the quality and effectiveness of the entity's management of IT, particularly regarding development, acquisition, and maintenance-related risks as outlined in this booklet. Examiners should use these procedures to measure the adequacy of the entity's ITRM process, including management awareness and participation, risk assessment, policies, standards, and procedures, reporting, ongoing monitoring, and follow-up.

Examiners may choose to use only particular examination procedure work steps based on the size, complexity, and nature of the entity's business.

Objective 1: Determine the appropriate scope and objectives for the examination.

1. Review past reports for outstanding issues or previous problems. Consider the following:
 - a. Regulatory reports of examination.
 - b. Internal and external audit reports (e.g., SSAE18).
 - c. Internal or independent tests or reviews of controls (e.g., penetration tests, vulnerability assessments, SOC reports, business continuity reviews, and third-party management reviews).
 - d. Regulatory and audit reports on service providers.
2. Review management's response to issues raised during, or since, the last examination. Consider the following:
 - a. Adequacy and timing of corrective action.
 - b. Resolution of root causes rather than just specific issues.
 - c. Existence of any outstanding issues.
 - d. Whether management has taken positive action toward correcting exceptions reported in audit and examination reports.
 - e. Independent review of resolution and reporting of resolution to the audit committee.
3. Interview management and review responses to pre-examination information requests to identify changes to the technology infrastructure or new products and services that might increase the entity's risk. Consider the following:
 - a. Any significant strategic or business line changes, including any third-party changes.
 - b. Products or services delivered to either internal or external users.
 - c. Current network diagrams and data flow diagrams, including changes to configuration or components.
 - d. Hardware and software inventories.
 - e. Loss or addition of key personnel.
 - f. Inventories of third-party providers and software vendors, including services provided.

- g. Organizational charts that include reporting relationships between business units and control functions (e.g., enterprise risk management, ITRM, and internal audit).
- h. Credit or operating losses primarily attributable (or thought to be attributable) to IT (e.g., system problems, inadequate controls, improperly implemented changes to systems, and fraud resulting from cybersecurity attacks, such as account takeover).
- i. Changes to internal business processes.
- j. Internal reorganizations.

Objective 2: Management establishes, and the board of directors (board) oversees, an effective governance structure that includes development, acquisition, and maintenance activities. Additionally, the board oversees related IT project management processes used to manage projects related to those activities. (Section II, [“Governance of Development, Acquisition, and Maintenance”](#))

Review the following documents to understand the overall structure and hierarchy of management and oversight activities related to development, acquisition, and maintenance:

- Enterprise-wide IT policies, procedures, and standards describing the entity’s requirements throughout the development, acquisition, and maintenance life cycle.
 - Charters (e.g., board, management, or committee), organizational charts, relevant documentation, and practices to determine whether appropriate roles and responsibilities are identified and assigned with suitable decision-making authority.
 - Project plans and meeting minutes of the board and committees to ensure that activities and projects align with the entity’s strategic objectives and the board’s risk appetite.
 - Project audit reports to determine whether the audit function provides independent, objective assurance of the effectiveness of an entity’s development, acquisition, and maintenance activities.
 - Documentation of controls for personnel with access to program code to limit placement into the production environment.
 - QA reports to evaluate processes for the detection of potential coding errors.
1. Determine whether the board and senior management provides for the following:
- a. An effective governance structure that allows for the effective oversight and management of the development, acquisition, and maintenance of the entity’s systems and components.
 - b. Oversight of development, acquisition, and maintenance IT project management processes and projects related to those activities.
 - c. Oversight of significant projects to ensure that they align with an entity’s strategic plans.
 - d. Consideration of business strategies and objectives, resilience needs, information security requirements, legal and regulatory requirements, and allocation of resources (e.g., personnel, budget, and time) when evaluating IT projects and activities.
 - e. Consideration of the needs of internal and external stakeholders when making decisions regarding IT development, acquisition, and maintenance activities.

- f. Establishment of audit's role in reviewing development, acquisition, and maintenance activities, and ability to raise objections if they believe the control environment is inadequate.
2. Determine whether the board and senior management develops and implements comprehensive, entity-wide IT policies, procedures, and standards addressing entity requirements throughout the development, acquisition, and maintenance life cycle. Does the board, senior management, and designated committees of the board perform the following:
 - a. Regularly review and approve IT policies and standards.
 - b. Review and approve procedures to meet changing IT policies and standards.
 - c. Provide for policies that clearly delineate development, acquisition, and maintenance responsibilities and provide for communication to all personnel, stakeholders, and appropriate third parties.
 - d. Review and approve deviations from policies, standards, and procedures related to development, acquisition, and maintenance.
 - e. Identify and assign appropriate roles and responsibilities for the entity's development, acquisition, and maintenance activities.
 - f. Identify and address training needs to support development, acquisition, and maintenance responsibilities.
 - g. Provide for an escalation process for development, acquisition, and maintenance issues.
3. Determine whether the board and senior management identified and provided for key management responsibilities related to development, acquisition, and maintenance activities. Examples of key roles which carry those responsibilities include the following:
 - a. Board and senior management.
 - b. CIO.
 - c. CISO.
 - d. IT steering committee.
 - e. Business line management.
4. Determine whether management identified and provided for the responsibilities of IT project management related to development, acquisition, and maintenance activities. Examples of key project management roles that carry those responsibilities include the following:
 - a. Sponsor.
 - b. Project owners.
 - c. Product owner.
 - d. Project or program manager.
 - e. Business change manager.
 - f. Program management office or organization personnel.
 - g. Stakeholders.

5. Determine whether management identified and provided for the responsibilities of key roles in development activities. Examples of key development roles that carry those responsibilities include the following:
 - a. Network architects.
 - b. Developers.
 - c. Software engineers.
 - d. Hardware engineers.
 - e. Information security analysts.
 - f. Systems analysts.
6. Determine whether management identified and provided for the responsibilities of key roles in acquisition activities, including examples such as procurement manager or third-party risk manager.
7. Determine whether maintenance personnel provide for appropriate maintenance throughout the life cycle of systems and components. Determine whether maintenance personnel
 - a. Have knowledge and understanding of all relevant systems and components they are expected to operate and maintain.
 - b. Analyze and understand the costs of maintenance (e.g., budget, time, or personnel) versus the costs of not performing maintenance (e.g., system failures, data breaches, and customer dissatisfaction).
 - c. Track the analysis of costs for reporting to management.
 - d. Maintain independence from development roles to prevent developers from accessing production environments.
8. Evaluate audit's role in reviewing development, acquisition, and maintenance activities. Consider the following audit activities:
 - a. Validating that sufficient time is built into project schedules to define controls and verify that all appropriate stakeholders are involved.
 - b. Determining the effectiveness of controls necessary in the entity's development, acquisition, and maintenance activities and recommending appropriate mitigation.
 - c. Guiding developers in considering appropriate control standards and frameworks throughout IT projects.
 - d. Reviewing the internal controls, testing, and audit trails included in systems and components during each SDLC phase.
 - e. Performing post-implementation reviews shortly after implementation of new or revised systems or components.

Objective 3: Evaluate whether management implements continuous risk management processes within the entity's development, acquisition, and maintenance activities to identify reasonably foreseeable internal and external risks and threats, including those that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information

or customer information systems. (Section III, “[Risk Management of Development, Acquisition, and Maintenance](#)”)

1. Examiners should review management’s continuous risk management processes for development, acquisition, and maintenance. Consider the following:
 - a. Policies, standards, and procedures for identifying, measuring, mitigating, monitoring, and reporting risks related to development, acquisition, and maintenance activities.
 - b. Documented processes and metrics used to measure the level of risk.
 - c. Detailed documentation of processes used to review, accept, and document risks that management cannot mitigate or transfer.
 - d. Documentation of risk assessment processes to identify key risks at the onset of IT projects and throughout their life cycles.
 - e. Risk assessments that highlight internal and external risks related to development, acquisition, and maintenance activities.
 - f. Documentation of ongoing processes and reports to monitor and communicate risk, including emerging risks related to development, acquisition, and maintenance activities.
 - g. Reports to stakeholders that are timely, accurate, and include clear, relevant metrics.

2. Evaluate whether management has identified reasonably foreseeable internal and external risks and threats, including those that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. Consider management’s risk management actions in addressing the following:
 - a. Risks that could result in a severe disruption or material compromise to critical service delivery.
 - b. Policies, standards, and procedures for identifying, measuring, mitigating, monitoring, and reporting risks related to development, acquisition, and maintenance activities.
 - c. Repeatable process adoption, to ensure that risks are consistently addressed across the entity over time.
 - d. Risk identification and assessments involving stakeholders with business process knowledge who may be affected by the development, acquisition, or maintenance activities or the related IT projects.
 - e. Threat model usage commensurate with the overall threats to the entity, to assess appropriateness of security policies, standards, and procedures.
 - f. Process to review, accept, and document risk when management cannot mitigate or transfer risk, and its acceptance by the board.
 - g. Regular review and approval of risk acceptance decisions consistent with the entity’s governance structure.
 - h. Information security concerns.

3. Determine whether management has established effective risk measurement, monitoring, and reporting processes, including for emerging risks. Consider the following:
 - a. Implementation of effective standards to measure risk in the entity's development, acquisition, and maintenance activities.
 - b. Establishment of an ongoing risk measurement process, commensurate with the size and complexity of the entity's activities.
 - c. Communication of technical aspects through reports to the board that are clear and understandable to board members (e.g., explaining acronyms or technical jargon) and that relate IT issues to business concerns.
 - d. Receipt of reports on IT project risks, such as critical projects that may miss key milestone dates, identification of negative test results, or changes to business or technical requirements.

Objective 4: Evaluate whether management has implemented effective risk mitigation throughout development, acquisition, and maintenance activities regardless of the phase of the project in the life cycle and agnostic as to the type of technology. Specific risks and controls should be considered depending on management's chosen solution. (Section IV, "[Common Development, Acquisition, and Maintenance Risk Topics](#)")

For this objective, examiners should review and assess the following:

- Systems, components, and services, including related contracts and licenses, throughout the supply chain for appropriate risk identification and mitigation.
- Secure coding standards, configurations, and security controls used to harden each system or component, data, and activity logs for appropriate processes and implementation and maintenance of confidentiality, integrity, and availability.
- Inventory of all systems, components (e.g., open-source, proprietary, APIs, and container images and registries), including related licenses, and data as part of ITAM.
- Processes for access controls, authorization, and authentication for systems and components, data, and related documentation throughout the supply chain to ensure appropriate security.
- Roles and responsibilities to evaluate segregation of duties in and ongoing management commitment to development, acquisition, and maintenance activities.
- Process of selecting and implementing methodologies to enable effective management and control of development, acquisition, or maintenance projects and alignment with entity objectives.
- Operating parameters (e.g., timing, speed, throughput, and data validation) for systems and components to determine performance.
- Activity logs related to systems, components, and data to identify operating risks.
- Monitoring processes of development and maintenance activity for identification of anomalies and unauthorized access or modification to systems, components, and data.
- Reporting processes for decision-making and measuring the level of project success.
- Training on development, acquisition, and maintenance concepts (e.g., methodologies); effectiveness of training; and capability of personnel to implement concepts learned.
- Documentation of internally developed programs and externally procured products and services to effectively operate and maintain the systems and components.

- Evaluation process (e.g., post-implementation review, stakeholder interview, problem documentation and resolution, cost-benefit analysis, and reports to senior management) for development, acquisition, and maintenance projects.
1. Evaluate management's oversight of use of open-source and COTS components. Consider the following:
 - a. Identification and mitigation of risks related to the use of open-source components.
 - b. Evaluation of documentation providing support if there are open-source components supporting any line of business.
 - c. Proactive maintenance of updated application and user documentation, especially when code changes are made.
 - d. Consultation with third-party providers and vendors regarding recommended security controls to harden the COTS solution.
 - e. Mitigation of risks related to integration (e.g., lack of interoperability or integration between systems and components).
 2. Evaluate management's ability to negotiate, administer, and implement practices regarding licenses, agreements, and copyright protection. Consider whether management
 - a. Accurately assesses current and future needs and ensures that licenses continue to meet the entity's needs.
 - b. Reviews licenses, obtaining confirmation that they clearly state whether system or component usage is exclusive, the number of user licenses, and whether there are any time, place, manner, or other types of limitations with the system or component's use.
 - c. Specifies in its agreements the appropriate time periods for all licenses and the minimum amount of notice required for license termination.
 - d. Periodically reviews system and component licenses to compare all installed licensed systems and components with the respective license terms.
 - e. Determines whether a third-party vendor provides access to source or object code ("code") when drafting agreements.
 - f. Reviews licenses to determine whether they include retention and use of backup copies of any mission-critical system or component on which the entity may rely for disaster recovery or business continuity purposes at remote sites.
 - g. Negotiates, when possible, with licensors to ensure the inclusion of retention and use of backup copies if they are omitted from the terms of a license.
 - h. Understands any resulting limitations and consequent risks if involved in difficult license agreement negotiations, including when an entity has limited negotiating power.
 - i. Periodically reviews system and component licenses to compare all installed licensed systems and components with the respective license terms.
 - j. Considers what is stated in the licenses; costs of obtaining them; and risks, fines, and other compliance liabilities for violating their provisions or requirements.
 - k. Includes related entities (e.g., subsidiaries or contractors) as users in their licenses when the entity plans to provide the systems or components to them.

- l. Implements appropriate licenses for the systems or components developed when management is responsible for developing systems and components and providing them to other entities or its subsidiaries.
 - m. Maintains awareness of the liabilities that come with licensing activities, including considerations related to hardware maintenance, integration, compatibility, and fraud, when the entity builds hardware and licenses that hardware to other entities.
 - n. Specifies in its agreements the appropriate time periods for all licenses and the minimum amount of notice required for license termination.
 - o. Addresses inappropriate usage if there is a discrepancy between actual usage and the total number of installed licenses allowed by the agreement.
 - p. Addresses maintenance agreements, which outline available maintenance services (e.g., provision of new versions, releases, or updates).
 - q. Obtains appropriate vendor permission and participation for modifications to the code for systems and components.
 - r. Ensures that the agreement addresses and prompts updates to application and user documentation when any changes are made to procured systems or components.
3. Assess whether management's ITAM program includes oversight and management of the software and hardware licenses for components used by the entity. Consider management
 - a. Awareness of the liabilities that come with licensing activities, including considerations related to software maintenance, integration, compatibility, and fraud if an entity develops software and licenses that software to others.
 - b. Maintenance of an accurate inventory of FOSS as part of an effective ITAM process and understanding of and abiding by the requirements of FOSS licenses.
 - c. Awareness of what information is shared when contributing in return to the FOSS development community.
 - d. Maintenance of program provisions for identification and management of any hardware licenses.
4. Evaluate management's oversight of copyright protections. Consider management's actions
 - a. When deploying procured systems or components for use in the entity's infrastructure, including physical and virtual networks.
 - b. When reviewing and approving the procurement and use of systems or components in the entity's IT environment to ensure appropriate use.
5. Assess management's actions to promote secure development practices for products and services developed and used. Consider management's actions to
 - a. Monitor third parties' activities to enforce conformance with the entity's contract requirements, Information Security Standards, and legal and regulatory requirements when management outsources development to third parties.
 - b. Evaluate or have a method to evaluate the third party's secure coding standards (e.g., through independent certification or audit) when acquiring systems and components.

- c. Determine that secure development standards apply to the development of any system or component changes (e.g., patches or updates) for the maintenance of systems and components.
 - d. Incorporate security in the code, and implement quality management, which is critical to the secure development process.
 - e. Determine that the embedded rules of the code review tools are appropriately configured and used if an automated code review process is implemented.
 - f. Maintain a secure operating environment throughout development, acquisition, and maintenance activities, promoting secure development practices whether operations are performed in-house by entity personnel or outsourced to a third party.
6. Assess management's actions to securely manage data. Consider management's actions to
 - a. Identify the data, their characteristics (e.g., customer sensitive information or proprietary information), and sensitivity (e.g., confidential, internal use only, or public).
 - b. Document the data in an inventory that includes locations and uses of data in development, acquisition, and maintenance activities and in IT projects.
 - c. Include data security in development, acquisition, and maintenance activities.
 - d. Provide appropriate data confidentiality, integrity, availability, and resilience procedures for data input and output, including the use of data in IT projects.
7. Assess management of microservices activities related to development, acquisition, and maintenance. Consider the following management actions:
 - a. Setting parameters for the processes of registration to and deregistration from the service registry.
 - b. Implementation options that meet the entity's security requirements.
 - c. Implementation and management of microservices-based architectures, including monitoring of the many services, which may be running on different servers or written in different languages.
 - d. Consideration of the following monitoring controls:
 - Monitoring at the gateway and service level.
 - Implementing a centralized dashboard to display the status of multiple services and network segments.
 - Creating a baseline and implementing intrusion detection to provide alerts on deviations from the baseline.
8. Assess management's consideration of risk in the use of containers, such as image risk, registry risk, orchestrator risk, container risk, and host OS risk, and effective countermeasures to risk. Consider management actions to address data isolation when setting up containers.

9. Evaluate management's risk mitigation strategies for API activities. Consider the following:
 - a. Configuration of the API with the necessary infrastructure services.
 - b. Application of extra layers of security beyond those for standard end-point security, and implementation of appropriate authorization checks at the object level.
 - c. Implementation of appropriate security, patches, updates for APIs, and disabling of unnecessary functions.
 - d. Appropriate setting of all API processing parameters (e.g., execution timeouts, maximum allocatable memory, number of file descriptors, number of processes, request size, number of requests per client or resource, and number of records per page to return in a single request response).
 - e. Verification that all access is denied by default and employ specific role-based permissions for users to gain access to functions.
 - f. Denial of access to properties unnecessary for the user's role, and access only allowed when necessary.
 - g. Validation and filtering of all data coming to an API with appropriate parameters.
 - h. Maintenance of logging of API activity (e.g., authentication, errors, redirects, rate limiting, and end points, including their parameters, requests, and responses).
 - i. Implementation of continuous logging and monitoring of relevant API activity (e.g., failed authentication attempts, denied access, and input validation errors).
 - j. Maintenance of secure logs and ensuring only appropriate access to them to maintain confidentiality and integrity of sensitive data in activity logs.
10. Assess management's implementation and use of any methodologies for project management. Consider management actions
 - a. Establishing appropriate methodologies to enable effective management and control of system and component development, acquisition, and maintenance activities.
 - b. Aligning implementation of any methodology with the overall strategic and business objectives.
 - c. Promoting effective planning through IT project management and support training for developers, quality management members, testers, and maintenance personnel.
 - d. Considering the risk of not following established control procedures when using prototyping models.
 - e. Considering security development process weaknesses when using agile methodologies and determining appropriate mitigation strategies.
11. Evaluate quality management actions. Consider
 - a. Implementation of compensating controls when they cannot fully achieve segregation of duties between quality management and development roles.
 - b. Provision of adequate support for projects throughout an entity to promote success of a project.

12. Assess documentation standards. Consider management's process for
 - a. Maintenance of documentation for internally developed programs and externally procured products and services.
 - b. Maintenance of necessary information and documentation to understand and convey how a system or component was developed, how it functions, and where appropriate security and resilience points are included.
 - c. Maintenance of detailed documentation for each system and component in development and production.
 - d. Implementation of established policies to prepare documentation before deployment and additionally when appropriate, such as when management makes changes.
 - e. Obtaining documentation from the third party and incorporating it into the entity's own stored documentation for acquired systems and components.
 - f. Validating before purchase (through an internal review or a third-party certification) that a procured system's documentation meets the entity's documentation needs and standards.

13. Assess management's post-implementation review processes. Consider effective evaluation of development, acquisition, and maintenance projects and management actions, such as
 - a. Conducting post-implementation reviews at the end of a project to validate completion of project objectives and assess development activities.
 - b. Interviewing key stakeholders actively involved in the operational use of a product to determine effectiveness of the completed project.
 - c. Documenting and addressing any identified problems to improve future projects and remediate issues in current projects.
 - d. Analyzing effectiveness of project management activities by comparing, among other things, planned and actual costs, benefits, risks, return on investment information, and development time frames.
 - e. Documenting results and presenting them to senior management and determining who should be informed of any operational or project management deficiencies.

Objective 5: Evaluate whether management has developed and followed consistent processes to identify risks and oversee IT projects to address any risks identified. IT projects should be managed according to the size and complexity of the entity and its project characteristics and risks. (Section IV.N "[IT Project Management](#)")

For this objective, examiners should review and assess

- Project plans, proposals, and status reports to determine whether the IT project manager works with stakeholders (e.g., PMO) to oversee and carry out IT projects.
- Board and committee minutes to evaluate whether management reviews and prioritizes projects and whether it considers the project's effect on operations and the entity's needs.

- Project plans, project requests, and documentation standards to determine whether they are structured appropriately to clearly define the project purpose, entity's requirements, and include deliverables for each project phase to address business needs.
 - Documentation of management approvals of any addition or modification of functional, security, or control features and demonstration that changes are aligned with the project charter and project plan.
 - Testing and quality management plans used to validate that the project meets the entity's project goals and stakeholder requirements.
 - Documentation for the closeout of the entity's IT projects.
1. Assess whether management develops and follows consistent processes to identify risks and oversee IT projects to address any risks identified. Consider whether management
 - a. Establishes project management policies, standards, and procedures that apply enterprise-wide.
 - b. Develops and follows consistent processes to identify risks and oversee IT projects to address any risks identified.
 - c. Considers the project's effect on operations and the entity's needs (e.g., IT, information security, lines of business, customer needs, and regulatory and legal compliance) when reviewing and prioritizing projects.
 - d. Performs analysis of system or component needs for a given project.
 - e. Monitors changes for any addition or modification of functional, security, or control features to help ensure that these changes are approved and aligned with the project charter and project plan.
 - f. Develops and executes testing plans, which validate whether the entity's project goals and stakeholder requirements are met.
 - g. Maintains comprehensive and accurate documentation reflecting the testing methodology employed, actual tests performed, and test results throughout the testing process.
 - h. Implements quality management (also may be referred to as QA and QC) processes to help ensure that project requirements are met and validated.
 - i. Defines and maintains the required elements for documentation of the closeout of the entity's IT projects.
 - j. Establishes standards and maintains appropriate documentation for IT projects to foster a consistent and accurate process across projects.
 - k. Maintains processes for developing IT project plans that describe existing system benefits and weaknesses and explain project objectives.

Objective 6: Evaluate whether management has an SDLC to manage systems and system components throughout their life cycle; to achieve the objectives of confidentiality, integrity, availability, and resilience; and to meet the entity's business objectives. (Section IV.O "[System Development Life Cycle](#)")

For this objective, examiners should review and assess

- The documented management and control processes for development.

- Description and detail of entity SDLC-related controls, including for supply chain partners.
 - Responsibility and accountability assignment.
 - Key stakeholder involvement.
 - Clear evidence of stakeholder communication and tracking of all SDLC phases and actions.
1. Assess management's oversight of the SDLC process. Consider management's implementation of a documented process, such as an SDLC, used to manage and control development activities, if the entity engages in internal development activities.
 2. Evaluate management's maintenance of protections (e.g., information security and resilience) in the information systems, components, and networks for data in transit and at rest, including for the entity's and supply chain partners' information, through all phases of the SDLC.

Objective 7: Evaluate whether management implements effective processes to address the plans and actions needed in each phase of an IT project, as part of the SDLC. (Section IV.O.1 [“SDLC Phases”](#))

For this objective, examiners should review and assess the activities associated with the entity's SDLC phases, such as the following example phases:

Initiation Phase

- Description of the project's purpose, expected benefits, support for entity business objectives, and any legal and regulatory requirements.
- Plans for addressing additional costs, resource needs, and alternate solutions.
- Validation of initial impact analysis, including any baseline security concerns.
- Documentation of the project proposal for all stakeholders in the supply chain.

Development or Acquisition Phase

- Documentation of design specifications.
- Documentation of mitigation strategies for risks identified in the impact analysis.
- Risk assessments, baseline controls design, and effectiveness of security controls.
- Documentation of initial development testing, conversion, implementation, and training plans, including confirmation of the functionality and controls.
- Documentation of additional design requirements and development changes.
- Documentation of draft user, operator, and maintenance manuals.

Implementation and Assessment Phase

- Documentation of design reviews and system tests, including any new specifications.
- Documentation of deployment approach selected.
- Training provided, including user and system support documentation.
- Post-implementation review, including any configuration changes.

Operations and Maintenance Phase

- Documentation of performance and controls monitoring.
- Documentation of configuration and change management controls and proposed changes.
- ITAM inventory and associated risk assessments.

Sunset and Disposal Phase

- Plans and validation measures for accessible data retrieval from archives.
 - Documentation of off-boarding procedures, including for third-party providers.
 - Documentation of a post-disposal review, including processes and lessons learned.
1. Assess management's oversight of SDLC phases. Consider whether management
 - a. Understands the SDLC phases and the actions in each phase.
 - b. Identifies the actions and assign responsibility and accountability for completing those actions.
 - c. Defines the phases that will be included in the entity's SDLC and helps ensure the completion of each phase to promote transparency and accountability for, and agreement and acceptance by, the stakeholders.
 2. Assess management's actions during the initiation phase of the SDLC. Consider management's actions to
 - a. Describe the development project's purpose, identify expected benefits, and explain how the proposed system or component supports the entity's objectives.
 - b. Address legal and regulatory requirements.
 - c. Identify alternative solutions and explain the entity's confidentiality, integrity, availability, and resilience requirements.
 - d. Consider and address any potential baseline security concerns during this phase by performing an initial impact analysis.
 - e. Address planning items, including the following:
 - Responsibilities of third-party service providers, internal audit, information security, and IT staff.
 - Established acceptance criteria for each SDLC phase.
 - Established review and approval procedures to help ensure that development teams complete all SDLC phase or independent sprint requirements before moving into subsequent phases.
 - Identify control and security features to be designed, built or acquired, and implemented.
 - Create processes for development and change management to minimize disruptions to the development process.
 - Create processes that address project methodology selection, approval authority, and risk management procedures.
 - Identify costs associated with project overhead (e.g., office space, hardware, and software used during the project) as well as soft costs in budgeting personnel expenses and outsourced activities.

- f. Consider input from all stakeholders.
 - g. Evaluate the appropriateness of each requested functional requirement.
 - h. Consider all proposals and analyze them to determine whether to develop or acquire the system or component.
3. Assess management's actions during the development or acquisition phase of the SDLC. Consider management's actions to
 - a. Determine other functionality, such as whether the configuration of the system or component (e.g., an IoT product) is possible, whether the system or component can be restored to a secure default setting, and whether there are restrictions on users or services that can make changes.
 - b. Consider the results of the impact analysis performed in the SDLC initiation phase and review those results throughout the SDLC.
 - c. Address or mitigate concerns from the impact analysis or new concerns that present risk beyond the board's risk appetite.
 - d. Conduct a risk assessment and use the results to design baseline controls to meet the entity's requirements.
 - e. Build in appropriate controls, including for network interfaces, to any products the entity develops or acquires to maintain confidentiality, integrity, availability, and resilience throughout the supply chain.
 - f. Review the appropriateness of new or modified design requirements or development changes and monitor for and minimize scope creep.
4. Assess management's actions during the implementation and assessment phase of the SDLC. Consider management's actions to
 - a. Perform design reviews and system tests before implementation of the system or component to ensure that all entity specifications are met.
 - b. Perform additional acceptance tests if new features or controls are added to the system or component.
 - c. Use and document the results of the design reviews and system tests, update documentation after performing new reviews or tests, and maintain test results for future review and use.
 - d. Determine the appropriate implementation strategy for the entity and system or component being deployed.
 - e. Coordinate training logistics, including who should be trained, what the training involves, and when training should be conducted.
 - f. Organize a training and awareness campaign, and notify users of any implementation and training responsibilities.
 - g. Perform a post-implementation review once the product is implemented.
 - h. Validate the initial impact analysis during the post-implementation review and report on any changes to the results.
 - i. Confirm that the implementation occurred as planned, and determine whether there were any unanticipated effects of the change on existing controls.

- j. Validate whether configurations (e.g., security, functionality, or performance) on the new system are appropriate.
5. Assess management's actions during the operations and maintenance phase of the SDLC. Consider management's actions to
 - a. Monitor performance of a system or component to help ensure that it is consistent with pre-established user, security, and other entity requirements, and making necessary modifications.
 - b. Conduct configuration management and control activities and document any proposed or actual changes in the entity's security or operational plan of the system or component.
 - c. Assess and document changes in the entity's ITAM inventory and related risk assessments.
 - d. Follow established change management policies, standards, and procedures to minimize the potential of a modification disrupting or degrading operations.
 - e. Perform operations and maintenance phase tasks regardless of whether entity personnel or a third party performs them.
6. Assess management's actions during the sunset and disposal phase of the SDLC. Consider management's actions to
 - a. Consider the need and plan for methods for future data retrieval before archiving information and if necessary.
 - b. Maintain archived data in an accessible and readable format, adhering to data retention guidelines.
 - c. Periodically validate the accessibility of the archived data or develop a plan to migrate potentially inaccessible data to an accessible format.
 - d. Maintain confidentiality, integrity, availability, and resilience throughout this phase.
 - e. Develop comprehensive off-boarding procedures if the system or component requiring disposal is managed by, or the related data are stored by, a third party.
 - f. Perform a post-disposal review at the end of the sunset and disposal phase that details the processes and lessons learned from shutting down and archiving the terminated system or component.

Objective 8: *Evaluate management's third-party relationship risk management processes related to development, acquisition, and maintenance. (Section IV.P "[Third-Party Relationship Risk Management](#)")*

1. Assess management's due diligence practices as part of its third-party selection and relationship risk management processes. Consider whether management
 - a. Identifies and documents any limitations of its due diligence, understands the risks from such limitations, and considers alternatives regarding how to mitigate development, acquisition, and maintenance risks.
 - b. Evaluates the conclusions from supplemental due diligence efforts, such as information derived from third parties (e.g., industry utilities or consortiums,

- consultations with other organizations, or engaging in joint efforts), based on the entity's own specific circumstances and performance criteria for the activity.
- c. Involves the board, through its oversight responsibilities, to ensure awareness of—and, as appropriate, request approval or delegated approval of—contracts involving higher-risk development, acquisition, and maintenance activities.

Objective 9: *Evaluate whether management implements policies to measure, monitor, and track changes and use all related information obtained to inform SCRM activities. (Section IV.Q “[Supply Chain Considerations](#)”)*

Examiners should review

- Policies, procedures, project plans, and SDLC procedures to determine whether SCRM activities are integrated into the SDLC for the entity and applicable third parties.
 - Control configurations and reports used by management to monitor, control, and protect communications at the key access points of supply chain information systems.
 - Architectural designs, software development techniques, and systems engineering principles that promote effective information security throughout the supply chain.
 - Topologies and process flow diagrams that identify interconnectivities and potential single points of failure, while also considering continuity and resilience.
 - Inventory and validation of documentation (e.g., due diligence, including contracts) for supply chain partners, as well as documentation for provenance of systems, components, and data.
 - Communication processes and documented communication of threat intelligence and vulnerability identification with supply chain partners.
 - Management's assessment of inauthentic or unapproved systems or components (e.g., counterfeit or shadow IT).
 - SCRM controls in maintenance-related situations, including monitoring for unauthorized modifications, communicating changes, and monitoring for EOL.
1. Assess implementation of policies for tracking changes and use of the obtained information to inform the entity's SCRM activities. Consider management's actions to
 - a. Ensure that SCRM activities are integrated into the SDLC for the entity and applicable third parties.
 - b. Monitor, control, and protect communications (i.e., information transmitted or received) at key access points (e.g., external boundaries and key internal boundaries) of supply chain information systems.
 - c. Use architectural designs, software development techniques, and systems engineering principles that promote effective information security in the supply chain.
 - d. Identify potential single points of failure among all entities in the entity's supply chain numerous interconnectivities and risks from all partners.
 - e. Identify and consider any nested third-party relationships through common ownership (e.g., affiliates, subsidiaries).

- f. Identify and consider risks related to supply chains by tracking interdependencies between all parties involved (e.g., owners and third-party service providers, including vendors) in the supply chain.
 - g. Consider any information pertinent to the security, integrity, resilience, quality, trustworthiness (e.g., not on the OFAC list, other concerns), or authenticity of their supply chain partners or products.
 - h. Evaluate supply chain partners consistently, based on available information, and depending on the specific context and purpose for which the assessment is being conducted, select additional factors for consideration.
 - i. Document the reference sources for assessment information to help establish the quality of information (e.g., its relevance, completeness, and accuracy) relied on for supply chain assessments.
2. Assess supply chain risk management practices. Consider management's processes and plans to analyze policies, standards, and procedures, which outline and describe an entity and third parties' processes for SCRM (including for subcontractors). Consider activities such as the following:
 - a. Maintaining a current and accurate inventory of all applicable suppliers and identify their criticality to the business.
 - b. Considering established national and international standards, as applicable, as a baseline for security requirements for the entity's supply chain.
 - c. Assessing and addressing supply chain risks associated with a given geographic location and apply appropriate risk responses (e.g., defining acceptable locations).
 - d. Defining roles and responsibilities for personnel (e.g., development, acquisition, and maintenance) to address various supply chain activities.
 - e. Providing general controls and processes.
 - f. Developing, documenting, and maintaining an accurate inventory of third parties that reflects the entity's key supply chain partners.
 - g. Considering configuration management minimum security requirements for the supply chain.
 - h. Applying appropriate configuration management controls to its own systems and encouraging or requiring the use of comparable controls by all parties in the entity's supply chain through contracts.
 - i. Understanding and mitigating all relevant risks associated with interdependencies throughout the various supply chains potentially affecting the entity.
 - j. Planning for resilience, including scenarios related to supply chain issues.
 - k. Documenting provenance for systems, components, and data, and monitoring for changes in the chain of custody that may increase risk to the entity throughout the SDLC.
 - l. Considering provisions for excess capacity, bandwidth, and redundancy in agreements with supply chain partners, and take appropriate mitigation action, as necessary.
 - m. Considering creation of SBOM for applicable and appropriate classes of software (e.g., purchased, open-source, and in-house developed software).

- n. Validating that existing SCRM capabilities (e.g., vulnerability management practices and vendor risk assessments) are not deprioritized under the mistaken assumption that SBOM replaces these activities.
- o. Ensuring the quality of information (e.g., its relevance, completeness, and accuracy) relied on for an assessment and documenting the reference sources for assessment information.
- p. Establishing effective project management processes that can help identify critical components, especially those that are used by multiple business lines, functions, systems, and components, such as the following:
 - Determine whether there is potential foreign ownership or influence, and whether the supply chain partner may have relationships with OFAC-sanctioned individuals, organizations, or countries.
 - Evaluate supply chain partner oversight of its subcontractors (i.e., fourth parties) or developers.
 - Identify the level of open-source systems and components used by the entity, and determine how the supply chain partner demonstrates its compliance with applicable open-source licensing agreements.
 - Conduct research on COTS systems and components (e.g., via publicly available resources) or request proof to determine whether the supply chain partner (e.g., OEM) has performed testing as part of their quality or security processes.
 - Use authorized resellers or distributors with an ongoing relationship with the supply chain partner for systems and components not directly acquired from an OEM entity.
 - Acquire directly from vetted OEMs or their authorized distributors and resellers when obtaining alternative sources for continued support.
 - Track chain of custody of systems, components, and underlying code as they move throughout the supply chain to minimize the potential for counterfeit or altered products.
- q. Communicating with its supply chain partners to promote awareness of threat intelligence and relevant vulnerabilities in the entity's supply chain to inform operational security processes.
- r. Monitoring for supply chain system and component security and threat intelligence alerts and advisories from supply chain partners and taking appropriate actions in response.
- s. Considering employment of techniques to introduce randomness into entity operations and assets in the entity's systems or networks.
- t. Considering concealment techniques, such as masking metadata that may be accessible in downloads or deliveries of systems and components, whether developed or acquired.
- u. Consulting with the entity's legal counsel and board, as appropriate, regarding advanced security protection techniques (e.g., misdirection, honeypots) beyond standard industry techniques (e.g., basic randomness and concealment) techniques before implementation, as they may present liability and additional risk to the entity.
- v. Considering incident response-related information (e.g., definition of an incident, roles, and responsibilities) in its agreements with its supply chain partners.

- w. Considering correlation of available threat information with potential threats and vulnerabilities.
- x. Considering implementation of advanced monitoring over activities performed by higher-risk personnel (e.g., users with elevated authority or privileges).
- y. Considering information-sharing clauses in agreements and contracts.
- z. Performing the following when implementing maintenance processes throughout the supply chain:
 - Defining agreements that identify roles, responsibilities, and practices that may be used for maintenance activities, especially when third parties are responsible for maintaining the entity's systems or components.
 - Monitoring for unauthorized modification or removal of the entity's systems or components (e.g., use of counterfeit systems and components, malware) in the supply chain.
 - Monitoring systems and components for planning for EOL to prepare for replacement or upgrade to the systems and components.
 - Considering any potential availability issues in the supply chain for systems and components, or providing agreements to continue support for legacy systems or components until a change can be made without significant disruption to operations.
- aa. Understanding and considering interconnectivities throughout the supply chain to effectively manage supply chain risks.
- bb. Incorporating third parties into business continuity and resilience activities throughout the supply chain, when applicable.
- cc. Considering use of available information, such as that provided by third-party user groups and associations, to augment ongoing monitoring and due diligence, threat intelligence, and security throughout the supply chain.
- dd. Implementing a process to validate the effectiveness of the security of systems and components throughout the supply chain when performing development, acquisition, and maintenance activities, and make appropriate adjustments to risk assessments to account for interconnectivity risk.
- ee. Considering risk management factors in the entire life cycle of a third-party relationship, including planning, due diligence, contract negotiation, ongoing monitoring, and termination.

Objective 10: Evaluate whether management implements sound processes for the development of systems and components supporting the entity's business needs and operations. (Section V "[Development](#)")

Examiners should review the following:

- Documentation of training in secure design and coding techniques for those responsible for development activities.
- Development standards, including procedures for managing changes and a back-out plan.
- Evidence of communication throughout the supply chain regarding identification of critical systems and components, potential threats and vulnerabilities, configurations, and responsibilities for selection and maintenance of system and network components.

- Entity coding standards and list of entity-approved software development languages.
 - Documentation of security certification for completed systems and component-related code.
 - Development designs used to validate security and functionality throughout the supply chain.
 - Documentation of risk assessment related to use of or switch to a DevOps approach and effectiveness of controls.
1. Assess management's ability to provide policies, procedures, and practices to oversee and manage development activities. Consider management's actions to
 - a. Provide access to training in secure design and coding techniques to those responsible for development activities to securely design and address key issues early in the development process for entities that develop or modify their own systems and software.
 - b. Maintain and follow policies, standards, and procedures documented for developing systems and components incorporating the entity's requirements for confidentiality, integrity, availability, and resilience.
 - c. Appropriately manage risks (e.g., eliminating inaccurate techniques or outdated tools and prototypes) with use of any additional design and coding techniques beyond standard coding techniques (e.g., computer-aided design) and prototypes.
 - d. Develop, as part of the SDLC, a trustworthy system that meets specific security and other critical requirements defined and set by entity management.
 - e. Employ secure program coding practices to help develop a trustworthy system.
 - f. Incorporate supply chain processes when choosing system and network components.
 - g. Plan for maintenance activities from the outset of the development process to address secure continuity of operations.
 2. Assess management's development of standards and controls. Consider the following:
 - a. Procedures for managing changes during the development process, that address:
 - System controls.
 - Quality management.
 - Release management.
 - Documentation.
 - Reporting.
 - b. Documentation of reasons for using specific programming styles and languages on a project or service in project documentation.
 - c. Documentation of completed systems and component-related code that have passed security certification in program libraries as discussed in the "[Additional Control Considerations in Change Management](#)" section of this booklet.
 - d. Design of information systems, components, and elements to be difficult to disable (e.g., tamper-proofing techniques), and, if they are disabled, trigger notification methods such as audit trails, tamper evidence, or alarms.
 - e. Design of delivery mechanisms (e.g., downloads for software) to avoid unnecessary exposure or access to the supply chain and systems or components traversing the supply chain.

- f. Design of relevant validation mechanisms to be used during implementation and operation.
- g. Agreement with partners on standards and controls used in customized system and component development throughout the supply chain.
- h. Work with suppliers and partners to ensure that critical systems and components are identified.
- i. Validate that suppliers or the entity itself has a continued ability to maintain customized systems and components that are critical to the entity's operations.

Objective 11: Evaluate whether management maintains formal testing processes and standards to govern the effectiveness of testing internally and externally developed systems and components. (Section V.B “[Testing](#)”)

Examiners should review the following:

- Testing policies and procedures to confirm that systems and components meet the entity's requirements.
 - Testing scope documentation, including for application interoperability and discovery of vulnerabilities.
 - Documentation regarding appropriate controls and approvals over the use of production data in testing.
 - Documentation of the type of testing, testing results, corrective actions, and testing completion.
 - Documentation of testing for any new controls added to systems and components to avoid conflicts.
 - Updates to manuals and training plans after testing.
1. Assess whether management appropriately tests systems and components to identify and mitigate risks or vulnerabilities before deployment. Consider the following management actions:
 - a. Determining the need for use of production data in testing and employing appropriate controls (e.g., masking) if its use is deemed necessary.
 - b. Documenting approval of the use of nonsanitized data by the board when sanitizing data is not feasible and implementing and maintaining controls similar to those used in the production environment to appropriately protect the data for compliance with legal and regulatory requirements.
 - c. Performing additional acceptance tests of new controls if they are added to the system to help ensure that new controls meet security specifications and do not conflict with or invalidate existing controls or functionality.
 - d. Establishing a methodical process to define and conduct testing necessary to demonstrate the effectiveness of a developed system or component.
 - e. Implementing practices to document, report, and address identified issues, including security-related issues, in a timely manner, regardless of the testing methods used.
 - f. Reviewing and finalizing all supporting documentation, such as user, operator, and maintenance manuals as well as any conversion, implementation, and training plans

- associated with a new release or significant update during the implementation and assessment phase.
2. Assess management's oversight and control of DevOps and DevSecOps activities. Consider management's activities to
 - a. Assess risks involved in using or switching to a DevOps approach and implementing appropriate controls.
 - b. Consider controls to secure the CI/CD pipeline process, such as the following:
 - Hardening servers hosting code and artifact repositories.
 - Securing credentials (e.g., authorization tokens) used for accessing repositories.
 - Implementing controls on who can check in and check out artifacts in container image registries.
 - Logging all code and build update activities.
 - Sending build reports to developers and stopping further pipeline tasks when a build or test fails in the CI pipeline and configuring code repositories to automatically block all subsequent pull requests from CD or continuous deployment pipeline until issues are resolved.
 - Sending build reports to the security team and stop further pipeline tasks when a code or build audit fails.
 - Ensuring that developers can only access the application code.
 - Digitally signing (preferably multiparty digital signing) the release artifact during each required CI/CD stage during the build and release process.
 - Verifying that all required digital signatures are present during production release to ensure that no one bypasses the pipeline.
 3. Assess management's oversight of database development. Consider management's actions to
 - a. Understand the different types, structures, and uses of databases to effectively mitigate the risks of database development.
 - b. Understand the benefits, limitations, and appropriate controls for the type of database used.
 - c. Choose the appropriate database to meet business and stakeholder objectives.
 - d. Consider access needed and services (e.g., management, analysis, and data services) that the databases will provide for internal and external customers.

Objective 12: Evaluate whether management establishes acquisition processes that are commensurate with the entity's business and procurement needs and assesses and mitigates procurement risks associated with overall entity strategic, regulatory, and operational risks. (Section VI "[Acquisition](#)")

Examiners should review the following:

- Project requests and plans related to acquisition.

- Risk assessments, strategic and business plans, and due diligence activities, including meeting minutes related to the acquisition process.
 - Contracts and licensing agreements for appropriate provisions, responsibilities and accountability, and mitigation strategies.
 - Acquisition-related requests containing documented evaluation criteria and sufficient information for decision-making.
 - Documentation standards and procedures, including for updating documentation.
 - Stakeholder training and guidance in the acquisition process.
 - Audits related to the acquisition process and procurement.
1. Assess management's mitigation of the risks associated with acquisition of systems or components. Consider its actions to coordinate implementation of the following:
 - a. Ascertaining whether the product specifications are "fit for purpose" and meet the entity's requirements, (regardless of whether the entity purchases directly from OEM partners or a secondary market) and are addressed in agreements with supply chain partners.
 - b. Developing policies, standards, and procedures to effectively carry out the entity's procurement processes aligned with the entity's acquisition activities.
 - c. Performing rigorous due diligence reviews of potential suppliers.
 - d. Aligning the depth of the due diligence evaluation with the complexity, scope, and risk assigned by the risk assessment for the system or component to be procured.
 - e. Implementing contract and licensing processes.
 - f. Reviewing contracts and licensing agreements to help ensure that the rights and responsibilities of each party are clear and identify accountability.
 2. Assess management's procurement process. Consider management actions to
 - a. Develop and manage an effective IT procurement process to meet the entity's acquisition and contract fulfillment needs.
 - b. Follow a structured procurement process for any IT procurement, but particularly when procuring significant systems, components, products, and services to help ensure that each step in the process is addressed.
 - c. Ascertain that, at a minimum, procured hardware, software, and services adhere to entity standards.
 3. Assess whether management has established policies, standards, and procedures to better assist in the effective and consistent management of the entity's acquisition process. Consider management's actions to
 - a. Provide for acquisition policies, standards, and procedures that promote the
 - Definition of a process for issuing information requests (e.g., RFIs and RFPs) to third parties.
 - Performance of appropriate third-party due diligence processes.

- Negotiation of the contract to ensure that it contains terms amenable to entity management and types of IT-related provisions to consider before contract execution.
 - Establishment of processes for the entity's contract signature authority and process for specialist review (e.g., subject matter experts, key stakeholder, legal, and compliance) of IT-related contracts before approval and signature.
 - Validation of the systems, components, products, and services to ensure that they meet user requirements before acceptance.
 - Transferability or portability of systems, components, products, and services if a third-party relationship is discontinued.
 - b. Understand the following risks and their effects on the business before entering foreign-based third-party relationships:
 - Legal.
 - Country.
 - Currency (or exchange rate).
 - Geopolitical.
 - Resilience.
 - c. Identify, plan, and address the root causes of foreign-based risks or crises to minimize their effects on the entity's operations.
 - d. Plan for maintenance activities from the outset of the acquisition process to address secure continuity of operations.
- 4. Assess management's project selection process. Consider management's actions to
 - a. Consider business needs, third-party solutions, specifications, and costs.
 - b. Involve appropriate stakeholders in defining the entity's IT, information security, and functional requirements, and that the project meets applicable legal and regulatory expectations.
 - c. Identify the entity's needs to avoid a third party's confusion with a request for information and omission of critical information needed for decision-making.
 - d. Refrain from making assumptions based on third-party responses when management receives information from them, and ask follow-up questions to clarify concerns or solicit more information.
 - e. Determine when a relationship is established and a contract is created when using an RFQ.
 - f. Consult with the entity's legal counsel to identify and resolve contractual issues.
 - g. Implement a formal process for evaluating information, proposals, and quotes received from the RFIs, RFPs, and RFQs that includes key information to help management select appropriate providers.
- 5. Assess management's oversight of contracts and agreements. Consider management's actions to
 - a. Implement standards and procedures for documentation, review, and approval.
 - b. Consult with legal representation to determine the entity's rights and enforceability of terms, because agreements may not always be enforceable in a court of law.

- c. Identify each of the agreements and contracts that help management complete the evaluation and selection steps.
 - d. Validate that contracts have clauses that address relevant security and privacy standards with third-party service providers or vendors that process, store, or transmit sensitive customer data or provide critical services to meet applicable legal and regulatory requirements.
 - e. Consider providing training and guidance to support a structured approach to SOW development.
 - f. Involve appropriate personnel (e.g., relevant stakeholders) in developing an SOW and establish an appropriate senior management review and approval process.
 - g. Validate that the provider's needs and requirements (e.g., price, security, and interoperability) are met in order to provide for delivery of a quality product or service.
 - h. Establish clear and measurable expectations for the services provided, recourse when expectations are not met, and accountability for both parties if management is procuring services related to a system or component.
 - i. Link SLAs to clauses in the contract regarding incentives, penalties, and contract termination to protect the entity in the event of third-party performance failures.
 - j. Outline rights in contracts, including licenses, if applicable, when using systems and components developed by third parties.
 - k. Consider risks and address them through contract clauses (e.g., representations, warranties, and indemnifications to vendor liability limitations, information security, and agreement modifications).
 - l. Ensure that contracts have clauses that address relevant security and privacy standards with third-party service providers or vendors that process, store, or transmit sensitive customer data or provide critical services to meet applicable legal and regulatory requirements.
 - m. Consider contract clauses that allow for a contract to be revisited if a key subcontractor changes, which may affect critical services in the entity.
 - n. Determine during contract negotiation whether management is willing to accept or can mitigate the risks related to systems or components without requested terms in situations when third parties cannot or will not agree to the terms an entity sets out in the draft contract.
 - o. Document, with appropriate approvals consistent with the entity's policies and governance structure, any accepted risk or compensating control factors if third parties cannot or will not agree to the terms an entity sets out in the draft contract.
 - p. Validate that the third-party software developer's development policies and standards meet or exceed those of the entity.
 - q. Validate that third-party developers are following industry standards, at a minimum.
 - r. Negotiate terms, if possible, that would enable another third-party service provider to access an affected system or component and help management in the conversion without violating agreement restrictions.
 - s. Consider alternative solutions if management cannot accept or mitigate the risk.
6. Assess whether management has provided appropriate oversight of escrow arrangements with third parties. Consider management's actions to

- a. Validate, at least annually, that the third party maintains a current version of the source code for software in escrow.
 - b. Consider incorporating provisions into escrow agreements such as
 - Definitions of minimum programming and system and component documentation.
 - Definitions of system and component maintenance procedures.
 - Conditions that should be present before an entity can access the source code and related documentation.
 - Assurances that the escrow agent will hold current versions of the source code and related documentation to validate that escrowed information is updated whenever significant program changes are made.
 - Arrangements for auditing or testing the integrity of the escrowed code.
 - Descriptions of the source code and related documentation and the storage type or location (e.g., magnetic tape or cloud) containing it.
 - Assurances that the storage type or location containing the source code and related documentation is accessible, operable, and compatible with an entity's existing IT environment.
 - Assurances that the source code can be compiled into executable code.
 - If the escrow agent is based outside the United States, consideration of the practical and legal implications of establishing foreign-based escrow arrangements.
7. Assess management's exit strategy plan for transitioning or terminating a product, service, or third-party relationship. Consider management's actions to
- a. Help minimize disruption to an entity's operations.
 - b. Develop an initial exit strategy during the procurement process to address a situation when a third party cannot or does not meet the contract terms.
 - c. Consider identifying alternative third parties that provide similar products and services at the onset of the relationship.

Objective 13: Evaluate whether management establishes formal policies, procedures, and responsibilities for managing systems and component maintenance, and processes that ensure the availability and continued operability of systems and components. (Section VII, "[Maintenance](#)")

Examiners should review the following:

- System and component inventory for key information (e.g., version, update, and patch level) to identify and address vulnerabilities.
- Maintenance plans, including maintenance schedule and logs, vendor and developer recommendations, cost-benefit analyses, operational risks, availability of qualified personnel, and other relevant industry factors.
- Change authorizations and review any reports for identification of anomalous activity.
- Change types and risk assessment processes for those changes.

- Configuration management practices to validate appropriate implementation and enforcement of established change processes.
 - Vulnerability and threat identification processes and remediation plans.
 - Reports to board and senior management regarding maintenance issues.
 - IT asset inventory including considerations for EOL, vulnerability management, planned obsolescence, and legacy systems and components.
 - Termination, disposal, and off-boarding processes of systems, components, and third-party relationships.
 - Maintenance documentation for any system, component, and configuration updates.
1. Assess whether management provides for development of policies for the maintenance of systems and components, including remote access for performing maintenance, roles and responsibilities of personnel with access for maintenance activities, and monitoring and audit mechanisms of maintenance activities. Consider management's actions to
 - a. Analyze and understand the costs of maintenance (e.g., budget, time, or personnel) versus the costs of not performing maintenance (e.g., system failures, data breaches, and customer dissatisfaction), and track costs for reporting purposes.
 - b. Plan for maintenance activities from the outset of the acquisition and development processes to address secure continuity of operations.
 - c. Perform preventive maintenance throughout an IT asset's useful life to prevent or minimize catastrophic failure and promote confidentiality, integrity, availability, and resilience.
 - d. Consider vendor or developer recommendations, cost-benefit analyses, operational risks, availability of qualified personnel, and other relevant industry factors (e.g., emerging technologies and threats) when developing the schedule for the maintenance plan.
 - e. Track system and component information, such as version, update, and patch level, as tracking and using this information helps personnel manage (e.g., through regular updates, data protection, and digital forensics) technology vulnerabilities.
 - f. Develop a process for identifying maintenance and vulnerability information and mechanisms for responding to user questions about developed or acquired IoT systems and components.
 - g. Validate that while a system or component is in use, it is appropriately maintained and updated through preventative maintenance and change management.
 - h. Establish a preventive maintenance plan, especially for mission-critical systems and components.
 - i. Maintain logs of maintenance activities and perform reviews of those logs as needed for authorization of changes, as well as anomalous or malicious activity.
 - j. Maintain awareness of the risks associated with unauthorized, untested, or unplanned changes.
 - k. Consider the capability of the product to receive, verify, and apply verified updates for configuration, patch, and vulnerability management for developed or acquired products.
 - l. Implement processes to manage changes regardless of whether the system or component was developed internally.

- m. Establish configuration management processes for developed and procured systems and components and help ensure that those processes are followed and enforced.
 - n. Validate that only authorized personnel implement configuration changes and make those changes only to designated systems.
 - o. Identify the sources of vulnerability information and threat intelligence for the entity's systems and components.
 - p. Receive the results of internal or external vulnerability scanning and penetration testing and identify remediation plans to resolve any issues detected through these tests.
 - q. Evaluate and mitigate the risk associated with the vulnerability to the entity's affected systems and components when obtaining vulnerability and threat intelligence from vendors, developers, third parties, and other sources.
 - r. Report the results of the testing and the remediation plans to the board.
 - s. Validate that the entity's patch management processes include procedures for identifying, evaluating, approving, testing, installing, and documenting patches or updates for systems and components.
2. Assess management's oversight of end-of-life activities. Consider management's actions to
- a. Maintain an accurate inventory of the entity's IT assets, including systems and components, regardless of whether they are developed internally or acquired from a third party.
 - b. Account for planned obsolescence if systems or components are developed internally.
 - c. Include a contract clause regarding advanced notification before the vendor's sunset timeline of an IT asset if a vendor decides not to replace, upgrade, or continue to support the asset.
 - d. Implement a process to determine EOL decisions (e.g., replace, upgrade, or migrate to a new system) before a system or component's EOL.
 - e. Document and monitor depreciation and obsolescence schedules of the entity's systems and components in its ITAM inventory to plan for EOL, as a part of its ITAM process.
 - f. Consider EOL risks tied to interconnections in the supply chain derived from maintaining legacy systems and components for an extended period of time.
 - g. Address EOL and the use of legacy systems and components, including time frames for necessary replacement or upgrade in contracts between the entity and its supply chain partners.
 - h. Address EOL risks related to the use of legacy systems and components by mitigation strategies such as the following:
 - Assess the risks of continued use of aging, outdated, and unsupported systems and components.
 - Consider transitioning to newer, supported systems and components.
 - Employ compensating controls.

3. Assess management's practices for termination and disposal of systems and components. Consider management's actions to
 - a. Implement appropriate termination and off-boarding procedures.
 - b. Include appropriate clauses in contracts with third parties to manage the termination of services, including related relationships (e.g., affiliates, subcontractors), if necessary. Clauses and contracts should address
 - Maintaining confidentiality, integrity, availability, and resilience of data and operations throughout the off-boarding process.
 - Specifying criteria defining termination.
 - c. Develop and implement procedures for the following:
 - Shutdown (i.e., sunset) of the systems and components.
 - Identification of the tasks involved.
 - Preservation and identification of the data and its disposition (i.e., archival or transfer).
 - Secure disposal of unnecessary systems and components (e.g., hardware and software).
 - d. Validate that appropriate personnel are aware of the procedures to coordinate the orderly disposition of the system, its components, and the data.
 - e. Develop and implement procedures to help ensure that the entity's critical or sensitive data and documents are removed (e.g., wiped, sanitized, or otherwise destroyed) logically and physically from the system and components before disposal.
 - f. Validate that data or documents maintained by the third party on behalf of the entity are addressed by the entity's requirements in the termination and disposal clauses of the contract.
4. Assess management's oversight of maintenance documentation, including working with third parties to help ensure that the entity receives current system, component, and user maintenance documentation.

Objective 14: Evaluate whether management establishes a formal process for the review, justification, approval, implementation, testing, and disposition of changes, and maintains confidentiality, integrity, availability, and resilience in the change management process. (Section VII.B, "[Change Management](#)")

Examiners should review the following:

- Change requests demonstrating prioritization, categorization, tracking, and reporting.
- Change control process, including for back-out plans and inventory, for all change types.
- Change management controls, including change logs, access control, and version control features.
- Risk assessment and change documentation, including approvals.
- Training for change management.
- Conversion plans and coordination with conversion partners and stakeholders.
- Reviews of change control processes for comprehensiveness and ongoing effectiveness, including review of all significant change reports and related documentation.

1. Assess whether management maintains policies, standards, and procedures that guide the change control process, including defined roles and responsibilities of key personnel in the change control process. Consider management's actions to
 - a. Designate personnel with the ability to create or initiate a request for a change and provide the processes they should follow.
 - b. Designate an individual (e.g., change manager) to facilitate a change who is responsible for managing all changes affecting the entity with minimal or no disruptions to operations.
 - c. Consider using a group of stakeholders that can aid the change manager in the assessment, prioritization, and scheduling of changes.
 - d. Prioritize and categorize changes.
 - e. Implement a method to track and report changes (e.g., standard change request forms, library and version controls, and spreadsheets or automated change logs).
2. Assess management's defined change control process to make routine and planned changes to systems or components, adjust configuration settings, and make changes to remediate flaws. Consider management's actions to
 - a. Follow a defined change control process to make routine and planned changes to systems or components, adjust configuration settings, and make changes to remediate flaws.
 - b. Account for
 - Emergency and unscheduled changes in the change control process.
 - Preparations for unexpected problems or failures with the change by defining a back-out plan and documenting the steps taken during the change in the order they occurred.
 - Requests for change.
 - Review of changes.
 - Approval of changes.
 - Design and build of changes.
 - Testing of changes.
 - Implementation of changes.
 - Verification of changes and close of the change process.
 - c. Follow processes, after verification of changes, to document completion of the change and close the change request.
 - d. Report on the status of the change after closing and monitor the implemented change for unintended issues.
 - e. Integrate security into its change control processes to help ensure that modifications do not adversely affect the security posture of varying systems.
 - f. Define the implementation plan (i.e., steps to deploy the change), create a full copy of the current version in production, and finalize the back-out plan before deploying the change.
 - g. Perform a post-implementation review to verify that the change was deployed according to the implementation plan and functions appropriately.

- h. Follow processes after verification to document completion of the change and close the change request.
 - i. Report on the status of the change after closing and monitor the implemented change for unintended issues.
3. Assess additional controls in change management. Consider management's actions to
 - a. Isolate and protect the testing environment to avoid it being a vulnerable vector for exploit in the entity.
 - b. Strictly control the movement of programs and files among development, quality management, and production libraries for purposes of change control.
 - c. Assign librarian functions to independent personnel, such as quality management personnel in larger, or more complex entities, or to nonoperations personnel in smaller or less complex entities.
 - d. Validate that library attributes include an auditable activity log with appropriate controls to ensure that information has not been altered or deleted.
 - e. Implement library controls, such as
 - Automated access controls.
 - Automated library applications.
 - f. Consider using these automated change controls commensurate with the complexity of the entity's IT environment and the number, types, and complexities of changes in that environment.
 - g. Strictly control access to production software libraries, particularly in distributed environments, regardless of whether the entity has automated change control tools.
 - h. Establish appropriate policies for the use of code repositories, such as determining what code repositories they use and where code repository data actually resides, especially for any cloud-based repositories (e.g., public, private, and community clouds).
 - i. Conduct periodic reconnaissance of open (i.e., public) code repositories for personal employee accounts and unauthorized posting of company-owned source code.
 - j. Use available version control features to track changes made to the code in the repository, providing accountability to the individual account that made the changes.
 - k. Implement access control processes, such as the following:
 - Request and approval processes for access to code repositories (e.g., development, staging, or production).
 - Appropriate access controls, such as use of MFA for employee access to all (internal and cloud-based) code repositories.
 - Appropriate segregation of duties to prevent developer access to the staging and production code repositories, prevent quality management personnel from having access to production code repositories, and grant access to production code repositories only to release management personnel.
 - Periodic review processes for access roles and repository logs.
4. Assess management's oversight of change or modification types. Consider management's actions to

- a. Develop procedures for changes that include change request, review, and approval that direct management to plan, test, and document changes before implementation.
 - b. Validate that changes to any IT system, component, or service are supported by an orderly, adaptable, documented, and measurable process to promote the consistent implementation of changes and provide an audit trail for changes, regardless of the change type.
 - c. Train personnel involved in changes to ensure that those changes support entity objectives and do not adversely affect confidentiality, integrity, availability, and resilience.
 - d. Coordinate change management for routine modifications, as IT changes often affect multiple business lines.
 - e. Develop an inventory of changes, including routine modifications, for back-out, resilience, and tracking purposes.
5. Assess management's oversight of planned changes. Consider management's actions to
- a. Perform a risk assessment for all major modifications and significant security-related changes.
 - b. Discuss requests for major modifications formally and assign appropriate key stakeholders or committees to have responsibility for approving the requests, based on predefined criteria.
 - c. Define the entity's training requirements associated with conversions or major hardware and software upgrades.
 - d. Evaluate the type, volume, and timing of training needs for each affected line of business and coordinate training programs with applicable third parties.
 - e. Plan when a conversion affects a core platform supporting business operations whether managed on-premises or at a third party to minimize conversion issues and costs.
 - f. Consider costs related to deconversions, system and component upgrades, and training for changes with the new system.
 - g. Effectively manage conversions beginning with due diligence, including a comprehensive analysis of a conversion's impact on existing operations (e.g., processing, storage, and communication requirements), while accounting for interdependencies.
 - h. Establish communication procedures, reporting needs, and lines of authority for timely decision-making and issue resolution, when working with a third-party partner.
 - i. Coordinate with conversion partners to consider the entity's conversion needs.
6. Assess management oversight of emergency modifications. Consider management's actions to
- a. Maintain appropriate implementation control standards, although an emergency modification should be completed quickly.
 - b. Periodically review the change control processes to optimize efficiency and determine whether they need revision.

- c. Perform testing before deployment in the case of an emergency change, if possible, as untested changes may cause even more damage than the initial risk being mitigated.
- d. Evaluate whether the potential damage resulting from an untested emergency change outweighs the immediate damage from the identified risk to determine the appropriateness of the decision to implement the emergency change.
- e. Develop a process for system and component owners to identify all sources of change to help ensure that emergency modifications go through the change control process, even if it is after the fact.
- f. Accelerate change management processes to implement changes rapidly to effectively mitigate the impact of emergency situations.
- g. Develop effective processes to address emergency situations.
- h. Strategically plan for emergency modifications, including budgeting contingency funds for execution and management of emergency situations.
- i. Consider appropriate measures to help effectively implement changes during emergencies. Examples include the following:
 - Organize a group (e.g., emergency change control review board) that can meet on extremely short notice to approve changes that need immediate implementation. The group could include senior leadership, management of critical lines of business, and management of key IT areas.
 - Plan for multiple methods of meeting (e.g., in-person, phone, and virtual) in case the emergency occurs outside normal business hours.
 - Create an emergency modification implementation plan that includes a list of individuals in the emergency group (e.g., emergency change control review board) and a list of procedures that are modified from standard change control and security processes.
 - Compress certain phases of the implementation process to save time but still perform testing and modeling or simulation before releasing the changes into the production environment.
 - Discuss and implement minimum recovery point objectives with stakeholders for emergencies to reduce the time required to perform backups of systems to adequately implement an emergency modification.
 - Define and use emergency downtime procedures (e.g., failover to alternate systems) that allow systems to be taken completely offline in emergencies.
 - Follow emergency procedures, such as use of “out-of-band” communication provisions, if normal channels for secure transmission of information becomes unavailable.
 - Leverage senior management to communicate the urgency of emergency modifications and help achieve rapid consensus for decisions affecting the change implementation timeline.
 - Perform periodic emergency drills in the test and modeling environment to prepare IT staff to deal with the stress of emergency modifications. Review the results of these drills and document lessons learned.
- j. Plan for emergency modifications, such as doing the following:
 - Establish who can declare an emergency and facilitate decision-making during emergencies.

- Designate individuals who can approve emergency changes and maintain contact information.
 - Develop a plan that outlines the responsible parties and procedures for enacting emergency changes.
 - Identify personnel responsible for change testing and implementation, as well as for initiating a back-out plan if implementation fails.
 - k. Validate every emergency modification after implementation to determine whether it was correctly classified, in order to keep the number of emergency modifications to a minimum.
 - l. Review reports of emergency modifications periodically for appropriateness of classification.
 - m. Control attempts by personnel to circumvent routine modification or planned change control processes by classifying changes as emergencies to avoid resource constraints (e.g., time, personnel, and cost).
 - n. Complete evaluations and documentation reviews of emergency modifications as soon as possible after implementation.
7. Assess management's change management documentation practices. Consider management's actions to
- a. Maintain documentation to track all changes (e.g., configuration settings, patches applied, system conversions, and emergency modifications) to systems and components.
 - b. Maintain appropriate documentation to support the impact analysis.
 - c. Prepare for the possibility of a failed or incomplete deployment and have procedures to address the issues and develop rollback or back-out procedures to reverse a failed deployment.
 - d. Consider the time required to perform rollback procedures, when to trigger the rollback plan, and how long it may take to roll back.
 - e. Determine whether the rollback plan can be accomplished in the defined timeline for the maintenance action.
 - f. Implement appropriate security controls to prevent unauthorized rollback.
 - g. Track and report issues that lead to the use of a back-out plan and the effects of a failed or incomplete change deployment.

Objective 15: Communicate and discuss findings, conclusions, and corrective actions.

1. Review preliminary conclusions with the examiner-in-charge regarding
 - a. Violations of law and regulation.
 - b. Significant issues warranting inclusion as matters requiring attention or recommendations in the report of examination.
 - c. Proposed Uniform Rating System for Information Technology management component rating and the potential impact of the examiner's conclusions on composite or other component IT ratings.
 - d. Potential impact of the examiner's conclusions on the entity's risk assessment.

2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.
3. Document conclusions in a memorandum to the examiner-in-charge that provides report-ready comments for all relevant sections of the report of examination and guidance to future examiners.
4. Organize work papers to ensure clear support for significant findings by examination objective.

APPENDIX B: GLOSSARY

The purpose of the glossary is to define technical terms used in the *FFIEC IT Examination Handbook* booklets in the context of supervisory activities for the entities over which FFIEC members may have supervisory authority. The FFIEC members strive to align terminology in the glossary with appropriate authoritative standards, including the [NIST Computer Security Resource Center Glossary](#) (NIST Glossary) as the primary source for cyber-related definitions, as appropriate. FFIEC members employed the following process to select, modify, or develop definitions.

When a NIST definition existed:

- If NIST had a defined term and modifications to the definition were unnecessary, the FFIEC members included the NIST definition in this glossary. When multiple NIST definitions were available for the same term, the FFIEC members selected a definition for supervisory purposes.
- If NIST had a defined term, but the definition needed additional clarity for supervisory purposes to assist with the identification of safety and soundness and enterprise risks related to IT, the FFIEC members included both the NIST definition and the FFIEC-adapted definition. These definitions are labeled “FFIEC Adapted for Supervisory Purposes” in this glossary’s source column.

When a NIST definition did not exist, or the definition was not appropriate for supervisory purposes:

- If NIST did not have a defined term, but there was an appropriate authoritative third-party source (e.g., the ISO Glossary), the FFIEC members included that authoritative definition.
- If NIST did not have a defined term and there was not an appropriate authoritative third-party source, the FFIEC members developed a definition for supervisory purposes. These definitions are labeled “FFIEC Developed for Supervisory Purposes” in this glossary’s source column.

Due to the constantly evolving nature of IT and its associated risks, the FFIEC members may update definitions to maintain alignment with other government agencies and the financial services industry.

Table 5: Glossary of Terms for Development, Acquisition, and Maintenance

Term	Definition	Source
A		
Access control	Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space.	NIST Glossary
Acquisition	All stages of the process of acquiring a product or services, beginning with the process for determining the need for the product or services and ending with contract completion and closeout.	NIST Glossary
Application	A system for collecting, saving, processing, and presenting data by means of a computer. The term “application” is generally used when referring to a component of software that can be executed. The	NIST Glossary

Term	Definition	Source
	terms “application” and “software application” are often used synonymously.	
Application programming interface (API)	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.	NIST Glossary
	Software code that allows two or more different programs to communicate with each other.	FFIEC Adapted for Supervisory Purposes
Architecture	Refers to the manner in which the strategic design of the hardware and software infrastructure components (e.g., devices, systems, and networks) are organized and integrated to achieve and support the entity’s business objectives.	FFIEC Developed for Supervisory Purposes
Artificial intelligence (AI)	Refers to the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action—whether digitally or as the smart software behind autonomous physical systems.	U.S. Department of Defense, <i>Summary of the 2018 Department Of Defense Artificial Intelligence Strategy</i>
Assembler	A computer program that automatically converts instructions written in assembly language into machine language.	Merriam-Webster
Attack surface	The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment.	NIST Glossary
Authentication	A process that establishes the source of information, provides assurance of an entity’s identity or provides assurance of the integrity of communications sessions, messages, documents or stored data.	NIST Glossary
	A process designed to establish the source of the information, validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information.	FFIEC Adapted for Supervisory Purposes
Authorization	The granting or denying of access rights to a user, program, or process.	NIST Glossary
Availability	Ensuring timely and reliable access to and use of information.	NIST Glossary
B		
Backdoor	An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.	NIST Glossary
Backup	A copy of files and programs made to facilitate recovery, if necessary.	NIST Glossary
Barcode	An optical machine-readable representation of data about an object.	NIST, “Automated Identification Technologies for Forensic Science”
Baseline configuration	A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.	NIST Glossary
Big data	Extensive datasets—primarily in the characteristics of volume, variety, velocity, and/or variability—that require a scalable architecture for efficient storage, manipulation, and analysis.	NIST SP 1500-1r2, <i>NIST Big Data Interoperability Framework: Volume 1, Definitions</i>
Blockchain	A distributed digital ledger of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older	NIST Glossary

Term	Definition	Source
	blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger in the network, and any conflicts are resolved automatically using established rules.	
Bounded context	In relation to microservices, it refers to having limited responsibility and dependence on other services.	NIST SP 800-204, Security Strategies for Microservices-Based Application Systems
Business case	A business case defines the value a project will deliver.	Project Management Institute (PMI), "Is This Really Worth the Effort? The Need for a Business Case"
	An evaluation of the benefit, cost, feasibility, and risk of alternative options to justify undertaking a project, program, or portfolio and define the value it will deliver.	FFIEC Adapted for Supervisory Purposes
C		
Capacity management	The process of planning and monitoring an entity's technology resources to support current and future strategic objectives.	FFIEC Developed for Supervisory Purposes
Central processing unit (CPU)	Computer hardware that houses the electronic circuits that control/direct all operations of the computer system.	Information Systems Audit and Control Association (ISACA) Glossary
Change control	Change control is the process through which all requests to change the approved baseline of a project, program, or portfolio are captured, evaluated and then approved, rejected, or deferred.	Association for Project Management
	Change control is the process through which all requests to change the approved baseline of a project, program, or portfolio are documented, evaluated and then approved, rejected, or deferred. Change control is an element in an overall change management process.	FFIEC Adapted for Supervisory Purposes
Change control board (CCB)	A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system. Also referred to as a configuration control board.	NIST Glossary
Change management	The continuous process of maintaining the integrity of hardware, software, firmware, and documentation and controlling and approving changes (e.g., addition, modification, or elimination) to information or technology assets or related infrastructure (aka configuration and change management).	CISA, CRR Supplemental Resource Guide, Volume 3: Configuration and Change Management, Version 1.1
Checksum	A value computed on data to detect error or manipulation.	NIST Glossary
Circuit	A dedicated single connection between two end points on a network.	NIST Glossary
Cloud access security broker	A software tool or service that sits between an entity's on-premises infrastructure and a cloud service provider's infrastructure as a "gatekeeper" to monitor activity and enforce the entity's security policies (e.g., authentication, single sign-on, authorization, credential mapping, and encryption) as the cloud-based resources are accessed.	FFIEC Developed for Supervisory Purposes
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g.,	NIST Glossary

Term	Definition	Source
	networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	
Cloud service provider	A cloud service provider, or CSP, is a company that offers some component of cloud computing; typically, when you search the internet a cloud service is defined as infrastructure as a service (IaaS), software as a service (SaaS), or platform as a service (PaaS) to other businesses or individuals.	Cloud Security Alliance
	A third-party service provider who offers clients services over the public internet. Examples of services could be applications (SaaS), operating systems (PaaS), or infrastructure (IaaS).	FFIEC Adapted for Supervisory Purposes
Code	See machine code.	
Commercial off-the-shelf (COTS) software	A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public. Also referred to as off-the-shelf.	NIST Glossary
Compiled	Processed through software that translates a complete set of high-level computer instructions into machine language before executing any of them.	Merriam-Webster
Component	A unique part of a system that is needed to do something, perform a function, or finish a product.	Black's Law Dictionary
	A unique part of a larger system, such as hardware, software, and firmware, that is a building block to do something, perform a function, or finish a product.	FFIEC Adapted for Supervisory Purposes
Compromise	The unauthorized disclosure, modification, substitution, or use of sensitive data (e.g., keying material and other security-related information).	NIST Glossary
Confidentiality	The property that sensitive information is not disclosed to unauthorized entities.	NIST Glossary
Configuration	The selection of one of the sets of possible combinations of features of a system.	NIST Glossary
	The selection of combinations of conditions, parameters, features, and specifications of a system.	FFIEC Adapted for Supervisory Purposes
Configuration control board (CCB)	A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system. Also referred to as a change control board.	NIST Glossary
	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.	FFIEC Adapted for Supervisory Purposes
Configuration settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.	NIST Glossary
Container	A container is a standard unit of software that packages up code and all its dependencies, down to, but not including the operating system (OS). It is a lightweight, standalone, executable package of software that includes everything needed to run an application except the OS: code, runtime, system tools, system libraries, and settings.	DOD Enterprise DevSecOps Reference Design: Version 1.0
Container image	A package that contains all the files required to run a container.	NIST SP 800-190, Application Container Security Guide

Term	Definition	Source
Container runtime	The environment for each container; comprised of binaries coordinating multiple operating system components that isolate resources and resource usage for running containers.	NIST Glossary
	Software that coordinates multiple operating system components to isolate resource and resource usage for running containers and managing container images on a node.	FFIEC Adapted for Supervisory Purposes
Continuous integration/continuous delivery or deployment (CI/CD) pipeline	The set of tools and the associated process workflows to achieve CI and CD with build, test, security, and release delivery activities, which are steered by a CI/CD orchestrator and automated as much as practice allows.	DOD Enterprise DevSecOps Fundamentals
Contract	A binding agreement between two or more parties, which may indicate prices and goods and services to be provided.	Merriam-Webster
Copyright	A type of intellectual property that protects original works of authorship as soon as an author fixes the work in a tangible form of expression.	U.S. Copyright Office
Counterfeit item	A counterfeit item is a suspect item that is a copy or substitute without legal right or authority to do so or one whose materials, performance, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer. An item that does not conform to established requirements is not normally considered an S/CI if the nonconformity results from one or more of the following conditions, which should be controlled by site procedures as nonconforming items: defects resulting from inadequate design or production quality control; damage during shipping, handling, or storage; improper installation; deterioration during service; degradation during removal; failure resulting from aging or misapplication; or other controllable causes.	U.S. Department of Energy, Suspect/Counterfeit Items Awareness Training
Cyber risk	Risk of financial loss, operational disruption, or damage from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system.	NIST Glossary
	Risk of financial loss, operational disruption, or damage from the failure of the digital technologies employed for informational and/or operational functions introduced to a system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system.	FFIEC Adapted for Supervisory Purposes
Cybersecurity	The process of protecting consumer and bank information by preventing, detecting, and responding to attacks.	NIST Glossary
D		
Dashboard	A tool that consolidates and communicates information relevant to the entity in near real-time. It is generally visual and often uses a variety of charts.	NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations
Data	A representation of information as stored or transmitted.	NIST Glossary
	A physical or digital representation of information processed, stored (at rest), or transmitted (in transit).	FFIEC Adapted for Supervisory Purposes
Data analytics	The systematic process of evaluating and organizing data sets to draw insights, make predictions, and reveal trends using logical analysis.	FFIEC Developed for Supervisory Purposes
Data center	A facility that houses virtual and/or physical information technology infrastructure(s) (e.g., computer, server, and networking systems and components) designed to store, process, and serve large amounts of data in support of an entity's strategic and business	FFIEC Developed for Supervisory Purposes

Term	Definition	Source
	objectives. A data center may be a dedicated facility or an area or room that contains computer, server, and networking systems and components, and may be private or shared (e.g., a co-location facility).	
Data classification	Categorizing data based on its level of sensitivity (e.g., confidentiality, integrity, or availability), value, and criticality to the entity.	FFIEC Developed for Supervisory Purposes
Data communications	The transfer of data over networks using a combination of telecommunication services and network devices.	FFIEC Developed for Supervisory Purposes
Data governance	A set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority and management and decision-making parameters related to the data produced or managed by the enterprise.	NIST Glossary
Data management	The practice of putting into place policies, procedures and best practices to ensure that data are understandable, trusted, visible, accessible and interoperable.	DHS Lexicon Terms and Definitions
	The practice of putting into place policies, procedures, and best practices to ensure that data are understandable, trusted, visible, accessible, and interoperable to ensure that user needs are met.	FFIEC Adapted for Supervisory Purposes
Database	A repository of information or data, which may or may not be a traditional relational database system.	NIST Glossary
	A repository of information or data organized to be accessed, managed, and updated.	FFIEC Adapted for Supervisory Purposes
Developer	A person or group that designs and/or builds, and/or documents and/or configures the hardware and/or software of computerized systems	ISACA Glossary
	A person or group that designs, builds, documents, and configures the hardware and software of systems.	FFIEC Adapted for Supervisory Purposes
Development	The systematic application of knowledge toward the production of useful materials, devices, and systems or methods that leverage the results of applied research activities; includes validation and demonstration of a chosen technology in laboratory, representative and operational environments, improving on research prototypes, integration into systems and subsystems, addressing manufacturing, producibility and sustainability needs, and independent operational test and evaluation.	DHS Lexicon Terms and Definitions
	The systematic application of knowledge toward the production of useful materials, devices, and systems or processes of defining, designing, testing, and implementing systems or components. Development includes validation and demonstration of a chosen technology, use of test and production environments, improvement of developed prototypes, integration into systems and subsystems, and inclusion of hardware builds.	FFIEC Adapted for Supervisory Purposes
Device	A piece of equipment or a mechanism designed to serve a special purpose or perform a special function.	Merriam-Webster
DevOps	A set of practices for automating the processes between software development and information technology operations teams so that they can build, test, and release software faster and more reliably. The goal is to shorten the SDLC and improve reliability while delivering features, fixes, and updates frequently in close alignment with business objectives.	NIST Glossary

Term	Definition	Source
DevSecOps	An organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops).	NIST SP 800-204C, Implementation of DevSecOps for a Microservices-Based Application With Services Mesh
	A software engineering culture and practice that aims at unifying software development (Dev), security (Sec), and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the SDLC.	FFIEC Adapted for Supervisory Purposes
Digital signature	An electronic analogue of a written signature, a digital signature provides assurance that the claimed signatory signed the information, and the information was not modified after signature generation.	NIST Computer Security Resource Center
Dynamic analysis	Testing that operates by executing a program using a set of input use-cases and analyzing the program's runtime behavior.	OWASP Vulnerability Management Guide (OVMG)
E		
Encryption	Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.	NIST Glossary
End-of-life (EOL)	With respect to technology, a time frame usually defined by a technology vendor to describe when an asset has reached the end of its useful life cycle and when the vendor no longer maintains and supports the asset or continues to sell or license it.	FFIEC Developed for Supervisory Purposes
F		
Feasibility study	An analysis of the known or anticipated need for a product, system or component to assess the degree to which the requirements, designs or plans can be implemented.	ISACA Glossary
	An analysis of a known problem or anticipated need and its potential solutions that considers all relevant factors—including economic, technical, legal, and scheduling considerations—to determine a project's viability, costs, and benefits.	FFIEC Adapted for Supervisory Purposes
Firewall	A gateway that limits access between networks in accordance with local security policy.	NIST Glossary
Firmware	Memory chips with embedded program code that hold their content when power is turned off.	ISACA Glossary
	A type of software, often included in read-only memory, that is embedded directly in a piece of hardware to make the hardware work as intended. Software is retained even when power is turned off.	FFIEC Adapted for Supervisory Purposes
Fourth party	Fourth (or nth) parties provide services to support the operations of third parties, which, in turn, provide services to the primary enterprise. Also referred to as subcontractor.	ISACA
Functional testing	Testing that verifies that an implementation of some function operates correctly.	NIST Glossary
Fuzz testing	A black box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion by tools referred to as "fuzzers," which are programs or scripts that submit some combination of inputs to the test target to reveal how it responds.	OWASP, Code Review Guide 2.0
	A black box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion.	FFIEC Adapted for Supervisory Purposes
G		
Gateway	An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.	NIST Glossary

Term	Definition	Source
H		
Hardening	A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services, and utilities from the system. (Referred to as system hardening)	ISACA Glossary
	A process intended to eliminate as many security risks as possible by implementing security controls (e.g., changing default passwords, enabling security settings, and protecting privileged accounts), patching vulnerabilities, turning off nonessential services, and removing all nonessential software programs, protocols, and utilities from the system.	FFIEC Adapted for Supervisory Purposes
Hardware	The physical components of an information system.	NIST Glossary
Help desk	A service offered via telephone/Internet by an enterprise to its clients or employees that provides information, assistance and troubleshooting advice regarding software, hardware, or networks.	ISACA Glossary
Heterogeneity	Consisting of dissimilar or diverse elements.	Merriam-Webster
Heuristics	Involving or serving as an aid to learning, discovery, or problem-solving by experimental and especially trial-and-error methods.	Merriam-Webster
Host	Any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include computers, personal electronic devices, thin clients, and multifunctional devices.	NIST Glossary
Human-readable code	Code that includes source code, scripts, and any other form of code that an organization deems human-readable.	NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities
Hypertext transfer protocol (HTTP)	A standard method for communication between clients and web servers.	NIST Glossary
Hypertext transfer protocol secure (HTTPS)	A protocol for accessing a secure web server, whereby all data transferred are encrypted. Standard port number is 443.	ISACA Glossary
Hypervisor	The virtualization component that manages the guest operating systems (OS) on a host and controls the flow of instructions between the guest OSs and the physical hardware.	NIST Glossary
I		
Identity and access management (IAM)	Encapsulates people, processes, and products to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources.	ISACA Glossary
Impact analysis	The analysis conducted by an organizational official to determine the extent to which a change to the information system have affected the security state of the system. Referred to as a security impact analysis.	NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
	The analysis conducted by qualified staff in an organization to determine the extent to which changes to the system affect the security posture of the system. This may involve security, resilience, and compliance.	FFIEC Adapted for Supervisory Purposes
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	NIST Glossary

Term	Definition	Source
Incident management	The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible.	FFIEC Developed for Supervisory Purposes
Incident response	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	DOD Cyber Exchange
Information security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	NIST Glossary
Information technology asset management (ITAM)	Refers to a set of policies and procedures that an organization uses to track, audit, and monitor the state of its IT assets, and maintain system configurations.	NIST SP 1800-5, IT Asset Management
Infrastructure	System of facilities, equipment, and services needed for the operation of an organization.	ISO Online Browsing Platform, Terms & Definitions
	The physical elements, products, and services necessary to provide and maintain ongoing operations to support business activity, including the maintenance of physical facilities.	FFIEC Adapted for Supervisory Purposes
Infrastructure as a service (IaaS)	IaaS provides entities with the ability to provision processing, storage, networks, and other fundamental computing resources where the entity is able to deploy and run software, which can include operating systems and applications. The entity does not manage or control the underlying cloud infrastructure; however, it has control over operating systems, storage, and deployed applications. Entities have the maximum flexibility to customize their cloud services and user interfaces.	NIST SP 500-316, Framework for Cloud Usability
Integration testing	An orderly progression of testing in which software elements, hardware elements or both are combined and tested to evaluate their interactions, until the entire system has been integrated.	ISACA Glossary
Integrity	A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored.	NIST Glossary
Interdependencies	When two or more departments, processes, functions, or third-party providers interact to successfully complete a task, business function, or process.	FFIEC Developed for Supervisory Purposes
Internet of things (IoT)	Refers to the collection of technologies that allow information to be sent to and received from physical devices (e.g., security systems, HVAC systems, intelligent personal assistants, and kitchen appliances), that were not traditionally thought of as IT assets, using the internet. These devices have the ability to send and receive data over a network without necessarily requiring human-to-human or human-to-computer interaction using embedded computing capability and network connectivity and unique identifiers (e.g., internet protocol address).	FFIEC Developed for Supervisory Purposes
Intrusion detection system (IDS)	A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.	NIST Glossary
Intrusion prevention system (IPS)	A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.	NIST Glossary
K		
Kernel	Core that provides basic services for all other parts of the OS.	FFIEC Developed for Supervisory Purposes

Term	Definition	Source
L		
Legacy	A custom environment containing older systems or applications that may need to be secured to meet today's threats, but often use older, less secure communication mechanisms and need to be able to communicate with other systems (aka legacy environment).	NIST Glossary
	Relates to older, outdated technology systems, components, or applications that may be critical to day-to-day operations. Often, they may need to be secured, updated, or replaced to meet current threats.	FFIEC Adapted for Supervisory Purposes
License	A permission granted by competent authority to engage in a business or occupation or in an activity otherwise unlawful.	Meriam-Webster
Log	A record of events occurring within an entity's systems and networks.	NIST Glossary
Loose coupling	An approach to designing systems so that linked components of networks, software, and services can be scaled to operate as independently as possible to avoid issues with one component adversely affecting others.	FFIEC Developed for Supervisory Purposes
M		
Machine code	Also referred to as "code" or "machine language." Computer instructions and definitions expressed in a form (binary code) that can be recognized by the CPU of a computer. All source code, regardless of the language in which it was programmed, is eventually converted to machine code.	ISACA Glossary
Machine language	See <i>machine code</i> .	
Machine learning (ML)	The process of using an algorithm(s) to help computers learn without being explicitly programmed and identify patterns in data. Those patterns are then used to create a data model that can make predictions.	FFIEC Developed for Supervisory Purposes
Mainframe	A large, high-speed computer, especially one supporting numerous workstations or peripherals.	ISACA Glossary
Maintenance	Any act that either prevents the failure or malfunction of equipment or restores its operating capability.	NIST Glossary
Malicious code	Unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses.	CISA, "Protecting Against Malicious Code"
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.	NIST Glossary
Markup language	A system (such as HTML or SGML) for marking or tagging a document that indicates its logical structure (such as paragraphs) and gives instructions for its layout on the page especially for electronic transmission and display.	Meriam-Webster
	A type of language used to annotate text and embed tags in a text document to control its structure, formatting, display, or the relationship between its parts to facilitate automated processing and use by humans.	FFIEC Adapted for Supervisory Purposes
Masking	The process of systematically removing a field or replacing it with a value in a way that does not preserve the analytic utility of the value, such as replacing a phone number with asterisks or a randomly generated pseudonym.	NIST Glossary
Master services agreement (MSA)	One legal document that consolidates separate but related agreements between the same signing parties. Also known as master contract.	Black's Law Dictionary
	Also known as a "master contract," it is a legal document that consolidates and governs multiple service agreements or transactions between the same signing parties or entities, and often addresses the terms that will govern future transactions or agreements.	FFIEC Adapted for Supervisory Purposes

Term	Definition	Source
Metadata	Data about data. For file systems, metadata are data that provide information about a file's contents.	NIST Glossary
	Data about data. Examples of metadata include purpose of the data, creator or owner of the data, file size, location where the data were created, and source of the data.	FFIEC Adapted for Supervisory Purposes
Microchip	A very small piece of silicon inside a computer. It has electronic circuits on it and can hold large quantities of information or perform mathematical and logical operations.	Collins Dictionary
Microcontroller	An integrated circuit that contains a microprocessor along with memory and associated circuits and that controls some or all of the functions of an electronic device (such as a home appliance) or system.	Merriam-Webster
Microservices	A set of containers that work together to compose an application.	NIST Glossary
Middleware	Middleware is a term used for a computer program that functions as a go between for two other programs.	DHS, Access Control Technologies Handbook
Misdirection	The process of maintaining and employing deception resources or environments and directing adversary activities to those resources or environments.	NIST Glossary
Mobile device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source.	NIST Glossary
Multifactor authentication (MFA)	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password or personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device or token); or (iii) something you are (e.g., biometric).	NIST Glossary
N		
Network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.	NIST Glossary
Network diagram	A network diagram (also referred to as a network map or network topology) is a visual representation of nodes and connections in a computer network.	FFIEC Developed for Supervisory Purposes
Networked	A database organized according to ownership of records, allowing records to have multiple owners and thus providing multiples access paths to the data. Database management systems (DBMSs) providing such capabilities are also referred to as CODASYL (Conference on Data Systems Languages) DBMSs.	Gartner Glossary
Network operations center (NOC)	The central location or department responsible for monitoring the health and performance of the network, including analyzing and maintaining network traffic, telecommunications, and network disruptions.	FFIEC Developed for Supervisory Purposes
Nonproduction environment	Systems (e.g., applications, infrastructure, networks, and operating systems) that are not used for production purposes. For example, systems that are used as development or test environments for new software or technologies or changes to existing software or technologies.	FFIEC Developed for Supervisory Purposes
O		
Object code	A code expressed in machine language ("1"s and "0"s), which is normally an output of a given translation" process that is ready to be executed by a computer.	U.S. Food and Drug Administration, Glossary of Computer System Software

Term	Definition	Source
		Development Terminology
Open-source software	Software released under a license that allows the software and its source code to be accessed, used, modified, and shared by anyone.	NIST S 6106.01, "Open Source Code"
Operating system (OS)	The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.	NIST Glossary
Operations	The performance of activities comprising methods, principles, processes, procedures, and services that support business functions.	FFIEC Developed for Supervisory Purposes
Operations management	The process of overseeing the methods, activities, or performance of practical work, and application of principles, processes, procedures, and services of an entity, using business resources.	FFIEC Developed for Supervisory Purposes
Orchestrator	A tool that enables DevOps personas or automation working on their behalf to pull images from registries, deploy those images into containers, and manage the running containers. Orchestrators are responsible for monitoring container resource consumption, job execution, and machine health across hosts.	NIST Glossary
Original equipment manufacturer	Technology providers (e.g., IT hardware vendors, hardware component makers, software vendors, resellers, and distributors) that distribute output devices and services produced by another company under their own brand name.	FFIEC Developed for Supervisory Purposes
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication.	NIST Glossary
P		
Patch	Fixes to software programming errors and vulnerabilities.	ISACA Glossary
Patch management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are referred to as patches, hot fixes, and service packs.	NIST Glossary
Penetration testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.	NIST Glossary
	A test methodology in which assessors, typically working under specific constraints and using all available documentation, attempt to circumvent or defeat the security features of a system, such as the network, application, its data, or its environment resources. Penetration tests often involve analyzing for individual and combinations of vulnerabilities on a system or multiple systems that can be used to gain access beyond what is achieved through a single vulnerability.	FFIEC Adapted for Supervisory Purposes
Planned obsolescence	The practice of making or designing something in such a way that it will only be usable for a short time so that people will have to buy another one.	Merriam-Webster
	A system disposal strategy developed and implemented, as needed, to address technology refresh in budget planning to limit the use of obsolete systems that present security or reliability risks.	FFIEC Adapted for Supervisory Purposes
Platform	A computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run.	NIST Glossary
Platform as a service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or	NIST Glossary

Term	Definition	Source
	control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.	
Policies	Statements, rules, or assertions that specify the correct or expected behavior of an entity.	NIST Glossary
Post-implementation review (PIR)	The process for reviewing IT projects in order to learn from past investments and initiatives by comparing actual results to estimates. PIRs also serve as vehicles for evaluating the entire IT investment management process.	U.S. Government Accountability Office, Information Technology Investment Management
	An evaluation of projects that provides a feedback mechanism to management that can measure project results, comparing actual results to estimates, and gather data necessary to analyze what corrective action may be required, if necessary.	FFIEC Adapted for Supervisory Purposes
Problem	In IT, the unknown underlying cause of one or more incidents.	ISACA Glossary
Procedures	A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.	ISACA Glossary
Procurement	The process of obtaining a system, product, or service.	NIST Glossary
	The corporate processes and functions that involve governance over purchasing decisions for obtaining a system, product, or service.	FFIEC Adapted for Supervisory Purposes
Program	An activity that focuses on the coordination of a number of related projects and other activities, over time, to deliver benefits to the organization.	PMI
Project	An activity chartered to create a specified deliverable as efficiently as possible.	PMI
Project management office (PMO)	Organizational unit that supports the management of projects and project-based organizations.	PMI, "The PMO: Your Key to Strategy Execution and Results Delivery"
Protocol	A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems.	NIST Glossary
Prototyping	The process of quickly putting together a working model (a prototype) to test various aspects of a design, illustrate ideas or features, and gather early user feedback. Prototyping uses programmed simulation techniques to represent a model of the final system to the user for advisement and critique. The emphasis is on end-user screens and reports. Internal controls are not a priority item since this is only a model.	ISACA Glossary
Provenance	Origin or source.	Merriam-Webster
Provisioning	The activity of obtaining the equipment and resources you need for a particular activity.	Cambridge Dictionary
	The activity of obtaining, modifying, and making available the equipment, resources, software, or services a user needs to carry out a particular activity.	FFIEC Adapted for Supervisory Purposes
Q		
Quality assurance (QA)	A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements	ISACA Glossary
	A planned and systematic pattern of all actions necessary to provide adequate confidence that a system, component, or facility conforms to established requirements.	FFIEC Adapted for Supervisory Purposes
Quality assurance/quality control (QA/QC)	Part of quality management focused on providing confidence that quality requirements will be fulfilled.	NIST Glossary

Term	Definition	Source
Quality control (QC)	The operational techniques and procedures used to achieve quality requirements.	ISACA Glossary
	The operational techniques and procedures (such as design analysis and inspection for defects) used to achieve quality requirements.	FFIEC Adapted for Supervisory Purposes
Quality of service	The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements. Properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, and packet jitter.	Committee on National Security Systems Glossary
Quality management	Coordinated activities to direct and control an organization with regard to quality.	NIST Glossary
Query	In databases, a request for data or information from a table or combination of tables.	FFIEC Developed for Supervisory Purposes
R		
Radio frequency identification (RFID)	A form of automatic identification and data capture technology that uses electric or magnetic fields at radio frequencies to transmit information.	NIST SP 800-98, Guidelines for Securing Radio Frequency Identification (RFID) Systems
Random access memory (RAM)	The computer's primary working memory. Each byte of RAM can be accessed randomly regardless of adjacent bytes.	ISACA Glossary
	The computer's primary working memory, which is kept where each byte of RAM can be quickly accessed by the device's processor.	FFIEC Adapted for Supervisory Purposes
Registry	A service that allows developers to easily store images as they are created; tag and catalog images for identification and version control to aid in discovery and reuse; and find and download images that others have created.	NIST SP 800-190, Application Container Security Guide
Regression	Defect or bug (in terms of code).	OWASP, Code Review Guide 2.0
Release	A collection of new and/or changed configuration items, which are tested and introduced into a production environment together.	NIST Glossary
Relational database	A database organized according to ownership of records, allowing records to have multiple owners and thus providing multiple access paths to the data. Database management systems (DBMSs) providing such capabilities are also referred to as CODASYL (Conference on Data Systems Languages) DBMSs.	Gartner Glossary
Remote access	Access to an organizational information system by a user (or an information system) communicating through an external, nonorganization-controlled network (e.g., the Internet).	NIST Glossary
Report	A detailed account or statement. For purposes of IT, the report provides analysis that supports informed decision-making.	Merriam-Webster
Request for information (RFI)	A market research tool used to obtain price, delivery, capabilities, and interest for planning purposes. Also referred to as a sources-sought notice.	GSA, "RFP, RFI, and RFQ: Understanding the Difference"
Request for proposal (RFP)	A solicitation method which communicates the [entity's] requirements and requests proposals.	GSA, "RFP, RFI, and RFQ: Understanding the Difference"
Request for quote (RFQ)	A solicitation method used to obtain price, cost, delivery, and related information from suppliers.	GSA, "RFP, RFI, and RFQ: Understanding the Difference"

Term	Definition	Source
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.	NIST Glossary
Role-based access	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.	NIST Glossary
Rollback	Updates to earlier firmware versions may provide a means to recover from a firmware update that is not functioning correctly.	NIST SP 800-193, Platform Firmware Resiliency Guidelines
	A means to recover from an update that is not functioning correctly or restore to a previous secure and functional version that may require the physical presence of a user.	FFIEC Adapted for Supervisory Purposes
Runtime	The period during which a computer program is executing.	NIST Glossary
S		
Sanitization	Actions taken to render data written on media unrecoverable by ordinary and, for some forms of sanitization, extraordinary means.	NIST Glossary
Scalability	Refers to how well a hardware and software system can adapt to increased demands. For example, a scalable network system would be one that can start with just a few nodes but can easily expand to thousands of nodes. Scalability can be a very important feature because it means the entity can invest in a system with confidence that the entity will not quickly outgrow it.	FFIEC Developed for Supervisory Purposes
Scheduling	A method used in the information processing facility to determine and establish the sequence of computer job processing.	ISACA Glossary
Scope creep	Also referred to as requirement creep, this refers to uncontrolled changes in a project's scope. Scope creep can occur when the scope of a project is not properly defined, documented, and controlled. Typically, the scope increase consists of either new products or new features of already approved products. Hence, the project team drifts away from its original purpose. Because of one's tendency to focus on only one dimension of a project, scope creep can also result in a project team overrunning its original budget and schedule. For example, scope creep can be a result of poor change control, lack of proper identification of what products and features are required to bring about the achievement of project objectives in the first place, or a weak project manager or executive sponsor.	ISACA Glossary
	Scope creep refers to uncontrolled changes in a project's scope, adding features and functionality without addressing the effects on time, costs, and resources. These changes may result from a lack of effective project change management, without approval (e.g., management or customer), or when the scope is not properly defined, documented, and controlled.	FFIEC Adapted for Supervisory Purposes
Secure code review	The process of auditing the source code of an application to verify that the proper security and logical controls are present, that they work as intended, and that they have been invoked in the right places. Code review aims to identify security flaws in the application related to its features and design, along with the exact root causes.	OWASP, Code Review Guide 2.0
	The process of auditing the source code of an application to verify that the proper security and logical controls are present, work as intended, and have been invoked in the right places.	FFIEC Adapted for Supervisory Purposes
Secure development	A hardware and software development approach with an objective of building systems and components while minimizing the potential for vulnerabilities and reducing the attack surface. This is done through measures such as secure coding practices, comprehensive development testing, and built-in security mechanisms (e.g., access control, authentication, and logging capabilities).	FFIEC Developed for Supervisory Purposes
Security	The state in which the integrity, confidentiality, and accessibility of information, service or network entity is assured.	NIST Glossary

Term	Definition	Source
Security impact analysis	The analysis conducted by qualified staff in an organization to determine the extent to which changes to the system affect the security posture of the system.	NIST 800-128, Guide for Security-Focused Configuration Management of Information Systems
Security testing	Testing that attempts to verify that an implementation protects data and maintains functionality as intended.	NIST Glossary
	Testing that attempts to verify that a modified or new system implementation includes appropriate controls and does not introduce any security holes that might compromise other systems or allow for any misuse of the system or its information and protects data and maintains functionality as intended.	FFIEC Adapted for Supervisory Purposes
Server	A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).	NIST Glossary
Service deregistration	Removal of a service from the service registry.	FFIEC Developed for Supervisory Purposes
Service discovery	The process by which an application learns what services are available on the network, and by which the network learns what services the application can provide.	Science Direct Topics in Computer Science
Service improvement	The actions taken to identify and execute methods to improve an entity's services and align them with its business objectives.	FFIEC Developed for Supervisory Purposes
Service level agreement (SLA)	Defines the specific responsibilities of the service provider and sets the customer expectations.	NIST Glossary
	A formal agreement between two parties that records a common understanding about products or services to be delivered, priorities, responsibilities, guarantees, and warranties between the parties. In addition, the agreement describes the nature, quality, security, availability, scope, and timeliness of delivery and response of the parties, the point(s) of contact for end-user problems, and the metrics by which the effectiveness of the process is monitored and approved and may include other measurable objectives. The agreement should cover not only expected day-to-day situations, but also unexpected or adverse events, as the need for the service may vary.	FFIEC Adapted Definition for Supervisory Purposes
Service mesh	A distributed computing middleware that optimizes communications between application services.	NIST SP 800-204A, Building Secure Microservices-Based Applications Using Service-Mesh Architecture
Service registration	The service registry service is used by microservices that are coming online to publish their locations in a process referred to as service registration and is used by microservices seeking to discover registered services.	NIST Glossary
	The process of microservices using the registry service to publish their locations when they come online. It is used by microservices seeking to discover other registered services.	FFIEC Adapted for Supervisory Purposes
Service registry	A directory where new service instances created for the microservices-based application register themselves while service instances going offline are deleted from it.	NIST SP 800-204A, Building Secure Microservices-Based Applications

Term	Definition	Source
		Using Service-Mesh Architecture
Shadow IT	Refers to unauthorized hardware and other devices, software, or services operating in an entity's IT environment.	FFIEC Developed for Supervisory Purposes
Signature	A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.	NIST Glossary
Signature-based detection	This intrusion detection method compares network traffic to a set of pre-defined signatures and triggers an alert when a match is detected. Signatures are derived from numerous sources and are specific machine-readable patterns of network traffic that affect the integrity, confidentiality, or availability of computer networks, systems, and information.	DHS, Privacy Impact Assessment for the National Cybersecurity Protection System (NCPS) - Intrusion Detection
Single point of failure	An element in the design, configuration, or implementation of a system that can cause the entire system to fail if it stops working.	FFIEC Developed for Supervisory Purposes
Social engineering	The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.	NIST Glossary
Software	Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.	NIST Glossary
Software as a service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.	NIST Glossary
Software bill of material (SBOM)	A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open-source and commercial software components. The SBOM enumerates these components in a product.	NIST Glossary
Source code	Computer commands written in a computer programming language that is meant to be read by people.	U.S. Department of Commerce, "Open Source Code"
	Computer commands written in a computer programming language that is meant to be read by people. Source code is not executable by the computer directly. It must first be converted (e.g., via compiler, assembler) into a machine language.	FFIEC Adapted for Supervisory Purposes
Spiral model	The "Spiral" model divides a software development project into several smaller projects that address the major risks first.	NIST IR 7499, Guidelines for Planning and Development of Software for Buildings and Building Systems
	A risk-driven software development process model that divides a software development project into several smaller projects that address the major risks first. The model illustrates activities (e.g., requirements analysis, preliminary and detailed design, coding, integration, and testing) that are performed iteratively until development is complete.	FFIEC Adapted for Supervisory Purposes

Term	Definition	Source
Standard image	The approved set of server configurations, applications, and systems, which can be used to deploy servers consistently and rebuild them more easily and quickly, when necessary.	FFIEC Developed for Supervisory Purposes
Standards	Rules, conditions, or requirements describing the following information for products, systems, services or practices: (i) Classification of components. (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures.	NIST Glossary
State	A condition or mode of existence in which a system, component or simulation may be, e.g., the preflight state of an aircraft navigation program or the input state of a given channel.	ISACA Glossary
	A condition or mode of existence in which a system, component, or simulation (including stored data and inputs) may be at a given point in time.	FFIEC Adapted for Supervisory Purposes
Stateful	Refers to a data representation or a process that is dependent on an external data store.	NIST Glossary
	Refers to a data representation or a process that is dependent on some external information or other process and has the ability to retain or store the data for reuse.	FFIEC Adapted for Supervisory Purposes
Stateful inspection	Packet filtering that tracks the state of connections and blocks packets that deviate from the expected state.	NIST Glossary
Stateful protocol analysis	A firewalling capability that improves upon standard stateful inspection by adding basic intrusion detection technology. This technology consists of an inspection engine that analyzes protocols at the application layer to compare vendor-developed profiles of benign protocol activity against observed events to identify deviations, allowing a firewall to allow or deny access based on how an application is running over a network.	NIST Glossary
Stateless	Refers to a data representation or a process that is self-contained and does not depend on any external data store.	NIST Glossary
	Refers to a data representation or a process that is self-contained and does not depend on any external information or other process and it does not store or reuse data.	FFIEC Adapted for Supervisory Purposes
Statement of objective (SOO)	When the government is open to a wide range of solutions to meet their objective(s), it will use a SOO. You will need to develop and include in your offer a proposed PWS (i.e., your solutions), performance metrics, a measurement plan, and a quality assurance plan.	GSA
	When an entity is open to a wide range of solutions to meet their objective(s), it may use a SOO. You will need to develop and include in your offer a proposed PWS (i.e., your solutions), performance metrics, a measurement plan, and a quality assurance plan.	FFIEC Adapted for Supervisory Purposes
Statement of work (SOW)	A document that details the developer's responsibilities in the performance of the contract. Documentation developed under the contract, for example, is specified in the SOW. Security assurance requirements, which detail many aspects of the processes the developer follows and what evidence must be provided to assure the organization that the processes have been conducted correctly and completely, may be specified in the SOW.	NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems
Static analysis	Detecting software vulnerabilities by examining the app source code and binary code and attempting to reason over all possible behaviors that might arise at runtime. Also referred to as static testing.	NIST 800-163, rev. 1, Vetting the Security of Mobile Applications
Structured data	Data that has a predefined data model or is organized in a predefined way.	NIST SP 1500-1r2, NIST Big Data Interoperability Framework: Vol. 1, Definitions
Subcontractor	An individual or business firm contracting to perform part or all of another's contract.	Merriam-Webster

Term	Definition	Source
Supplier	Organization or an individual that enters into an agreement with the acquirer for the supply of a product or service.	NIST Glossary
	External or internal organization, business unit, or individual that enters into an agreement with the acquirer for the supply of a product, component, or service. This includes suppliers, developers, and manufacturers in the supply chain.	FFIEC Adapted for Supervisory Purposes
Supply chain	A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.	NIST Glossary
Supply chain risk management (SCRM)	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.	NIST Glossary
	The process of identifying, assessing, and mitigating the risks interconnected throughout the supply chains and their components, such as susceptibilities, vulnerabilities, and threats, associated with the global and distributed nature of information and communications technology product and service supply chains.	FFIEC Adapted for Supervisory Purposes
System	A combination of interacting elements organized to achieve one or more stated purposes.	NIST Glossary
System and organization controls (SOC)	The suite of services CPAs may provide relating to system-level controls of a service organization and system- or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the American Institute of Certified Public Accountants [AICPA] enables the introduction of new internal control examinations that may be performed (a) for other types of organizations, in addition to service organizations, and (b) on either system-level or entity-level controls of such organizations.	AICPA, System and Organization Controls: SOC Suite of Services
System development life cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.	NIST Glossary
System test	A test performed on a complete system to evaluate its compliance with specified requirements.	NIST Glossary
T		
Telecommunications	The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.	NIST Glossary
Term of support	The length of time for which the device will be supported by the manufacturer or supporting parties for such actions and materials as part replacements, software updates, vulnerability notices, technical support questions, etc.	NIST Glossary
	The length of time for which the software, hardware, or service will be supported by the manufacturer or supporting parties for such actions and materials as part replacements, software updates, vulnerability notices, and technical support questions.	FFIEC Adapted for Supervisory Purposes
Third-party service provider	Any independent party to whom an entity outsources activities that the entity itself is authorized to perform, including a technology service provider.	FFIEC Developed for Supervisory Purposes
Threat intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.	NIST Glossary
Threat model	A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment.	NIST Glossary
Transmission	An act, process, or instance of transmitting.	Merriam-Webster
	The act of sending or conveying data, voice, audio, or video from one person or place to another.	FFIEC Adapted for Supervisory Purposes

Term	Definition	Source
U		
Unit testing	A testing technique that is used to test program logic in a particular program or module. The purpose of the test is to ensure that the internal operation of the program performs according to specification. It uses a set of test cases that focus on the control structure of the procedural design.	ISACA Glossary
Unstructured data	Data that does not have a predefined data model or is not organized in a predefined way.	NIST SP 1500-1r2, NIST Big Data Interoperability Framework: Vol. 1, Definitions
Useful life	The normal expected operating life of an asset.	Internal Revenue Service
User acceptance testing (UAT)	Testing that involves taking use cases or procedures for how the system was designed to perform and ensuring that someone who follows the procedure gets the intended result; however, it does not necessarily demonstrate how well the system supports users in performing those functions.	NIST IR 7741, NIST Guide to the Processes Approach for Improving the Usability of Electronic Health Records
V		
Virtualization	The simulation of the software and/or hardware upon which other software runs.	NIST Glossary
Virtual machine (VM)	Software that allows a single host to run one or more guest operating systems.	NIST Glossary
	A simulated environment created by virtualization using software that allows a single host to run one or more guest operating systems.	FFIEC Adapted for Supervisory Purposes
Vulnerability	Weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.	NIST Glossary
Vulnerability assessment	Systematic examination of an information system or product to determine the adequacy of security and privacy measures, identify security and privacy deficiencies, provide data from which to predict the effectiveness of proposed security and privacy measures, and confirm the adequacy of such measures after implementation.	NIST Glossary
Vulnerability management	The practice of identification, classification, remediation, and mitigation of vulnerabilities in systems, subsystems, and system components.	DoD Instruction 8531.01; DoD Vulnerability Management
Vulnerability scanning	A technique used to identify hosts/host attributes and associated vulnerabilities.	NIST Glossary
W		
Workstation	A computer used for tasks such as programming, engineering, and design.	NIST Glossary
Z		
Zero-day exploit	Referred to as zero-day attack; an attack that exploits a previously unknown hardware, firmware, or software vulnerability.	NIST Glossary
	An exploit that exploits a previously unknown hardware, firmware, or software vulnerability.	FFIEC Adapted for Supervisory Purposes

APPENDIX C: ABBREVIATIONS

AI	artificial intelligence
AICPA	American Institute of Certified Public Accountants
API	application programming interface
ATM	automated teller machine
CA	Consumer Affairs (for FRB SR Letters)
CCB	configuration or change control board
CD	continuous delivery
CFPB	Consumer Financial Protection Bureau
CFR	Code of Federal Regulations
CI	continuous integration
CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	chief information security officer
COTS	commercial off-the-shelf
CPU	central processing unit
DevOps	development and operations
DevSecOps	development security operations
DOD	Department of Defense
EOL	end-of-life
EULA	end user license agreement
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
Fintech	financial technology
FOSS	free and open-source software
FIL	Financial Institution Letter
FRB	Board of Governors of the Federal Reserve System
FS-ISAC	Financial Services Information Sharing and Analysis Center
FTC	Federal Trade Commission
GLBA	Gramm–Leach–Bliley Act
GSA	U.S. General Services Administration
HVAC	heating, ventilation, and air conditioning
IaaS	infrastructure-as-a-service
IoT	internet of things
IR	Internal Report
ISACA	Information Systems Audit and Control Association
ISAC	information sharing and analysis center
IT	information technology
ITAM	IT asset management
ITL	Information Technology Laboratory
ITRM	IT risk management
FFIEC IT Handbook	FFIEC Information Technology Examination Handbook
MFA	multifactor authentication
MSA	master services agreement
NCUA	National Credit Union Administration

NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OCC	Office of the Comptroller of the Currency
OEM	original equipment manufacturer
OFAC	Office of Foreign Assets Control
OWASP	Open Worldwide Application Security Project
OS	operating system
PaaS	platform-as-a-service
PIR	post-implementation review
PMI	Project Management Institute
PMO	program management office
PWS	performance work statement
QA	quality assurance
QC	quality control
RAM	random access memory
RFI	request for information
RFID	radio frequency identification
RFP	request for proposal
RFQ	request for quote
SaaS	software-as-a-service
SBOM	software bill of material
SCRM	supply chain risk management
SDLC	system development life cycle
SLA	service-level agreement
SLC	State Liaison Committee
SOC	security operations center
SOC	system and organization control
SOW	statement of work
SP	Special Publication
SQL	Structured Query Language
SR	Supervision and Regulation Letter
UAT	user acceptance testing
USB	universal serial bus
USC	U.S. Code

APPENDIX D: REFERENCES

Laws

- 11 USC 101–112, “[Bankruptcy](#)” and “[Office of the Law Revision Counsel: U.S. Code; Title 11](#)”
- 12 USC 226, “[Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978](#)”
- 12 USC 1461–1468, “[Home Owners’ Loan Act](#)”
- 12 USC 1813.3(u), “[Institution-Affiliated Party](#)”
- 12 USC 1841–1852, “[Bank Holding Company Act](#)”
- 12 USC 1861–1867, “[Bank Service Company Act](#)”
- 12 USC 1882, “[Bank Protection Act of 1968](#)”
- 12 USC 5481(14) and (26), 5514, 5515, and 5531, “[Dodd–Frank Wall Street Reform and Consumer Protection Act](#)”
- 15 USC 1681w, “[Fair and Accurate Credit Transactions Act](#)”
- 15 USC 6801–6809 and 6821–6827, “Financial Modernization Act of 1999” (“[Gramm–Leach–Bliley Act](#)” [GLBA])
- 17 USC 1–8, 10–12, “[Copyright Law of the United States](#)”
- 18 USC 1030, “[Fraud and Related Activity in Connection With Computers](#)”
- 29 USC 794d, “[Rehabilitation Act of 1973, Section 508](#)”

Consumer Financial Protection Bureau

Regulations

- 12 CFR 1005, “[Electronic Fund Transfers \(Regulation E\)](#)”
- 12 CFR 1016, “[Privacy of Consumer Financial Information \(Regulation P\)](#)”
- 12 CFR 1022, “[Fair Credit Reporting Act \(Regulation V\)](#)”

Guidance

CFPB Compliance Bulletin and Policy Guidance 2016-02, “[Service Providers](#)” (October 2016)

Federal Deposit Insurance Corporation

Regulations

- 12 CFR 304.3(d), “[Notification of Performance of Bank Services, Form FDIC 6120/06](#)”
- 12 CFR 326, subpart A, “[Minimum Security Procedures](#)”
- 12 CFR 332, “[Privacy of Consumer Financial Information](#)”
- 12 CFR 364, appendix A, “[Interagency Guidelines Establishing Standards for Safety and Soundness](#)”

- 12 CFR 364, appendix B, “[Interagency Guidelines Establishing Information Security Standards](#)”
- 12 CFR 364, supplement A to appendix B, “[Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#)”

Guidance

- FIL-29-2023, “[Interagency Guidance on Third-Party Relationships: Risk Management](#)” (June 6, 2023)
- FIL-10-2023, “[Financial Institutions Are Required to Meet Contractual Obligations With Bridge Banks](#)” (March 14, 2023)
- FIL-08-2023, “[Joint Statement on Liquidity Risks to Banking Organizations Resulting From Crypto-Asset Market Vulnerabilities](#)” (February 23, 2023)
- FIL-01-2023, “[Joint Statement on Crypto-Asset Risks to Banking Organizations](#)” (January 5, 2023)
- FIL-35-2022, “[Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings With Crypto Companies](#)” (July 29, 2022)
- FIL-30-2022, “[FDIC Updates on Brokered Deposits](#)” (July 15, 2022)
- FIL-16-2022, “[Notification of Engaging in Crypto-Related Activities](#)” (April 7, 2022)
- FIL-12-2022, “[Computer-Security Incident Notification Implementation](#)” (March 29, 2022)
- FIL-74-2021, “[Computer-Security Incident Notification Final Rule](#)” (November 18, 2021)
- FIL-59-2021, “[Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks](#)” (August 27, 2021)
- FIL-55-2021, “[Authentication and Access to Financial Institution Services and Systems](#)” (August 11, 2021)
- FIL-27-2021, “[Bank Secrecy Act: Agencies Address Model Risk Management for Bank Models and Systems Supporting Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Assets Control Compliance](#)” (April 9, 2021)
- FIL-103-2020, “[The FDIC Publishes Sound Practices to Strengthen Operational Resilience](#)” (November 2, 2020)
- FIL-52-2020, “[FFIEC Joint Statement on Risk Management for Cloud Computing Services](#)” (April 30, 2020)
- FIL-14-2020, “[Interagency Statement on Pandemic Planning](#)” (March 6, 2020)
- FIL-19-2019, “[Technology Service Provider Contracts](#)” (April 2, 2019)
- FIL-16-2018, “[FFIEC Issues Joint Statement: Cyber Insurance and Its Potential Role in Risk Management Programs](#)” (April 10, 2018)
- FIL-68-2016, “[FFIEC Cybersecurity Assessment Tool: Frequently Asked Questions](#)” (October 18, 2016)
- FIL-43-2016, “[Information Technology Risk Examination \(InTREx\) Program](#)” (June 30, 2016)
- FIL-37-2016, “[FFIEC Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks](#)” (June 7, 2016)
- FIL-28-2015, “[Cybersecurity Assessment Tool](#)” (July 2, 2015)
- FIL-13-2015, “[FFIEC Joint Statements on Destructive Malware and Compromised Credentials](#)” (March 30, 2015)

- FIL-49-2014, “[Technology Alert: GNU Bourne-Again Shell \(Bash\) Vulnerability](#)” (September 29, 2014)
- FIL-41-2014, “[FDIC Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors](#)” (July 28, 2014)
- FIL-16-2014, “[Technology Alert: OpenSSL “Heartbleed” Vulnerability](#)” (April 11, 2014)
- FIL-13-2014, “[Technology Outsourcing: Informational Tools for Community Bankers](#)” (April 7, 2014)
- FIL-3-2012, “[Payment Processor Relationships Revised Guidance \(Revised July 2014\)](#)” (January 31, 2012)
- FIL-4-2009, “[Risk Management of Remote Deposit Capture](#)” (January 14, 2009)
- FIL-127-2008, “[Guidance on Payment Processor Relationships](#)” (November 7, 2008)
- FIL-44-2008, “[Third-Party Risk: Guidance for Managing Third-Party Risk](#)” (June 6, 2008)
- FIL-77-2006, “[Authentication in an Internet Banking Environment: Frequently Asked Questions](#)” (August 21, 2006)
- FIL-52-2006, “[Foreign-Based Third-Party Service Providers: Guidance on Managing Risks in These Outsourcing Relationships](#)” (June 21, 2006)
- FIL-69-2005, “[Voice Over Internet Protocol: Guidance on the Security Risks of VoIP](#)” (July 27, 2005)
- FIL-66-2005, “[Spyware: Guidance on Mitigating Risks From Spyware](#)” (July 22, 2005)
- FIL-121-2004, “[Computer Software Due Diligence Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance](#)” (November 16, 2004)
- FIL-114-2004, “[Risk Management of Free and Open Source Software](#)” (October 21, 2004)
- FIL-84-2004, “[Guidance on Instant Messaging](#)” (July 21, 2004)
- FIL-27-2004, “[Guidance on Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes](#)” (March 12, 2004)
- FIL-43-2003, “[Guidance on Developing an Effective Software Patch Management Program](#)” (May 29, 2003)
- FIL-30-2003, “[Federal Bank and Credit Union Regulatory Agencies Jointly Issue Guidance on the Risks Associated With Weblinking](#)” (April 23, 2003)
- FIL-8-2002, “[Guidance on Managing Risks Associated With Wireless Networks and Customer Access](#)” (February 1, 2002)
- FIL-50-2001, “[Bank Technology Bulletin on Outsourcing](#)” (June 4, 2001)
- FIL-81-2000, “[FFIEC Guidance on Managing Risks Associated With Outsourcing Technology Services](#)” (November 29, 2000)
- FIL-49-1999, “[Bank Service Company Act](#)” (June 3, 1999)
- FIL-12-99, “[FFIEC Adopts Updated Uniform Rating System for Information Technology](#)” (February 5, 1999)
- FIL-82-96, “[Interagency Statement on the Risks to Financial Institutions Involving Client/Server Computer Systems](#)” (October 8, 1996)
- FIL-46-95, “[Minimum Security Devices and Procedures](#)” (July 7, 1995)

Note: While listed FIL announcements may be noted as inactive, the underlying guidance remains in effect, unless specifically superseded or rescinded.

Board of Governors of the Federal Reserve System

Regulations

Regulation H

- 12 CFR 208, appendix D-1, “[Interagency Guidelines Establishing Standards for Safety and Soundness](#)”
- 12 CFR 208, appendix D-2, “[Interagency Guidelines Establishing Information Security Standards](#)”
- 12 CFR 208.61, “[Bank Security Procedures](#)”

Regulation K

- 12 CFR 211.5 and 211.24 (i), “[Protection of Customer and Consumer Information](#)”

Regulation Y

- 12 CFR 225, appendix F, “[Interagency Guidelines Establishing Information Security Standards](#)”

Guidance

- SR Letter 23-4, “[Interagency Guidance on Third-Party Relationships: Risk Management](#)” (June 7, 2023)
- SR Letter 22-4/CA 22-3, “[Contact Information in Relation to Computer-Security Incident Notification Requirements](#)” (March 29, 2022)
- SR Letter 21-14, “[Authentication and Access to Financial Institution Services and Systems](#)” (August 11, 2021)
- SR Letter 20-24, “[Interagency Paper on Sound Practices to Strengthen Operational Resilience](#)” (November 2, 2020)
- SR Letter 20-3/CA 20-2, “[Interagency Statement on Pandemic Planning](#)” (March 10, 2020)
- SR Letter 16-11, “[Supervisory Guidance for Assessing Risk Management at Supervised Institutions With Total Consolidated Assets Less than \\$100 Billion](#)” (June 8, 2016, revised February 17, 2021)
- SR Letter 15-9, “[FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors](#)” (July 2, 2015)
- SR Letter 12-17/CA 12-14, “[Consolidated Supervision Framework for Large Financial Institutions](#)” (December 17, 2012)
- SR Letter 11-7, “[Guidance on Model Risk Management](#)” (April 4, 2011)
- SR Letter 05-23/CA 05-10, “[Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#)” (December 1, 2005)
- SR Letter 04-17, “[FFIEC Guidance on the Use of Free and Open Source Software](#)” (December 6, 2004)
- SR Letter 01-15, “[Standards for Safeguarding Customer Information](#)” (May 31, 2001)
- SR Letter 99-8, “[Uniform Rating System for Information Technology](#)” (March 31, 1999)
- SR Letter 98-9, “[Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations](#)” (April 20, 1998, revised February 26, 2021)

SR Letter 96-14, “[Risk-Focused Safety and Soundness Examinations and Inspections](#)” (May 24, 1996)

National Credit Union Administration

Regulations

- 12 CFR 748, “[Security Program, Suspicious Transactions, Catastrophic Acts, Cyber Incidents, and Bank Secrecy Act Compliance](#)”
- 12 CFR 748, appendix A, “[Guidelines for Safeguarding Member Information](#)”
- 12 CFR 749, “[Records Preservation Program and Appendices—Record Retention Guidelines; Catastrophic Act Preparedness Guidelines](#)”
- 12 CFR 749, appendix A, “[Record Retention Guidelines](#)”

Guidance

- Letter to Credit Unions 22-CU-07, “[Federally Insured Credit Union Use of Distributed Ledger Technologies](#)” (May 2022)
- Letter to Credit Unions 07-CU-13, “[Evaluating Third Party Relationships](#)” (December 2007)
- Letter to Credit Unions 06-CU-07, “[IT Security Compliance Guide for Credit Unions](#)” (April 2006)
- Letter to Credit Unions 03-CU-14, “[Computer Software Patch Management](#)” (September 2003)
- Letter to Credit Unions 01-CU-20, “[Due Diligence Over Third Party Service Providers](#)” (November 2001)
- Letter to Credit Unions 00-CU-11, “[Risk Management of Outsourced Technology Services](#)” (December 2000)

Office of the Comptroller of the Currency

Regulations

- 12 CFR 5.30, “[Establishment, Acquisition, and Relocation of a Branch of a National Bank](#)”
- 12 CFR 5.31, “[Establishment, Acquisition, and Relocation of a Branch and Establishment of an Agency Office of a Federal Savings Association](#)”
- 12 CFR 30, appendix A, “[Interagency Guidelines Establishing Standards for Safety and Soundness](#)”
- 12 CFR 30, appendix B, “[Interagency Guidelines Establishing Information Security Standards](#)”
- 12 CFR 30, appendix D, “[OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches](#)”
- 12 CFR 30, appendix E, “[OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches](#)”
- 12 CFR 41.83, “[Proper Disposal of Records Containing Consumer Information](#)”

Guidance

- OCC Bulletin 2023-22, “[Cybersecurity: Cybersecurity Supervision Work Program](#)” (June 26, 2023)
- OCC Bulletin 2023-17, “[Third-Party Relationships: Interagency Guidance on Risk Management](#)” (June 6, 2023)
- OCC Bulletin 2023-1, “[Crypto-Assets: Joint Statement on Crypto-Asset Risks to Banking Organizations](#)” (January 3, 2023)
- OCC Bulletin 2022-22, “[Cybersecurity: 2022 Cybersecurity Resource Guide for Financial Institutions](#)” (October 6, 2022)
- OCC Bulletin 2022-8, “[Information Technology: OCC Points of Contact for Banks’ Computer-Security Incident Notifications](#)” (March 29, 2022)
- OCC Bulletin 2021-55, “[Computer-Security Incident Notification: Final Rule](#)” (November 23, 2021)
- OCC Bulletin 2021-40, “[Third-Party Relationships: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks](#)” (August 27, 2021)
- OCC Bulletin 2021-36, “[Information Security: FFIEC Statement on Authentication and Access to Financial Institution Services and Systems](#)” (August 11, 2021)
- OCC Bulletin 2021-30, “[FFIEC Information Technology Examination Handbook: New Architecture, Infrastructure, and Operations Booklet](#)” (June 30, 2021)
- OCC Bulletin 2021-17, “[Artificial Intelligence: Request for Information on Financial Institutions’ Use of Artificial Intelligence, Including Machine Learning](#)” (March 31, 2021)
- OCC Bulletin 2020-94, “[Operational Risk: Sound Practices to Strengthen Operational Resilience](#)” (October 30, 2020)
- OCC Bulletin 2020-46, “[Cybersecurity: Joint Statement on Security in a Cloud Computing Environment](#)” (April 30, 2020)
- OCC Bulletin 2020-23, “[Pandemic Planning: Essential Critical Infrastructure Workers in the Financial Services Sector](#)” (March 25, 2020)
- OCC Bulletin 2020-13, “[Pandemic Planning: Updated FFIEC Guidance](#)” (March 6, 2020)
- OCC Bulletin 2020-5, “[Cybersecurity: Joint Statement on Heightened Cybersecurity Risk](#)” (January 16, 2020)
- OCC Bulletin 2019-57, “[FFIEC Information Technology Examination Handbook: Revised Business Continuity Management Booklet](#)” (November 14, 2019)
- OCC Bulletin 2019-37, “[Operational Risk: Fraud Risk Management Principles](#)” (July 24, 2019)
- OCC Bulletin 2019-13, “[Recovery Planning: Updated Comptroller's Handbook Booklet and Rescissions](#)” (March 15, 2019)
- OCC Bulletin 2018-40, “[Cybersecurity: Cyber-Related Sanctions](#)” (November 5, 2018)
- OCC Bulletin 2017-43, “[New, Modified, or Expanded Bank Products and Services: Risk Management Principles](#)” (October 20, 2017)
- OCC Bulletin 2017-7, “[Third-Party Relationships: Supplemental Examination Procedures](#)” (January 24, 2017)
- OCC Bulletin 2016-34, “[Cybersecurity: Frequently Asked Questions on the FFIEC Cybersecurity Assessment Tool](#)” (October 17, 2016)

- OCC Bulletin 2016-18, "[Cybersecurity of Interbank Messaging and Wholesale Payment Networks: FFIEC Statement](#)" (June 7, 2016)
- OCC Bulletin 2015-44, "[FFIEC Information Technology Examination Handbook: Revised Management Booklet](#)" (November 10, 2015)
- OCC Bulletin 2015-40, "[Cybersecurity: Joint Statement on Cyber Attacks Involving Extortion](#)" (November 3, 2015)
- OCC Bulletin 2015-31, "[Cybersecurity: FFIEC Cybersecurity Assessment Tool](#)" (June 30, 2015)
- OCC Bulletin 2015-20, "[Cybersecurity: Destructive Malware Joint Statement](#)" (March 30, 2015)
- OCC Bulletin 2015-19, "[Cybersecurity: Cyber Attacks Compromising Credentials Joint Statement](#)" (March 30, 2015)
- OCC Bulletin 2014-48, "[Bourne-Again Shell \(Bash\) 'Shellshock' Vulnerability: FFIEC Alert](#)" (September 26, 2014)
- OCC Bulletin 2014-17, "[Information Security Vulnerability in OpenSSL Encryption Tool \(Heartbleed\): Joint Statement](#)" (April 25, 2014)
- OCC Bulletin 2014-13, "[Cyber Attacks on Financial Institutions' Automated Teller Machine and Card Authorization Systems: Joint Statement](#)" (April 2, 2014)
- OCC Bulletin 2011-12, "[Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management](#)" (April 4, 2011)
- OCC Bulletin 2008-16, "[Information Security: Application Security](#)" (May 8, 2008)
- OCC Bulletin 2006-35, "[Authentication in an Internet Banking Environment: Frequently Asked Questions](#)" (August 15, 2006)
- OCC Bulletin 2006-31, "[FFIEC Information Security Booklet: Information Security Guidance](#)" (July 27, 2006)
- OCC Bulletin 2005-13, "[Response Programs for Unauthorized Access to Customer Information and Customer Notice - Final Guidance: Interagency Guidance](#)" (April 14, 2005)
- OCC Bulletin 2004-47, "[FFIEC Guidance: Risk Management for the Use of Free and Open Source Software](#)" (October 27, 2004)
- OCC Bulletin 2004-32, "[FFIEC Information Technology Examination Handbook: FFIEC IT Booklets on Outsourcing Technology Services and Management](#)" (July 15, 2004)
- OCC Bulletin 2002-16, "[Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance](#)" (May 15, 2002)
- OCC Bulletin 2002-10, "[Country Risk: Sound Risk Management Practices](#)" (March 11, 2002)
- OCC Bulletin 2001-35, "[Examination Procedures to Evaluate Compliance With the Guidelines to Safeguard Customer Information: Examination Procedures](#)" (July 18, 2001)
- OCC Bulletin 2001-12, "[Bank-Provided Account Aggregation Services: Guidance to Banks](#)" (February 28, 2001)
- OCC Bulletin 1998-31, "[Guidance on Electronic Financial Services and Consumer Compliance: FFIEC Guidance](#)" (July 30, 1998)
- OCC Bulletin 1998-3, "[Technology Risk Management: Guidance for Bankers and Examiners](#)" (February 4, 1998)

Other References

Federal Regulations

16 CFR 314 (FTC), “[Standards for Safeguarding Customer Information](#)”

16 CFR 314.4(j) (FTC), “[Amendment to Standards for Safeguarding Customer Information](#)”

National Institute of Standards and Technology (NIST)

[NIST, “Automated Identification Technologies for Forensic Science”](#)

[NIST Glossary](#)

[National Checklist Program](#) (security configurations)

[National Vulnerability Database](#)

NIST Advanced Manufacturing Series 100-40, [Agile for Model-Based-Standards Development](#)

NIST SP 500-292, [NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology](#)

NIST SP 500-316, [Framework for Cloud Usability](#)

NIST SP 800-28, version 2, [Guidelines on Active Content and Mobile Code](#)

NIST SP 800-37, rev. 2, [Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#)

NIST SP 800-47, rev. 1, [Managing the Security of Information Exchanges](#)

NIST SP 800-53, rev. 5, [Security and Privacy Controls for Information Systems and Organizations](#)

NIST SP 800-53, rev. 5, SR-3, [Supply Chain Controls and Processes](#)

NIST SP 800-58, [Security Considerations for Voice Over IP Systems](#)

NIST SP 800-63-3, [Digital Identity Guidelines](#)

NIST SP 800-82, rev. 3, [Guide to Operational Technology \(OT\) Security](#)

NIST 800-98, [Guidelines for Securing Radio Frequency Identification \(RFID\) Systems](#)

NIST SP 800-115, [Technical Guide to Information Security Testing and Assessment](#)

NIST SP 800-125, [Guide to Security for Full Virtualization Technologies](#)

NIST SP 800-128, [Guide for Security-Focused Configuration Management of Information Systems](#)

NIST SP 800-137, [Information Security Continuous Monitoring \(ISCM\) for Federal Systems and Organizations](#)

NIST SP 800-145, [The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology](#)

NIST SP 800-146, [Cloud Computing Synopsis and Recommendations](#)

NIST SP 800-160, vol. 1, rev. 1, [Engineering Trustworthy Secure Systems](#)

NIST SP 800-160, vol. 2, rev. 1, [Developing Cyber Resilient Systems: A Systems Security Engineering Approach](#)

NIST SP 800-161r1, [Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#)

NIST SP 800-163, rev. 1, [Vetting the Security of Mobile Applications](#)

NIST SP 800-190, [Application Container Security Guide](#)

NIST SP 800-193, [Platform Firmware Resiliency Guidelines](#)

NIST SP 800-204, [*Security Strategies for Microservices-Based Application Systems*](#)
 NIST SP 800-204A, [*Building Secure Microservices-Based Applications Using Service-Mesh Architecture*](#)
 NIST SP 800-204C, [*Implementation of DevSecOps for a Microservices-Based Application With Service Mesh*](#)
 NIST SP 800-207, [*Zero Trust Architecture*](#)
 NIST SP 800-210, [*General Access Control Guidance for Cloud Systems*](#)
 NIST SP 800-218, [*Secure Software Development Framework \(SSDF\) Version 1: Recommendations for Mitigating the Risks of Software Vulnerabilities*](#)
 NIST SP 1500-1r2, [*NIST Big Data Interoperability Framework: Volume 1, Definitions*](#)
 NIST SP 1800-5, [*IT Asset Management*](#)
 NIST SP 1800-16, [*Securing Web Transactions: TLS Server Certificate Management*](#).
 NIST Response to Executive Order 14028, [*Software Security in Supply Chains*](#)
 NIST Information Technology Laboratory (ITL) Bulletin, “[*Security Considerations for Exchanging Files Over the Internet*](#)” (August 2020)
 NIST ITL Bulletin, “[*Security for Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Solutions*](#)”(March 2020)
 NIST ITL Bulletin, “[*The System Development Life Cycle \(SDLC\)*](#)” (April 2009)
 NIST National Construction Safety Team Act Report (NCSTAR) 1-4B, [*Fire Suppression Systems*](#)
 NIST Directive S 6106.01, “[*Open Source Code*](#)”
 NIST Internal Report (IR) 7499, [*Guidelines for Planning and Development of Software for Buildings and Building Systems*](#)
 NIST IR 7622, [*Notional Supply Chain Risk Management for Federal Information Systems*](#)
 NIST IR 7741, [*NIST Guide to the Processes Approach for Improving the Usability of Electronic Health Records*](#)
 NIST IR 8228, [*Considerations for Managing Internet of Things \(IoT\) Cybersecurity and Privacy Risks*](#)
 NIST IR 8259A, [*IoT Device Cybersecurity Capability Core Baseline*](#)
 NIST IR 8397, [*Guidelines on Minimum Standards for Developer Verification of Software*](#)
 NIST IR 8419, [*Block Chain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives*](#)
 NIST IR 8425, [*Profile of the IoT Core Baseline for Consumer IoT Products*](#)

Documents referenced by NIST

Gallagher, Leonard, and Jeff Offutt, “[*Test Sequence Generation for Integration Testing of Component Software*](#),” *Computer Journal*, 2005
 Martzloff, François, [*A New IEC Standard on the Measurement of Power Quality Parameters*](#)
 Rapp, Paul, [*Copyright Law*](#)

Other Federal Government

Bureau of Labor Statistics

Occupational Outlook Handbook

[“Customer Service Representatives”](#)

[“Purchasing Managers, Buyers, and Purchasing Agents”](#)

[“Software Developers, Quality Assurance Analysts, and Testers”](#)

Centers for Disease Control

[“Implementation Phase”](#)

Cybersecurity and Infrastructure Security Agency (CISA)

[“CISA Insights - Cyber: Remediate Vulnerabilities for Internet Accessible Systems”](#)

[*CRR Supplemental Resource Guide, Volume 3: Configuration and Change Management, Version 1.1*](#)

[*CRR Supplemental Resource Guide, Volume 5: Incident Management Resource Guide, Version 1.1*](#)

[“Infrastructure Dependency Primer”](#)

[“Protecting Against Malicious Code”](#)

[*Securing the Software Supply Chain: Recommended Practices Guide for Developers*](#)

[*Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default*](#)

Department of Defense (DOD)

[*DOD Enterprise DevSecOps Fundamentals*](#)

[*DoD Enterprise DevSecOps Reference Design: Version 1.0*](#)

[*Securing Defense-Critical Supply Chains*](#)

[“DoD Open Source Software FAQ”](#)

[*DOD Instruction 8531.01: DoD Vulnerability Management*](#)

Documents referenced by DOD

Davis, Noopur, [*Secure Software Development Life Cycle Processes: A Technology Scouting Report*](#), Carnegie Mellon University Software Engineering Institute (Defense Technical Information Center)

Food and Drug Administration

[Glossary of Computer System Software Development Terminology](#)

National Aeronautics and Space Administration

[A Software Development Simulation Model of a Spiral Process](#) (NASA Technical Reports Server)

National Telecommunications and Information Administration (NTIA)

[Framing Software Component Transparency: Establishing a Common Software Bill of Materials \(SBOM\)](#)

[“SBOM at a Glance”](#)

[“SBOM Myths vs. Facts”](#)

U.S. Department of Commerce

[“Open Source Code”](#)

U.S. Copyright Office

[Copyright Law of the United States \(Title 17\)](#)

[“Copyright in General”](#)

[“What Is Copyright?”](#)

U.S. Department of Energy

[Suspect/Counterfeit Items Awareness Training](#)

U.S. Department of Homeland Security

[Access Control Technologies Handbook](#)

[DHS Lexicon Terms and Definitions](#)

[Privacy Impact Assessment for the National Cybersecurity Protection System \(NCPS\) – Intrusion Detection](#)

[Systems Engineering Life Cycle](#)

U.S. Department of Justice

Systems Development Life Cycle Guidance, chapter 12, [“Disposition Phase”](#)

U.S. Government Accountability Office

[*Information Technology Investment Management*](#)

[*The Post-Implementation Review*](#)

U.S. General Services Administration (GSA)

[“Performance Work Statement”](#)

[“PWS, SOO, SOW - Finding the Best Fit”](#)

[“Respond to a Solicitation”](#)

[“RFP, RFI, and RFQ: Understanding the Difference”](#)

U.S. Patent and Trademark Office

[“Copyright Basics”](#)

[“Trademark, Patent, or Copyright”](#)

State Government**New York State Office of Information Technology Services**

[*NYS Project Management Guidebook Release 2*](#)

[*System Implementation*](#)

Industry References**American Institute of Certified Public Accountants (AICPA)**

[*System and Organization Controls: SOC Suite of Services*](#)

[“What Are You Doing to Prevent Cyberattacks? SOC 2 and SOC for Cybersecurity: How They’re Different and How They Can Help”](#)

Center for Internet Security

[“CIS Critical Security Control 7: Continuous Vulnerability Management”](#)

Cloud Security Alliance

[“Understanding the OWASP API Security Top 10”](#)

Creative Commons

[CC0](#)

Financial Accounting Standards Board

[“Post-Implementation Review”](#)

[Financial Services Information Sharing and Analysis Center](#) (FS-ISAC)

Information Systems Audit and Control Association (ISACA)

[ISACA Glossary](#)

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)

[ISO Online Browsing Platform, Terms & Definitions](#)

Internet Engineering Task Force (IETF)

[“OAuth 2.0 Dynamic Client Registration Protocol”](#)

The MITRE Corporation ([MITRE](#))

[*Improperly Controlled Modification of Dynamically-Determined Object Attributes*](#)

The National Automated Clearinghouse Association ([Nacha](#))

[National Council of ISACs](#)

Open Worldwide Application Security Project ([OWASP](#))

[“OWASP API Security Project”](#)

[*Component Analysis*](#)

[*Fuzzing*](#)

[*OWASP Vulnerability Management Guide \(OVMG\)*](#)

[*Code Review Guide 2.0*](#)

[Payments Card Industry \(PCI\) Security Standards Council](#)

Project Management Institute ([PMI](#))

[A Guide to the Project Management Body of Knowledge](#), fifth edition

[“Running IS Maintenance as a Project”](#)

[“Statement of Work: The Foundation for Delivering Successful Service Projects”](#)

[“What Is Project Management?”](#)

[“Is This Really Worth the Effort? The Need for a Business Case”](#)

Society for Human Resource Management

[“Top Database Security Threats and How to Mitigate Them”](#)

Other References

[Black’s Law Dictionary](#)

[Law Insider Dictionary](#)

[“IT Security Health Check”](#)



FFIEC Information Technology Examination Handbook

Information Security

SEPTEMBER 2016

Contents

INTRODUCTION.....	1
I GOVERNANCE OF THE INFORMATION SECURITY PROGRAM.....	3
I.A Security Culture.....	3
I.B Responsibility and Accountability	3
I.C Resources	5
II INFORMATION SECURITY PROGRAM MANAGEMENT	6
II.A Risk Identification.....	7
II.A.1 Threats	8
II.A.2 Vulnerabilities	8
II.A.3 Supervision of Cybersecurity Risk and Resources for Cybersecurity Preparedness	9
II.B Risk Measurement.....	10
II.C Risk Mitigation	11
II.C.1 Policies, Standards, and Procedures.....	11
II.C.2 Technology Design.....	12
II.C.3 Control Types	12
II.C.4 Control Implementation	13
II.C.5 Inventory and Classification of Assets	14
II.C.6 Mitigating Interconnectivity Risk	14
II.C.7 User Security Controls.....	15
II.C.8 Physical Security	18
II.C.9 Network Controls	19
II.C.10 Change Management Within the IT Environment.....	21
II.C.11 End-of-Life Management	25
II.C.12 Malware Mitigation.....	25
II.C.13 Control of Information	26
II.C.14 Supply Chain	29
II.C.15 Logical Security	30
II.C.16 Customer Remote Access to Financial Services	35
II.C.17 Application Security	38
II.C.18 Database Security	40
II.C.19 Encryption	40
II.C.20 Oversight of Third-Party Service Providers	42

II.C.21	Business Continuity Considerations	43
II.C.22	Log Management.....	44
II.D	Risk Monitoring and Reporting	45
II.D.1	Metrics.....	45
III	SECURITY OPERATIONS.....	46
III.A	Threat Identification and Assessment.....	47
III.B	Threat Monitoring	48
III.C	Incident Identification and Assessment	49
III.D	Incident Response.....	50
IV	INFORMATION SECURITY PROGRAM EFFECTIVENESS	52
IV.A	Assurance and Testing	53
IV.A.1	Key Testing Factors.....	53
IV.A.2	Types of Tests and Evaluations	54
IV.A.3	Independence of Tests and Audits	56
IV.A.4	Assurance Reporting.....	56
APPENDIX A: EXAMINATION PROCEDURES		57
APPENDIX B: GLOSSARY		75
APPENDIX C: LAWS, REGULATIONS, AND GUIDANCE		89

Introduction

This “Information Security” booklet is an integral part of the *Federal Financial Institutions Examination Council (FFIEC)¹ Information Technology Examination Handbook (IT Handbook)* and should be read in conjunction with the other booklets in the *IT Handbook*. This booklet provides guidance to examiners and addresses factors necessary to assess the level of security risks to a financial institution’s² information systems.³ It also helps examiners evaluate the adequacy of the information security program’s integration into overall risk management.⁴

Information security is the process by which a financial institution protects the creation, collection, storage, use, transmission, and disposal of sensitive information, including the protection of hardware and infrastructure used to store and transmit such information. Information security promotes the commonly accepted objectives of confidentiality, integrity, and availability of information and is essential to the overall safety and soundness of an institution. Information security exists to provide protection from malicious and non-malicious actions that increase the risk of adverse effects on earnings, capital, or enterprise value. The potential adverse effects can arise from the following:

- Disclosure of information to unauthorized individuals.
- Unavailability or degradation of services.
- Misappropriation or theft of information or services.
- Modification or destruction of systems or information.
- Records that are not timely, accurate, complete, or consistent.

¹ The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-630. The FFIEC is composed of the principals of the following: the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), the State Liaison Committee (SLC), and the Consumer Financial Protection Bureau (CFPB).

² The term “financial institution” includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions. The term is used interchangeably with “institution” in this booklet.

³ Examiners should also use this booklet to evaluate the performance by third-party service providers, including technology service providers, of services on behalf of financial institutions.

⁴ This booklet addresses regulatory expectations regarding the security of all information systems and information maintained by or on behalf of a financial institution, including a financial institution’s own information and that of all of its customers. An institution’s overall information security program must also address the specific information security requirements applicable to “customer information” set forth in the “Interagency Guidelines Establishing Information Security Standards” implementing section 501(b) of the Gramm–Leach–Bliley Act and section 216 of the Fair and Accurate Credit Transactions Act of 2003. See 12 CFR 30, appendix B (OCC); 12 CFR 208, appendix D-2 and 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA) (collectively referenced in this booklet as the “Information Security Standards”).

Institutions should maintain effective information security programs commensurate with their operational complexities.⁵ Information security programs should have strong board and senior management support, promote integration of security activities and controls throughout the institution's business processes, and establish clear accountability for carrying out security responsibilities. In addition, because of the frequency and severity of cyber attacks, the institution should place an increasing focus on cybersecurity controls, a key component of information security.

Institutions should also assess and refine their controls on an ongoing basis. The condition of a financial institution's controls, however, is just one indicator of its overall security posture. Other indicators include the ability of the institution's board and management to continually review the institution's security posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions. Information security is far more effective when management does the following:

- Integrates processes, people, and technology to maintain a risk profile that is in accordance with the board's risk appetite.⁶
- Aligns the information security program with the enterprise risk management program and identifies, measures, mitigates, and monitors risk.

Because risk mitigation frequently depends on institution-specific factors, this booklet describes processes and controls that an institution can use to protect information and supporting systems from various threats. Management should be able to identify and characterize the threats, assess the risks, make decisions regarding the implementation of appropriate controls, and provide appropriate monitoring and reporting.

Financial institutions may outsource some or all of their IT-related functions. Although the use of outsourcing may change the location of certain activities from financial institutions to third-party service providers, outsourcing does not change the regulatory expectations for an effective information security program. Examiners should use this booklet when evaluating a financial institution's risk management process, including the duties, obligations, and responsibilities of the third-party service provider regarding information security and the oversight exercised by the financial institution.

⁵ See also Information Security Standards, section II.A, requiring each financial institution to have a comprehensive written information security program, appropriate to its size and complexity, designed to (1) ensure the security and confidentiality of "customer information"; (2) protect against any anticipated threats or hazards to the security or integrity of such information; (3) protect against unauthorized access to or use of such information that could result in a substantial harm or inconvenience to any customer; and (4) ensure the proper disposal of both "customer information" and any "consumer information."

⁶ Risk appetite can be defined as the amount of risk a financial institution is prepared to accept when trying to achieve its objectives.

I Governance of the Information Security Program

Action Summary

Management should promote effective IT governance by doing the following:

- Establishing an information security culture that promotes an effective information security program and the role of all employees in protecting the institution's information and systems.
- Clearly defining and communicating information security responsibilities and accountability throughout the institution.
- Providing adequate resources to effectively support the information security program.

While IT governance is generally addressed in the *IT Handbook's* "Management" booklet, this booklet addresses specific governance topics related to information security, including the following:

- Implementation and promotion of security culture.
- Assignment of responsibilities and accountability.
- Effective funding and use of resources.

I.A Security Culture

An institution's security culture contributes to the effectiveness of the information security program. The information security program is more effective when security processes are deeply embedded in the institution's culture.

The board and management should understand and support information security and provide appropriate resources for developing, implementing, and maintaining the information security program. The result of this understanding and support is a program in which management and employees are committed to integrating the program into the institution's lines of business, support functions, and third-party management program.

The introduction of new business initiatives (such as new service offerings or applications) can reveal the maturity of and degree to which information security is part of the institution's culture. An institution with a stronger security culture generally integrates information security into new initiatives from the outset and throughout the life cycles of services and applications. Another indicator of an effective culture is whether management and employees are held accountable for complying with the institution's information security program.

I.B Responsibility and Accountability

The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions. The board should reasonably

understand the business case for information security and the business implications of information security risks; provide management with direction; approve information security plans, policies, and programs; review assessments of the information security program's effectiveness; and, when appropriate, discuss management's recommendations for corrective action. The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program.

The board, or designated board committee, should approve the institution's written information security program; affirm responsibilities for the development, implementation, and maintenance of the program; and review a report on the overall status of the program at least annually.⁷

Management should provide a report to the board at least annually⁸ that describes the overall status of the program and material matters related to the program, including the following:

- Risk assessment process, including threat identification and assessment.
- Risk management and control decisions, including risk acceptance and avoidance.
- Third-party service provider arrangements.
- Results of testing.
- Security breaches or violations of law or regulation and management's responses to such incidents.
- Recommendations for updates to the information security program.

When providing reports on information security, management should include the results of management assessments and reviews; internal and external audit activity related to information security; third-party reviews of the information security program and information security measures; and other internal or external reviews designed to assess the adequacy of the information security program, processes, policies, and controls.

Management also should do the following:

- Implement the board-approved information security program.
- Establish appropriate policies, standards, and procedures to support the information security program.
- Participate in assessing the effect of security threats or incidents on the institution and its lines of business and processes.
- Delineate clear lines of responsibility and communicate accountability for information security.

⁷ See also Information Security Standards, section III.A, requiring the board of directors or an appropriate committee of the board of each financial institution to approve the institution's written information security program, and oversee the development, implementation, and maintenance of the program, including assigning specific responsibility for its implementation and reviewing management reports.

⁸ See also Information Security Standards, section III.F, requiring each financial institution to report to its board or an appropriate committee of the board at least annually. The report should include a description of the institution's compliance with the Information Security Standards and discuss material matters related to its information security program.

- Adhere to board-approved risk thresholds relating to information security threats or incidents, including those relating to cybersecurity.
- Oversee risk mitigation activities that support the information security program.
- Implement a risk acceptance process that identifies the risk and when, how, to what extent, and who in management has accepted the risk associated with identified vulnerabilities.
- Establish segregation of duties.
- Coordinate information and physical security.
- Integrate security controls throughout the institution.
- Require that data with similar criticality and sensitivity be protected consistently throughout the institution.
- Establish and monitor the information security responsibilities of third parties, as further described in the “Oversight of Third-Party Service Providers” section of this booklet.
- Maintain job descriptions or employment contracts that include specific information security responsibilities.
- Provide information security and awareness training and ongoing security-related communications to employees, and ensure employees complete such training annually.

Management should designate at least one information security officer responsible and accountable for implementing and monitoring the information security program. Information security management responsibilities may be distributed across various lines of business depending on where the risk decisions are made and the institution’s size, complexity, culture, nature of operations, or other factors.

Information security officers should report directly to the board or senior management and have sufficient authority, stature within the organization, knowledge, background, training, and independence to perform their assigned tasks. To ensure appropriate segregation of duties, the information security officers should be independent of the IT operations staff and should not report to IT operations management. Information security officers should be responsible for responding to security events by ordering emergency actions to protect the institution and its customers from imminent loss of information; managing the negative effects on the confidentiality, integrity, availability, or value of information; and minimizing the disruption or degradation of critical services.

Internal auditors should implement a risk-based audit program to ensure management maintains and the board oversees an effective information security program. Additionally, management should issue appropriate reports to the board. Refer to the *IT Handbook*’s “Audit” booklet.

I.C Resources

Funding, along with technical and managerial talent, also contributes to the effectiveness of the information security program. Management should provide, and the board should oversee, adequate funding to develop, implement, and maintain a successful information security program. The program should be staffed by sufficient personnel who have skills that are aligned with the institution’s technical and managerial needs and commensurate with its size, complexity, and risk profile. Knowledge of technology standards, practices, and risk methodologies is particularly important to the success of the information security program.

When third-party service providers supplement an institution's technical and managerial capabilities, management oversight should be commensurate with the sensitivity and criticality of the information and business processes supported by the third-party service provider. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

II Information Security Program Management

Action Summary

Management should develop and implement an information security program that does the following:

- Supports the institution's IT risk management (ITRM) process by identifying threats, measuring risk, defining information security requirements, and implementing controls.
- Integrates with lines of business and support functions in which risk decisions are made.
- Integrates third-party service provider activities with the information security program.

The institution should have a robust and effective information security program that supports the institution's ITRM process.⁹ An effective information security program includes the following:

- Risk identification
- Risk measurement
- Risk mitigation
- Risk monitoring and reporting

Refer to the *IT Handbook's* "Management" booklet for more information. A comprehensive information security program should incorporate cybersecurity elements, and management should identify, measure, mitigate, monitor, and report cybersecurity-related risks in accordance with the information security program and the ITRM process. In addition, to determine the overall effectiveness of the information security program, management should have comprehensive assurance and testing processes.

Management should integrate the information security program with the institution's lines of business and support functions. An integrated program provides management the ability to assess the likelihood and potential damage to the institution from an incident, identify the root cause(s) of the incident, and implement controls to address identified issues.

Institutions that outsource technology, line of business activities, and support functions should ensure integration of these activities with the information security program through an effective

⁹ See also Information Security Standards, section III.B, requiring each financial institution to assess risk including through the identification of reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of "customer information" or "customer information systems," and section III.C, requiring each financial institution to manage and control its risks by (1) designing an information security program to control risks it identifies commensurate with the sensitivity of the information and the complexity and scope of the institution's activities, and (2) adopting an enumerated list of controls, as appropriate.

third-party service provider management program.¹⁰ Effective integration of these programs is evident when the institution creates and enforces expectations that align with the internal information security program in such a way that the combined activities of the institution and its third-party service providers result in an acceptable level of risk. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

II.A Risk Identification

Action Summary

Management should develop and implement a process to identify risk.

Risk is the potential that events, expected or unanticipated, may adversely affect the institution's earnings or capital. Risk is considered in terms of categories, one of which is operational risk. Operational risk is the risk of failure or loss resulting from inadequate or failed processes, people, or systems. Internal and external events can affect operational risk. Internal events include human errors, misconduct, and insider attacks. External events affecting IT and the institution's ability to meet its operating objectives include natural disasters, cyber attacks, changes in market conditions, new competitors, new technologies, litigation, and new laws or regulations. These events pose risks and opportunities, and the institution should factor them into the risk identification process.

To be effective, an information security program should have documented processes to identify threats and vulnerabilities continuously. Risk identification should produce groupings of threats, including significant cybersecurity threats. A taxonomy¹¹ for categorizing threats, sources, and vulnerabilities can help support the risk identification process. Management should perform these risk identification activities to determine the institution's information security risk profile, including cybersecurity risk.

¹⁰ See also Information Security Standards, section III.D, requiring each financial institution to oversee service provider arrangements by (1) exercising appropriate due diligence in selecting its service providers; (2) requiring its service providers by contract to implement appropriate measures designed to ensure the security and confidentiality of the institution's "customer information"; and (3) where indicated by the institution's risk assessment, monitoring its service providers to confirm that the service providers have satisfied their contractual obligations, including by reviewing audits, summaries of test results, or other equivalent evaluations of its service providers.

¹¹ A taxonomy is a method for classifying items into ordered categories. Institutions use taxonomies to find relevant information from a large collection of data and to better detect or understand the patterns and trends.

II.A.1 Threats

According to the National Institute of Standards and Technology (NIST), a threat is any circumstance or event with the potential to create loss.¹² A threat can be a natural occurrence, technology or physical failure, a person with intent to harm, or a person who unintentionally causes harm. Information about threats is available from public and private sources. Public sources include the news media, blogs, government publications and announcements, and various websites. Private sources include information security vendors and information-sharing organizations.

The threat identification process is a means to collect data on potential threats that can assist management in its identification of information security risks. Threat modeling is a structured approach that enables an institution to aggregate and quantify potential threats. Institutions should consider using threat modeling to better understand the nature, frequency, and sophistication of threats; evaluate the information security risks to the institution; and apply this knowledge to the institution's information security program. As threats evolve rapidly, however, it is understood that modeling may not account for attacks that have not previously been seen, such as zero-day attacks, but could have significant impacts.

II.A.2 Vulnerabilities

A vulnerability is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source.¹³ A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation. These flaws provide opportunities for hackers to gain access to a computer system, execute commands as another user, or access data contrary to specified access restrictions. Institutions can use automated vulnerability scanners to scan their computer systems for known security exposures, as well as services available from third parties, such as the Mitre Corporation's Common Vulnerability and Exposures (CVE),¹⁴ to track vulnerabilities.

In addition to technology-based vulnerabilities, weaknesses in business operational processes can create security vulnerabilities, exposing financial institutions to unwarranted risk. These vulnerabilities can include weaknesses in security procedures, administrative controls, physical layout, or internal controls that could be exploited to gain unauthorized access to information or to disrupt critical services. For example, an institution's systems architecture may be designed based on management's assumption that manual validation of wire transfers takes place before execution, when in practice the business process does not perform that validation until after transfers have taken place.

¹² NIST SP (Special Publication) 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments," September 2012.

¹³ Ibid.

¹⁴ CVE is a dictionary of publicly known information security vulnerabilities and exposures. The Mitre Corporation maintains the system. CVE is sponsored by the U.S. Computer Emergency Readiness Team in the Office of Cybersecurity and Communications at the U.S. Department of Homeland Security.

In addition to the vulnerabilities within a financial institution's system, vulnerabilities may also arise from interdependent and interconnected systems. Financial institutions connect their systems through mergers and acquisitions and through relationships with third parties. Over time, as these systems become increasingly interdependent and complex, new vulnerabilities may be introduced. Moreover, financial institutions are dependent on a vast array of hardware and services that may result in vulnerabilities from their supply chains, including those found in hardware and software products.

Management should assess whether the institution has processes and procedures in place to identify and maintain a catalogue of relevant vulnerabilities, determine which pose a significant risk to the institution, and effectively mitigate and monitor the risks posed by those vulnerabilities. When management cannot or chooses not to mitigate a vulnerability, management should document the decision to accept the risk, the level of risk associated with the vulnerability, and the person accountable for accepting the risk. Refer to the "Security Operations" section of this booklet for more information.

II.A.3 Supervision of Cybersecurity Risk and Resources for Cybersecurity Preparedness

II.A.3(a) *Supervision of Cybersecurity Risk*

Cybersecurity is the process of protecting consumer and bank information by preventing, detecting, and responding to attacks. As part of cybersecurity, institutions should consider management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks. In light of the increasing volume and sophistication of cybersecurity threats, examiners should focus on cybersecurity preparedness in assessing the effectiveness of an institution's overall information security program.

II.A.3(b) *Resources for Cybersecurity Preparedness*

The FFIEC members issued a voluntary Cybersecurity Assessment Tool¹⁵ to help institution boards and management identify risks to their institutions and evaluate their institution's cybersecurity preparedness. In addition, there are other resources available to help management develop and evaluate information security and cyber resilience, such as the NIST Cybersecurity Framework, common approaches developed by the Mitre Corporation, and the U.S. Computer Emergency Readiness Team's (US-CERT)¹⁶ National Cyber Awareness System. Institution management can select a single framework or use a combination of resources to help identify its risks and determine its cybersecurity preparedness. Regardless of the source, frameworks can help management identify a cybersecurity and resilience posture that is commensurate with the institution's risk and complexity.

¹⁵ Refer to the [Cybersecurity Assessment Tool](#) on the FFIEC website.

¹⁶ US-CERT, of the Department of Homeland Security, responds to major incidents, analyzes threats, and exchanges critical cybersecurity information with trusted partners around the world.

II.B Risk Measurement

Action Summary

Management should develop risk measurement processes that evaluate the inherent risk to the institution.

The risk measurement process should be used to understand the institution's inherent risk and determine the risk associated with different threats. Management should use its measurement of the risks to guide its recommendations for and use of mitigating controls.

Threat analysis tools assist in understanding and supporting the measurement of information security-related risks. Such tools can include event trees,¹⁷ attack trees,¹⁸ kill chains,¹⁹ and other security-related schemata.²⁰ These tools help management deconstruct an event into stages, better understand the event, identify the most effective and efficient means of mitigating risk, and improve the information security program. Additionally, management could use a taxonomy for security-related events to help accomplish the following:

- Map threats and vulnerabilities.
- Incorporate legal and regulatory requirements.
- Improve consistency in risk measurement.
- Highlight potential areas for mitigation.
- Select proper controls to cover various attack stages, channels, and assets.
- Allow comparisons among different threats, events, and potential mitigating controls.

Refer to the *IT Handbook's* "Management" booklet for more information.

¹⁷ An event tree is a diagram of a chronological series of events in a system or activity that displays sequence progression, end states, and dependencies across time.

¹⁸ An attack tree is a diagram showing how an asset, or target, might be attacked through various attack scenarios. Using an attack tree helps describe threats on computer systems and possible attacks to realize those threats.

¹⁹ A kill chain originally was used as a military concept related to the structure of an attack. In information security, a kill chain is a method for modeling intrusions on a computer network.

²⁰ Security-related schemata are lists of software vulnerabilities and include the Mitre Corporation's Common Attack Pattern Enumeration and Classification, CVE, Common Weakness Enumeration, "ATT&CK Matrix," and Malware Attribute Enumeration and Characterization, and Mandiant's Open Indicators of Compromise.

II.C Risk Mitigation

Action Summary

Management should develop and implement appropriate controls to mitigate identified risks.

Once management has identified and measured the risks, it should develop and implement an appropriate plan to mitigate those risks. This plan should include an understanding of the extent and quality of the current control environment. When conducting an evaluation of the strength of controls, or the ability to mitigate risk, the institution should consider the system of controls rather than any discrete control.

Management should also obtain, analyze, and respond to information from various sources (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC]) on cyber threats and vulnerabilities that may affect the institution. Management should incorporate available information on cyber events into the institution's information security program. Additionally, management should develop, maintain, and update a repository of cybersecurity threat and vulnerability information that may be used in conducting risk assessments and provide updates to senior management and the board on cyber risk trends.

II.C.1 Policies, Standards, and Procedures

Information security policies, standards, and procedures should define the institution's control environment through a governance structure and provide descriptions of required, expected, and prohibited activities. Policies, standards, and procedures guide decisions and activities of users, developers, administrators, and managers and inform those individuals of their information security responsibilities. Policies, standards, and procedures should also specify the mechanisms through which responsibilities can be met. In addition, they should provide guidance on acquiring, designing, implementing, configuring, operating, maintaining, and auditing information systems. Policies, standards, and procedures that address the information security program should describe the roles of the information security department, lines of business, and IT organization in administering the information security program. Information security policies, standards, and procedures form the means by which the objectives of the information security program are achieved. Key attributes that contribute to the success of information security policies, standards, and procedures include the following:

- Scope that describes the expectations for appropriate actions by affected parties.
- Sufficient details to guide behavior.
- Implementation through ordinary means, such as system administration procedures and acceptable use policies.
- Enforcement through security tools and restrictions.
- Delineation of the areas of responsibility for users, developers, administrators, and managers.
- Clear and easily understandable communications to all affected parties.
- Certification that employees have read and understand the policies.

- Flexibility to address changes in the environment.
- Annual board review and approval.

II.C.2 Technology Design

While technology can introduce risk, it can also serve as a mitigation tool. Management should understand the benefits and limitations of the technology that the institution uses and whether other types of controls are necessary to compensate for those limitations.

Information security issues arise when (a) the design of the technology and the policies governing its use do not effectively defend against identified and unidentified threats, (b) threats change in ways not envisioned by the designers, and (c) the controls are not operating as intended. Management should continually assess the capability of the institution's processes, people, and technologies to sustain the appropriate level of information security based on the institution's risk profile, size, complexity, and risk appetite.

II.C.3 Control Types

Management may mitigate information security risks by implementing controls. Controls may be categorized according to timing and nature.

Table 1: Examples of Timing- and Nature-Related Controls

Timing		
Control type	Description	Example
Preventive	Controls designed to prevent incidents from occurring	Access controls to applications and systems that prevent unauthorized individuals from performing transactions
Detective	Controls designed to alert management when incidents occur	Reports that show suspicious activity
Corrective	Controls that lessen impact to the institution when adverse incidents occur	Business continuity plans
Nature		
Control type	Description	Example
Administrative	Controls that align with the board-approved risk appetite and inform employees of management's expectations	Policies or procedures that guide implementation of the information security program
Technical	Software or hardware (or both) that prevents unauthorized activity	A firewall that prevents unauthorized logical access to or from a network
Physical	Devices to prevent unauthorized physical access to a facility or computer system	A deadbolt lock on a door

It is important to have a layered control system, which deploys different controls at different points of a business process and throughout an IT system so that the strength of one control can

compensate for weaknesses in or possible failure of another control. Therefore, layered controls function in an integrated fashion to more effectively mitigate risk.

Economic and technical considerations generally affect prevention and detection or response choices in system design. Compensating controls are controls that adjust for weaknesses within the system or process. An example of compensating controls would be a review of activity logs for applications that do not allow proper segregation of duties.

II.C.4 Control Implementation

Management should implement controls that align security with the nature of the institution's operations and strategic direction. Based on the institution's risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging and monitoring, and secure software development (including third-party software development). In implementing controls, management should ensure it has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls.

The level at which controls are implemented should depend on the institution's size, complexity, and risk profile, but all institutions should implement appropriate controls. In light of increasing cybersecurity risks, management should implement risk-based controls for managing cybersecurity threats and vulnerabilities, such as interconnectivity risk. Management should review and update the security controls as necessary depending on changes to the internal and external operating environment, technologies, business processes, and other factors.

The institution can reference one or more recognized technology frameworks and industry standards. Several organizations have published control listings in addition to implementation guidance, including the following:

- **NIST 800 series of publications.** These publications provide descriptions of some management processes and technical guidance on many individual controls.
- **Control Objectives for Information and Related Technology (COBIT).** COBIT provides a broad and deep framework for governance and management of enterprise IT.
- **IT Infrastructure Library (ITIL).** ITIL provides a list of recognized practices for IT service management.
- **International Organization for Standardization (ISO)²¹ 27000 series.** The ISO 27000 series provides control standards specific to information security.
- **Industry publications and sources.²²** Management and staff may find these useful for discrete controls and processes.

²¹ ISO is an independent, non-governmental, international organization that brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards.

²² Some industry publications or organizations that provide security-related information include the ISACA Journal, SANS Institute, the Financial Services Roundtable, the Council on Cybersecurity, and the Open Web Application Security Project.

- **Vendor-provided publications, bulletin boards, and user groups.** Vendors often publish recommendations for securing their products. Additionally, some offer bulletin boards and user groups for clients to interact among themselves.

II.C.5 Inventory and Classification of Assets

Action Summary

Management should inventory and classify assets, including hardware, software, information, and connections.

Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections. Management should have policies to govern the inventory and classification of assets both at inception and throughout their life cycle, and wherever the assets are stored, transmitted, or processed. Inventories enable management and staff to identify assets and their functions. Classification enables the institution to determine the sensitivity and criticality of assets. Management should use this classification to implement controls required to safeguard the institution's physical and information assets. Additionally, management can use the inventory to discover specific vulnerabilities, such as unauthorized software.

Inventories are important for management to identify assets that require additional protection, such as those that store, transmit, or process sensitive customer information, trade secrets, or other information or assets that could be a target of cyber criminals. Knowing what information assets the institution has and where they are stored, transmitted, or processed helps management comply with federal and state laws and regulations regarding privacy and security of sensitive customer information.

After inventorying the assets, management should classify the information according to the appropriate level of protection needed. For example, systems containing sensitive customer information may require access controls based on job responsibilities. These systems should have stronger controls than systems containing information meant for the general public. Some institutions classify information as public, non-public, or institution-confidential, while others use the classifications high, moderate, and low. Additional classifications, such as critical and noncritical, may be helpful to certain types of institutions.

II.C.6 Mitigating Interconnectivity Risk

Business processes often require institutions to share information with other institutions and third-party service providers that require connectivity. The extent of interconnectivity is a function of network architecture, network complexity, traffic volume, and number of connections. Interconnectivity risk arises from misuse, mismanagement, or compromise of these connections.

To mitigate interconnectivity risk, management should do the following:

- Identify connections with third parties, including other financial institutions, financial institution intermediaries, and third-party service providers.
- Identify all access points and connection types that pose risk, such as local area network (LAN) connections to other networks or Internet service providers (ISP), Wi-Fi, and cellular connections.
- Identify connections between and access across low-risk and high-risk systems.
- Assess all connections with third parties that provide remote access capability or control over internal systems.
- Implement and assess the adequacy of controls to ensure the security of connections regardless of criticality or sensitivity.

Management should maintain network and connectivity diagrams and data flow charts to ensure adequacy of layered controls and to facilitate more timely recovery and restoration of systems when incidents occur.

II.C.7 User Security Controls

Action Summary

Management should mitigate the risks posed by users by doing the following:

- Establishing and administering security screening in IT hiring practices.
- Establishing and administering a user access program for physical and logical access.
- Employing segregation of duties.
- Obtaining agreements covering confidentiality, nondisclosure, and authorized use.
- Providing training to support awareness and policy compliance.

Users should be granted access to systems, applications, and databases based on their job responsibilities. Access rights should be granted in accordance with the institution's physical and logical access control policies. Authorized users with elevated or administrator privileges can pose a potential threat to systems and data. Employees, contractors, or third-party service providers can exploit their legitimate computer access for unauthorized purposes. Additionally, the degree of internal access granted to some users increases the risk of damage or loss of information and systems. Risk exposures from internal users include the following:

- Alteration of data.
- Deletion of production and backup data.
- Misdirected data.
- Disruption of systems.
- Destruction of systems.
- Misuse of systems for personal gain or to damage the institution.
- Appropriation of strategic or customer data for espionage or fraud schemes.
- Extortion for stolen data.
- Misuse of data following the termination or change in job responsibility of an employee.

Management should understand the risks to the institution's information-processing environment and establish appropriate user access controls to mitigate these and other potential risks to the institution's assets. Users should understand and confirm their understanding of their roles and responsibilities in maintaining a sound security environment, which includes both physical and logical areas.

II.C.7(a) *Security Screening in Hiring Practices*

Management should have a process to verify job application information for all new employees. The sensitivity of a particular job or access level may warrant additional screening and recurring background and credit checks. Management should verify that contractors are subject to similar screening procedures. In addition to initial screening, management should remain alert to changes in personal circumstances of employees and contractors that could increase incentives for system misuse or fraud.

II.C.7(b) *User Access Program*

Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements:

- Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity.
- Alignment of employee job descriptions to the user access program.
- Requirements for business and application owners to define user profiles.
- Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel.
- Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations.
- Periodic independent reviews that ensure effective administration of user access, both physical and logical.

For more information, refer to the "Physical Security" and "Logical Security" sections of this booklet.

II.C.7(c) *Segregation of Duties*

Segregation of duties, or job designs that require more than one person to complete critical or sensitive tasks, can help mitigate risk. Employees and third parties with access to sensitive resources could cause substantial damage and potential loss. System administrators, for instance, have the most powerful role in the user access process and have unlimited access to an institution's information assets and technology. Given this extensive access, management should evaluate the process for determining which individuals should be granted system administrator privileges. Such access should be appropriately monitored for unauthorized or inappropriate activity. Management should incorporate independent reviews or approvals for individuals who

perform multiple functions to minimize the potential for fraud, irregularities, and errors. Examples of segregation of duties include the following:

- Independent monitoring of the activities performed by the users with increased privileges (e.g., system administrators and super users²³).
- Distribution of system administration activities so no administrator can hide his or her activities or control an entire system.
- Additional levels of approval as the criticality and sensitivity of decisions increase.

If an activity is conducted without appropriate segregation of duties, management should require an independent review (e.g., audit) of that activity.

II.C.7(d) Confidentiality Agreements

The institution should protect the confidentiality of customer and institution information. A breach in confidentiality could disclose proprietary information, increase fraud risk, violate customer privacy and associated rights, and violate laws or regulations. Confidentiality agreements can be used to put all parties on notice that the financial institution owns its information, expects strict confidentiality, and prohibits information sharing outside of that required for legitimate business needs. Management should obtain signed confidentiality agreements before granting employees and contractors access to IT systems.

II.C.7(e) Training

Training ensures personnel have the necessary knowledge and skills to perform their job functions.²⁴ Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Management should educate users about their security roles and responsibilities and communicate them through acceptable use policies. Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected. Management should have the ability to impose sanctions for noncompliance.

Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. The institution should collect signed acknowledgments of the employee acceptable use policy as part of the annual training program.

²³ In computing, the super user is a special user account used for system administration. Depending on the operating system, the name of this account might be root, administrator, admin, or supervisor.

²⁴ See also Information Security Standards, section III.C.2, requiring each financial institution to train staff to implement its information security program.

II.C.8 Physical Security

Action Summary

Management should implement appropriate preventive, detective, and corrective controls for physical security.

Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Management should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones.

A data center houses an institution's most important information system components. When selecting a site for a data center, one major objective should be to limit the risk of exposure from internal and external threats, including, where possible, environmental threats inherent to physical locations (e.g., hurricanes, earthquakes, and blizzards). The selection process should include reviewing the surrounding area to determine whether it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Guards, fences, barriers, surveillance equipment, or other devices can deter intruders. Because access to key information systems' hardware and software should be limited, appropriate physical controls should be in place. Additionally, the location should not be identified or advertised by signage or other indicators.

Detection devices, when applicable, should be used to prevent theft and safeguard the equipment. The devices should provide continuous coverage. Detection devices have two purposes—to send alarms when responses are necessary and to support subsequent forensics. Alarms are useful only when response will occur. Some detection devices include the following:

- Switches that activate alarms when electrical circuits are broken.
- Light and laser beams, ultraviolet beams, sound, or vibration detectors that are invisible to intruders, and ultrasonic or radar devices that detect movement.
- Closed-circuit television (CCTV) that provides visual observation and records intrusions.

A combination of fire suppression, smoke alarms, raised flooring, and heat and moisture sensors should address risks from environmental threats (e.g., fire, flood, and excessive heat). Environmental threat monitoring should be continuous, and responses should occur when alarms activate.

Physical security devices frequently need preventive maintenance to function properly. The institution should be able to provide maintenance logs to demonstrate that physical security devices are regularly maintained. Periodic testing provides assurance that the devices are operating correctly.

The institution should have policies governing the duties and responsibilities of security guards. Employees who access secured areas should have proper identification and authorization to enter the areas. All non-employees should provide identification to a security guard before obtaining

access. Security guards should be trained to restrict the removal of technology assets from the premises and to record the identity of anyone attempting to remove those assets. Management should implement a specific and formal authorization process for the removal of hardware and software from the premises.

Access should be restricted to the following equipment or areas:

- Operations centers (e.g., data center operations, security operations center, and network operations center) or server rooms; uninterruptible power supplies and backup generators.
- Funds transfer and automated clearinghouse routers.
- Telecommunications equipment.
- Media libraries.
- Equipment removed from the network and awaiting disposal.
- Spare or backup devices.

II.C.9 Network Controls

Action Summary

Management should secure access to computer networks through multiple layers of access controls by doing the following:

- Establishing zones (e.g., trusted and untrusted) according to the risk profile and criticality of assets contained within the zones and appropriate access requirements within and between each security zone.
- Maintaining accurate network diagrams and data flow charts.
- Implementing appropriate controls over wired and wireless networks.

Networks should be protected by a secure boundary, identifying “trusted” and “untrusted” zones. Internal zones, typically trusted, should segregate various components into distinct areas, each with the level of controls appropriate to the content and function of the assets within the zone. The institution’s trusted network should be protected through appropriate configuration and patch management, privileged access controls, segregation of duties, implementation of effective security policies, and use of perimeter devices and systems to prevent and detect unauthorized access. Tools used to enforce and detect perimeter protection include routers, firewalls, intrusion detection systems (IDS) and intrusion prevention systems, proxies, gateways, jump boxes,²⁵ demilitarized zones, virtual private networks (VPN), virtual LANs (VLAN), log monitoring and network traffic inspecting systems, data loss prevention (DLP) systems, and access control lists.

The trusted network should be further segregated into internal layers, including production, staging, and development environments. Within those environments, management should

²⁵ A jump box, or jump server, provides administrators with access to or control of other servers or devices in the network. Because of this capability, additional security measures should be implemented.

consider segregating sensitive traffic, by using Voice Over Internet Protocol²⁶ (VOIP) and network management (such as virtualization infrastructure that carries server boot images between storage devices and hosts). Each zone should have a security policy appropriate to its use, ensuring that zone restrictions are defined by risk, sensitivity of data, user roles, and appropriate access to application systems. Access to zones should be controlled according to the principle of least privilege and segregation of duties. To ensure appropriate network security, management should maintain accurate network and data flow diagrams, and store them securely, providing access only to essential personnel. These diagrams should identify hardware, software, and network components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture.

II.C.9(a) *Wireless Network Considerations*

A wireless LAN (WLAN) is a medium of network connectivity, supported by radio wave transmissions that provides more convenient network access to employees or devices that need flexibility to connect to multiple locations within the institution's facilities. Because the user is not physically connected to the network and the wireless signal is broadcast and available to others, wireless networks are inherently less secure than wired networks and require additional scrutiny, controls, and oversight. Wireless access points are the devices that broadcast the radio wave signals and should be physically secure to prevent compromise and securely configured to provide the same level of control as a wired connection. Wireless gateways can allow management to implement more complex access controls, including advanced identity management capabilities and services to detect and remediate malicious software.

Policies should prohibit installation of wireless access points and gateways without approval and formal inclusion in the hardware inventory. Network monitoring systems should be configured to detect the addition of new devices. Alternatively, network access control (NAC) systems could prevent the recognition of any unauthorized device.²⁷ Management should consider limiting the WLAN signal to authorized areas, within the boundaries of the institution, if feasible. Management should use an industry-accepted level of encryption with strength commensurate with the institution's risk profile on the institution's wireless networks.

Malicious insiders and attackers may also set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities. The institution should scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices.

²⁶ VOIP is the transmission of voice telephone conversations using the Internet or IP networks.

²⁷ A NAC system typically provides an IP address only after validating that the newly connected device is authorized, by means of some identification (such as a computer's physical address—MAC address—or certificate) or pre-installed client software.

The institution may provide guests with access to a wired or wireless network. The guest network generally is used to provide access to the Internet and should be configured to prevent access to any portion of the production network.

Institutions often provide remote network connectivity for employees or third-party service providers²⁸ who are not located within or around the institution's facilities. This connectivity presents operational advantages, but steps should be taken to ensure that the connection is encrypted and secured. VPN connections should be used for both broadband networks and wireless air card connections to isolate and encrypt remote traffic to institution networks. IP geolocation information may not always be available when using broadband networks, which can limit the effectiveness of monitoring. Therefore, management should consider implementing compensating controls, such as restricting access to network resources.

II.C.10 Change Management Within the IT Environment

Action Summary

Management should have a process to introduce changes to the environment in a controlled manner. Changes to the IT environment include the following:

- Configuration management of IT systems and applications.
- Hardening of systems and applications.
- Use of standard builds.
- Patch management.

The IT environment consists of operating systems,²⁹ middleware,³⁰ applications, file systems, and communications protocols. The institution should have an effective process to introduce application and system changes, including hardware, software, and network devices, into the IT environment. The process for introducing software should encompass securely developing, implementing, and testing changes to both internally developed and acquired software.

Application and system control considerations for introducing changes to the IT environment before implementation should include the following:

- Developing procedures to guide the process of introducing changes to the environment.
- Clearly defining requirements for changes.
- Restricting changes to authorized users.

²⁸ In some cases, the institution provides remote access via VPN to a third-party service provider. Controls over third-party access should be commensurate with the sensitivity and criticality of the system and information accessed.

²⁹ An operating system is fundamental software that supports and manages software applications, allocates system resources, provides access and security controls, maintains file systems, and manages communications between end users and hardware devices.

³⁰ Middleware is software that connects two or more software components or applications.

- Reviewing the impact that changes have on security controls.
- Identifying all system components affected by the changes.
- Developing test scripts and implementation plans.
- Performing necessary tests of all changes to the environment (e.g., systems testing, integration testing, functional testing, user acceptance testing, and security testing).
- Defining rollback procedures in the event of unintended or negative consequences with the introduced changes.
- Ensuring the application or system owner has authorized changes in advance.
- Maintaining strict version control of all software updates.
- Validating that new hardware complies with institution policies.
- Ensuring network devices are properly configured and function appropriately within the environment.
- Maintaining an audit trail of all changes.

Refer to the *IT Handbook's* "Development and Acquisition" booklet for more information.

II.C.10(a) Configuration Management

Configuration management is a process to securely maintain the institution's technology by developing expected baselines for tracking, controlling, and managing systems settings. To mitigate information security risk, management should control configurations of systems, applications, and other technology. Effective configuration management relies on policies and procedures to ensure compliance with minimally acceptable system configuration requirements. When information systems change, management should update baselines; confirm security settings; and track, verify, and report configuration items. Configurations should be monitored for unauthorized changes, and misconfigurations should be identified. Management can use automated solutions to help track, manage, and identify necessary corrections.

II.C.10(b) Hardening

Institutions typically use commercial off-the-shelf (COTS) software for operating systems and applications, on such diverse platforms as network infrastructure, servers, desktops, laptops, and mobile devices. COTS systems generally provide more functions than are required for the specific purposes for which they are employed. A default installation of a server operating system may include mail, web, and file-sharing services on a system that does not require those functions. Unnecessary software and services represent a potential security weakness. Their presence increases the potential number of discovered and undiscovered vulnerabilities in the system. Additionally, system administrators may not install patches or monitor the unused software and services to the same degree as they would operational software and services. Protection against those risks begins when the systems are constructed and software installed through a process that is referred to as hardening a system.

Management should consult operating system and software vendor-recommended security controls. When deploying COTS applications and systems, management should harden the resulting applications and systems. Hardening can include the following actions:

- Determining the purpose of the applications and systems and documenting minimum software and hardware requirements and services to be included.
- Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure.
- Installing necessary patches.
- Installing the most secure and up-to-date versions of applications.
- Configuring privilege and access controls by first denying all, then granting back the minimum necessary to each user (i.e., enforcing the principle of least privilege).
- Configuring security settings as appropriate, enabling allowed activity, and prohibiting non-approved activities.
- Enabling logging.
- Creating cryptographic hashes³¹ of key files.
- Archiving the configuration and checksums³² in secure storage before system deployment.
- Using secure replication procedures for additional, identically configured systems and making configuration changes on a case-by-case basis.
- Changing all default passwords.
- Testing the system to ensure a secure configuration.

Additionally, the systems should be audited periodically to ensure that the hardware, software, and services are authorized and properly configured.

II.C.10(c) *Standard Builds*

Consistency in system configuration makes security easier to implement and maintain. The institution should use standard builds, which allow one documented configuration to be applied to multiple computers in a controlled manner. Some institutions, depending on their size and complexity, may have many standard builds for the different system configurations needed to address various business functions. Through standard builds, an institution simplifies the following activities:

- Creating hardware and software inventories.
- Updating and patching systems.
- Restoring systems in the event of a disaster or outage.
- Investigating anomalous activity.
- Auditing configurations for conformance with the approved configuration.

The institution may not be able to meet all of its requirements from its standard builds. The use of nonstandard builds should be documented and approved by management, with appropriate changes made to patch management and disaster recovery plans.

³¹ A hash is a fixed-length cryptographic output of variables, such as a message, being operated on by a formula or cryptographic algorithm.

³² A checksum is a simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message, which allows the receiver to verify the accuracy of the message.

II.C.10(d) *Patch Management*

Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Hackers often will attempt to exploit these known vulnerabilities to try to gain access to the institution's systems. Third parties issue patches to address vulnerabilities found on institution systems and applications.³³ Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. In addition, management should use vulnerability scanners periodically to identify vulnerabilities in a timely manner.

As part of the institution's patch management process, management should establish and implement the following:

- A monitoring process that identifies the availability of software patches.
- A process to evaluate the patches against the threat and network environment.
- A prioritization process to determine which patches to apply across classes of computers and applications.
- A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments.
- An exception process, with appropriate documentation, for patches that management decides to delay or not apply.
- A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner.
- A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied.

The institution should have procedures that include how to implement patches to mitigate risks of changing systems and address systems with unique configurations. Before applying a patch, management should back up the production system. Additionally, management should define appropriate patch windows and, whenever possible, restrict the implementation of patches to defined time frames to minimize business impact or potential down time.

Patches make direct changes to the software and configuration of each system to which they are applied. While patches are necessary and useful, they may have unintended negative consequences, such as introducing new vulnerabilities, reintroducing old vulnerabilities, or degrading system performance. The following actions can help ensure patches do not compromise the security of the institution's systems:

- Obtain the patch from a known, trusted source.
- Verify the integrity of the patch through comparisons of cryptographic hashes to ensure the patch obtained is correct and unaltered.
- Protect and monitor the systems used to distribute patches to ensure only authorized patches are distributed.

³³ If an institution develops or maintains software in-house, management should have a process to update the software with appropriate patches.

- Apply the patch to an isolated test system before installing on the production system to ensure the patch is compatible with other software used on systems, does not alter the system's security posture in unexpected ways (such as altering log settings), and corrects the pertinent vulnerability.
- Test the resulting system to validate the effectiveness of the applied patch.

II.C.11 End-of-Life Management

Management should plan for a system's life cycle, eventual end of life, and any corresponding security and business impacts. The institution's strategy should incorporate planned changes to systems, including an evaluation of the current environment to identify potential vulnerabilities, upgrade opportunities, or new defense layers. Also included in this strategy should be considerations for the support provided by third-party system vendors and the risks related to operating unsupported legacy systems. Management should have policies to manage both the hardware and software life cycles. Security risks related to reaching a system's end of life include (a) the increased potential for vulnerabilities because the third party no longer provides patches or support, (b) incompatibility with other systems in the institution's environment, and (c) limitations in security features in older or obsolete systems.

Effective end-of-life management should include the following:

- Maintaining inventories of systems and applications.
- Adhering to an approved end-of-life or sunset policy for older systems.
- Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor.
- Conducting risk assessments on systems and applications to help determine end-of-life.
- Planning for the replacement of systems nearing obsolescence and complying with policy requirements for implementing new systems or applications.
- Developing specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information.

If an end-of-life system or application must remain in use, management should ensure appropriate mitigating controls are in place, which may include segregating the system or application from the network. Management should also have a plan to replace the system or application and implement compensating controls until replacement. Strategies for replacing and updating hardware and software should incorporate and align with overall information security and business strategies as appropriate.

II.C.12 Malware Mitigation

Attackers use malware to obtain access to an institution's environment and to execute an attack within the environment. Malware may enter through public or private networks and from devices

attached to the network. Although protective mechanisms may block most malware before it does damage, even a single malicious executable³⁴ may create a significant potential for loss.

Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. Methods or systems that management should consider include the following:

- Hardware-based roots of trust, which use cryptographic means to verify the integrity of software.
- Servers that run active content at the gateway and disallow content based on policy.
- Blacklists that disallow code execution based on code fragments, Internet locations, and other factors that correlate with malicious code.
- White lists of allowed programs.
- Port monitoring to identify unauthorized network connections.
- Network segregation.
- Computer configuration to permit the least amount of privileges necessary to perform the user's job.
- Application sandboxing³⁵ to limit the access and functionality of executed code.
- Monitoring for unauthorized software and disallowing the ability to install unauthorized software.
- Monitoring for anomalous activity for malware and polymorphic code.
- Monitoring of network traffic.
- User education in awareness, safe computing practices, indicators of malicious code, and response actions.

II.C.13 Control of Information

Action Summary

Management should control and protect access to and transmission of information to avoid loss or damage and do the following:

- Establish and supervise compliance with policies for storing and handling information, including storing data on mobile devices and cloud services.
- Define and implement appropriate controls over the electronic transmission of information.
- Facilitate safe and secure disposal of sensitive information.
- Secure physical media in transit.

³⁴ In computing, an executable is a file or a program that is able to be run by a computer.

³⁵ Sandboxing is the use of a restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

II.C.13(a) *Storage*

Management should implement policies to govern the secure storage of all types of sensitive information, whether on computer systems, on physical media, or in hard-copy documents. Management can achieve secure storage with physical controls,³⁶ logical controls (e.g., passwords, tokens, and biometrics), and environmental controls (e.g., fire and flood protection). In addition, stored information, in any form, should be classified and inventoried so that it can be retrieved when needed. Inventories should be updated periodically to remain current.

More sensitive information, such as system documentation, application source code, and production transaction data, should have more extensive controls to guard against alteration (e.g., integrity checkers and cryptographic hashes). Management should have appropriate logging and monitoring controls over stored information to ensure authorized access and appropriate use. Periodically, the security staff, audit staff, and data owners should review access rights to ensure the access rights remain appropriate and current.

Data storage in portable devices, such as laptops, smart phones, and tablets, poses unique problems. These devices may be lost, stolen, or subject to unauthorized and undetected use. Risk mitigation typically involves data encryption, host-provided access controls, homing beacons,³⁷ and remote deletion³⁸ capabilities. Management should implement appropriate controls (such as the use of a DLP program) over portable devices and the sensitive information contained on them.

Many institutions create or use a third-party cloud for storage. Cloud storage³⁹ provides unique issues and challenges. Management should understand the nature of the cloud technology being used; the physical location(s) where the data are stored and related legal jurisdiction; the access controls used and protection of the institution's data (e.g., how access is controlled and how that information is retrieved); and the frequency and method of backup used by the cloud provider. Management should verify that the cloud provider offers the capability for the institution to monitor its system activity, significant security incidents, performance and uptime, and success and failure of backups.

II.C.13(b) *Electronic Transmission of Information*

Electronic transmission of information can include e-mail, file transfer protocol (FTP), secure FTP (sFTP), secure shell, dedicated line, short message service/texting, and transmission via the Internet. Management should determine the type of transmission method, sensitivity of the

³⁶ Refer to the "Physical Security" section of this booklet.

³⁷ Homing beacons send messages to the institution when they connect to a network and enable recovery of the device.

³⁸ Remote deletion is a technology that enables the institution to remotely delete certain data from a portable device.

³⁹ Cloud storage is a model of data storage in which the digital data are stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.

information to be transmitted, and types of safeguards available to protect information. Management should implement appropriate controls or, if they are not available, restrict the type of information that can be transmitted. When transmitting sensitive information over a public network, information should be encrypted to protect it from interception or eavesdropping. Techniques include secure e-mail protocols, sFTP, and secure sockets layer (SSL) certificates.

II.C.13(c) *Disposal of Information*

The institution should have appropriate disposal procedures for paper-based and electronic information.⁴⁰ Designating a single individual, department, or function to be responsible for disposal facilitates accountability and promotes compliance with disposal policies.

Policies should prohibit employees from discarding paper-based information containing sensitive information by using the same disposal system as regular garbage to avoid accidental disclosure. Many institutions shred paper-based media on-site while others use collection and disposal services to ensure the media are rendered unreadable and unlikely to be reconstructed. Institutions that contract with third-party service providers should conduct due diligence to ensure those third parties conduct adequate employee background checks and employ appropriate controls. Contracts with third-party disposal firms should address acceptable disposal procedures.

Electronic information and computer-based media present distinct disposal challenges. In addition to disk drives and other forms of storage, information frequently is contained in or on the memory of other devices (e.g., printers, fax machines, and cellphones). Residual data frequently remain on media, even after deletion. Because the data can be recovered, additional disposal techniques should be applied to devices containing sensitive data. Overwriting destroys data by replacing it with new, random data. Overwriting may be preferable when the media will be reused. To be effective, overwriting may have to be performed many times.

Another disposal technique is degaussing, which scrambles the data recorded on the media with powerful, varying magnetic fields. Physical destruction of the media can make the data unrecoverable. Data can sometimes be destroyed after overwriting. Management should determine the most effective method of disposal based on the type of information. Policies and procedures should address making data non-recoverable. The institution should base its disposal policies on the sensitivity of the information. Policies, procedures, and training should inform employees about what actions should be taken to securely dispose of computer-based media and protect the data from the risks of reconstruction. Management should log the disposal of sensitive media. Logs should record the party responsible for disposal, as well as the date, media type, hardware serial number, and method of disposal. In cases when such devices are rented, rather than owned, by the institution, media sanitization should be addressed contractually so that sensitive information is disposed of properly before returning equipment at the end of the rental period.

⁴⁰ See also Information Security Standards, section III.C.4., requiring each financial institution to develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of “customer information” and “consumer information.”

II.C.13(d) *Transit of Physical Media*

Management should implement policies for maintaining the security of physical media (including backup tapes) containing sensitive information while in transit, including to off-site storage, or when shared with third parties. Policies should include the following:

- Contractual requirements that incorporate necessary risk-based controls.
- Restrictions on the carriers used.
- Procedures to verify the identity of couriers.
- Requirements for appropriate packaging to protect the media from damage.
- Use of adequate encryption of sensitive information recorded on media that is being physically transported.
- Tracking of shipments to provide early indications of loss or damage.
- Security reviews or independent security reports of receiving companies.
- Use of nondisclosure agreements for couriers and third parties.

II.C.13(e) *Rogue or Shadow IT*

Management should have policies explaining that employees should not and are not authorized to use unsanctioned or unapproved IT resources (e.g., online storage services, unapproved mobile device applications, and unapproved devices). Security awareness or information security training should include procedures for identifying and reporting shadow IT.

II.C.14 *Supply Chain*

The typical institution purchases a wide variety of hardware and software, which often is manufactured or developed internationally. In a supply chain attack, a threat source incorporates unidentified and harmful features into the purchased items before delivery. During the risk identification process, management should identify factors that may increase risk from supply chain attacks and respond with appropriate risk mitigations. An effective information security program seeks to limit the potential for harm through techniques tailored to specific acquisitions and services. Examples of techniques to mitigate the risk from such attacks include the following:

- Only making purchases through reputable sellers who demonstrate an ability to control their own supply chains.
- Purchasing hardware and software through third parties to shield the institution's identity.
- Reviewing hardware for anomalies.
- Using automated software testing and code reviews for software.
- Regularly reviewing the reliability of software and hardware items purchased through activity monitoring and evaluations by user groups.

II.C.15 Logical Security

Action Summary

Management should have an effective process to administer logical security access rights for the network, operating systems, applications, databases, and network devices, which should include the following:

- Assigning users and devices the access required to perform required functions.
- Updating access rights based on personnel or system changes.
- Reviewing users' access rights at an appropriate frequency based on the risk to the application or system.
- Designing appropriate acceptable-use policies and requiring users to agree to them.
- Controlling privileged access.
- Changing or disabling default user accounts and passwords.

System devices, programs, and data are system resources. Because users may access these resources through the institution's network, management should identify and restrict logical access to all system resources to the minimum required for legitimate and approved work activities, according to the principle of least privilege. Access beyond the minimum required for work to be performed exposes the institution's systems and information to a potential loss of confidentiality, integrity, and availability. The institution's logical security policy and procedures should address access rights and how those rights are to be administered. Management and system administrators should regularly evaluate information system access.

Logical user access rights administration consists of three processes:

- Enrolling new users to the system.
- Authorizing modifications to user access and deletions.
- Monitoring access rights granted to each user, including periodic review and validation of access rights.

The enrollment process establishes the user's identity and anticipated business needs for information and systems. Management should identify and evaluate all users, including new employees, IT outsourcing relationships, and contractors. The assignment of access rights is typically performed by the employee's manager and the application or data owners responsible for each accessed resource, with documented approval. The assignment of rights may also be established by the employee's role or group membership, which confers certain user access rights.

Management should have an authorization process to enable the employee's manager and the application or data owners to modify or delete existing user access rights to information and systems. The authorization process should include controls to verify that proper authorizations were granted or removed. Modifications to access rights should occur when an individual's business needs change. Job changes can result in an expansion, reduction, or deletion of needed

access rights. Job changes that could trigger a modification or deletion of access rights include transfers, mandatory leave, resignations, and terminations. The institution should promptly review, and modify as needed, access rights for all users who experience job changes, particularly those with privileged access, remote access privileges, and access to customer information.

As part of the user access rights monitoring process, management should perform regular reviews to validate user access. Reviews should test whether access rights continue to be appropriate or whether they should be modified or deleted. Management should review access rights on a schedule commensurate with risk.

Logical user access rights administration also constrains user activities through an acceptable use policy that details permitted system uses, user activities, and the consequences of noncompliance. Management should maintain an acceptable use policy, and employees should be required to acknowledge and agree in writing to the policy. When implemented correctly, an acceptable use policy is a key control for user awareness and administrative policing of system activities. Elements of an acceptable use policy can include the following:

- Specific access devices that can be used to access the network.
- Hardware and software changes the user can make to his or her access device.
- Purpose and scope of network activity.
- Permitted network services.
- Information that can or cannot be transmitted, and authorized transmission methods.
- Bans on attempts to break into accounts, crack passwords, or disrupt service.
- Responsibilities for secure operation.
- Consequences of noncompliance.

Authorization for privileged access should be tightly controlled. Privileged access refers to the ability to override system or application controls, and may include system administrator access. All individuals who are granted privileged access should have the appropriate training commensurate with the risk and complexity of the systems and information they access. Prudent practices for controlling privileged access include the following:

- Identifying each privilege associated with each system resource.
- Implementing a process to allocate privileges on a need-to-use or an event-by-event basis.
- Documenting the granting and extent of privileged access.
- Assigning privileges to a unique user ID apart from the one used for normal business use.
- Prohibiting shared privileged user accounts.
- Logging and independent monitoring of the use of privileged access.
- Reviewing, by an independent party, privileged access rights and allocations at appropriate intervals.

Access rights to new software and hardware present a different problem. Typically, hardware and software are shipped with default users and at least one default user has privileged access. Lists of default accounts and passwords are readily available and can enable anyone with access to the system to obtain privileged access. These passwords should be changed, and the accounts

should be disabled. Alternately, if these accounts are not disabled, access should be monitored closely.

II.C.15(a) *Operating System Access*

Access to the operating system and system utilities provide users with the authority to make fundamental changes to the system. System utilities are programs that perform repetitive functions, such as creating, deleting, changing, or copying files. System utilities also could include numerous types of system management software that can supplement operating system functionality by supporting common system tasks, such as security, system monitoring, or transaction processing.

Unauthorized access to the operating system and system utilities could result in significant financial and operational losses. System and security administrators should restrict and monitor privileged access to operating systems and system utilities. Many operating systems have integrated or third-party access control software, which is often essential to effective access control and can be used to integrate the security management of the operating system and applications. To prevent unauthorized access to or inappropriate activity on the operating system and system utilities, management should do the following:

- Implement effective user access to appropriately restrict system access for both users and applications and, depending on the sensitivity, extend protection at the program, file, record, or field level.
- Limit the number of employees with access to operating systems and grant only the minimum level of access required to perform job responsibilities.
- Restrict and log access to and activity on operating system parameters, system utilities (especially those with data-altering capabilities), and sensitive system resources (including files, programs, and processes), and supplement with additional security software, as necessary.
- Restrict operating system access to specific terminals in physically secure and monitored locations.
- Secure or remove external drives and portable media from system consoles, terminals, or personal computers (PC) running terminal emulations, residing outside of physically secure locations.
- Prohibit remote access to operating system and system utilities, where feasible, and, at a minimum, require strong authentication and encrypted sessions before allowing such remote access.
- Filter and review logs for potential security events and provide adequate reports and alerts.
- Independently monitor operating system access by user, terminal, date, and time of access.

II.C.15(b) *Application Access*

Sensitive or mission-critical applications should incorporate appropriate access controls that restrict which functions are available to users and other applications. These access controls allow authorized users and other applications to interface with related databases. Some security software programs integrate access control between the operating system and some applications.

Such software is useful when applications do not have their own access controls or when the institution uses security software instead of the application's native access controls. Management should understand the functionality and vulnerabilities of the application access control solutions and consider those issues in the risk management process.

Management should implement effective application access controls by doing the following:

- Implementing a robust authentication⁴¹ method consistent with the criticality and sensitivity of the application.
- Easing the administrative burden of managing application access rights by using group profiles. Managing access rights individually can lead to inconsistent or inappropriate access levels.
- Periodically reviewing and approving the application access assigned to users for appropriateness.
- Communicating and enforcing the responsibilities of programmers, security administrators, and application owners for maintaining effective application access control.
- Setting time-of-day or terminal limitations for some applications or for more sensitive functions within an application.
- Logging access and events, defining alerts for significant events, and developing processes to monitor and respond to anomalies and alerts.

II.C.15(c) *Remote Access*

Management should develop policies to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner. Such policies and procedures should define how the institution provides remote access and the controls necessary to offer remote access securely. Management should employ the following measures:

- Disable remote communications if no business need exists.
- Tightly control remote access through management approvals and subsequent audits.
- Implement robust controls over configurations at both ends of the remote connection to prevent potential malicious use.
- Log and monitor all remote access communications.
- Secure remote access devices.
- Restrict remote access during specific times.
- Limit the applications available for remote access.
- Use robust authentication methods for access and encryption to secure communications.

There are several methods to provide remote access to employees. A prevalent form of remote access is through a VPN, which provides employees with a remote connection to the institution's network through a secure channel. The VPN connection uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure

⁴¹ Stronger authentication and layered security methods, such as the use of tokens, public-key infrastructure-based systems, or out-of-band verification coupled with a robust identity and access management process, can reduce the potential for unauthorized access.

access to their organization's network. VPN provides an encrypted isolated “tunnel” or connection between a remote user’s computer and the internal network.

Because VPN connections provide access to sensitive internal networks, the connections require additional authentication from the remote user. Use of physical token devices is a common method that can provide one-time passwords to strongly authenticate remote users.

While VPNs effectively connect the remote computer to the internal network, other alternatives provide virtual desktop capability. In these cases, the remote computer connects to a special purpose software system (sometimes a website), authenticates the user, and establishes a secure connection to an internal network server. That server establishes a local internal network desktop session and connects it to the screen, keyboard, mouse, and speakers of the remote computer. This is an actual remote control environment, where the remote user’s actions have the same effect as if connected to an actual internal network desktop. The remote control configuration may permit file transfer between the remote and internal computers. If the remote access method allows users to store sensitive institution information, management should consider limiting this access to institution-owned devices.

Other methods of remote access are available, including remote control software and third-party services, file transfer software (e.g., FTP), conferencing/session sharing tools, and other remote desktop software. Management should conduct a risk assessment and implement appropriate controls before adopting any remote access solution.

If the institution allows employees to use authorized remote access methods with institution-owned devices, management should implement the following mitigating controls:

- Prevent users from installing software on the devices.
- Prohibit users from having administrative privileges on the devices.
- Use firewalls, host-based IDS, and packet content filtering to identify, monitor, and limit remote access activities.

II.C.15(d) *Use of Remote Devices*

Management may choose to allow employees to connect remotely to the institution’s network using either an institution-owned or a personally owned device (often referred to as BYOD or “bring your own device”). Institution-owned devices are easier to secure because the institution controls the devices’ configuration and often can implement remote wiping if the devices are lost or stolen. It may be more difficult to implement remote wiping or a similar measure on an employee’s personally owned device. BYOD is becoming more popular, however, with institutions and employees because it reduces costs to the institution and enables employees to carry one device instead of two.

For all remote devices, management should do the following to control employee remote access to the institution’s network:

- Disallow remote access unless a compelling business justification exists.

- Require management approval of employee remote access.
- Regularly review remote access approvals and rescind those that no longer have a compelling business justification.
- Restrict remote access to authorized network areas and applications by using VLANs, permissions, and other techniques.
- Log remote access communications (including date, time, user, user location, duration, and activity), analyze logs in a timely manner, and follow up on anomalies.
- Implement robust authentication methods for remote access.
- Use encryption to protect communications between the access device and the institution.
- Use application white-listing.⁴²

For institution-owned devices, the institution should have the ability to manage the remote devices. The following controls should be implemented:

- Securely configure remote access devices.
- Protect remote access devices against malware.
- Patch, update, and maintain all software on remote access devices.
- Encrypt sensitive data residing on the access device.
- Implement secure containers with internal boundaries to store sensitive information, in a way that is not accessible to the device without permission.
- Periodically audit the access device configurations and patch levels.
- Remotely disable or wipe the device in the event of theft or loss.
- Use geolocation of the device to support device recovery efforts.

For personally owned devices, the institution may not have the ability to configure the devices; therefore, management should have an effective method or solution to ensure that such devices meet defined institution security standards, such as operating system version, patch levels, and anti-malware solutions, before such devices are allowed to log on to the network.

II.C.16 Customer Remote Access to Financial Services

Action Summary

Management should do the following:

- Develop and maintain policies and procedures to securely offer and strengthen the resilience of remote financial services, if the institution offers such services.
- Plan for actions that adversely affect the availability of remote banking services to customers.
- Coordinate appropriate responses with the institution's ISPs and third-party service providers.
- Regularly test the institution's response plans.

⁴² Application white-listing is the maintenance and use of a list of applications and their components (e.g., libraries and configuration files) that are authorized to be present or active on a system according to a well-defined baseline.

Institutions increasingly offer services to customers through remotely accessible technology, such as the Internet and mobile financial services. If the institution offers such services, management should implement appropriate authentication techniques⁴³ commensurate with the risk from remote banking activities. Beyond authentication, remote access controls should include additional layered security controls and may include some combination of the following:

- Application time-outs with mandatory re-authentication.
- Fraud detection and monitoring systems that include consideration of customer history and behavior to alert management, and enable a timely and effective institution response.
- Dual customer authorization through different access devices.
- Out-of-band⁴⁴ verification for transactions.
- Positive pay,⁴⁵ debit blocks, and other techniques to appropriately limit the transactional use of the account.
- Supplementary controls over certain account activities, such as transaction value limits, restrictions on devices for adding payment recipients, limits on the number of transactions allowed per day, and allowable payment windows (e.g., days and times).
- Tools to block connections to the institution's servers based on device or network indicators known or suspected to be associated with fraudulent activities.
- Device authentication with appropriate enrollment and de-enrollment processes.
- Policies for addressing customer devices identified as potentially compromised and identifying customers who may be facilitating fraud.
- Controls over changes to account maintenance activities (e.g., address or password changes) performed by customers either online or through customer service channels.
- Supplementary controls for system administrators who are granted privileges to set up or change system configurations of business accounts.⁴⁶
- Customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

Institution customers may also use e-mail or other electronic means to transmit instructions. All instructions received through such channels should be authenticated and validated in accordance with institution policies.

An area of heightened concern when financial institutions offer remote financial services is the potential for malicious activity against the institution's mobile or online services. Malicious actors may restrict availability to those services through denial of service (DOS) attacks that target the institution's ISPs, third-party service providers, infrastructure, or applications.

⁴³ Techniques include multiple factor authentication, device authentication, location consistency, and additional authentication for sensitive functions.

⁴⁴ Out-of-band refers to activity outside of the primary means of interfacing with the customer. For example, if a user is performing activity online, he or she may be authenticated through a one-time password sent via text message.

⁴⁵ Positive pay is a technique that can reduce check fraud by requesting businesses to send electronic files of information to the financial institution on all checks the business has issued.

⁴⁶ Refer to the FFIEC's ["Supplement to Authentication in an Internet Banking Environment."](#)

Additionally, attacks on organizations that share infrastructure with the institution, including domain name services, may adversely affect the availability of remote services. Management should develop and maintain policies and procedures to identify, measure, mitigate, monitor, and report on significant security incidents to ensure the resilience of remote financial services. Planning and coordination by the institution and its third-party service providers may improve the resilience of services in the face of those attacks. To prevent or minimize exposure to these incidents, management should do the following:

- Monitor threat alerts.
- Monitor service availability and diagnose causes of reduced availability.
- Monitor applications and network traffic for indicators of nefarious activity.
- Ensure traffic filtering by the institution's ISP or upstream ISP,⁴⁷ third-party service providers, and internal resources.
- Design and implement applications to withstand application-level DOS.
- Utilize distributed architecture.
- Limit traffic (e.g., allow valid traffic and block known bad traffic by port or IP address).
- Add bandwidth.
- Enable access to services through alternative channels.

The institution should develop and test an incident response plan in conjunction with the institution's ISPs and third-party service providers to mitigate the interruption of mobile or remote financial services. Refer to the "Incident Response" section of this booklet for more information.

Customers may be provided with a website disclosure with the institution's customer acceptable-use policy. Depending on the nature of the website, the institution may require customers to demonstrate knowledge of and agreement to abide by the terms of the acceptable use policy. That evidence can be paper-based or electronic.

Refer to appendix E⁴⁸ of the *IT Handbook's* "Retail Payment Systems" booklet for more information about mobile financial services.

II.C.16(a) Customer Awareness

The institution's customer awareness and education efforts should consider both retail and commercial account holders and include the following elements:

- An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts accessible online.

⁴⁷ An upstream ISP is usually a large ISP that provides Internet access to a local ISP.

⁴⁸ See the *IT Handbook's* "Retail Payment Systems" booklet, appendix E, "[Mobile Financial Services](#)."

- An explanation that while the institution may contact a customer regarding his or her account or suspicious activities related to his or her account, the institution should never ask the customer to provide his or her log-in credentials over the phone or via e-mail.
- A list of recommended controls and prudent practices that the customer should implement when using the institution's remote financial services.
- A suggestion that commercial online customers perform a related risk assessment and controls evaluation periodically.
- Recommendations of technical and business controls to commercial customers that can be implemented to mitigate the risks from fraud schemes such as Business Email Compromise.⁴⁹
- A method to contact the institution if customers notice suspicious account activity.

II.C.17 Application Security

Action Summary

Management should use applications that have been developed following secure development practices and that meet a prudent level of security. Management should develop security control requirements for all applications, whether the institution acquires or develops them. Information security personnel should be involved in monitoring the application development process to verify that secure development practices are followed, security controls are implemented, and information security needs are met.

Institutions and their customers use a wide variety of applications. Such applications include core banking applications, web applications, and installable applications (e.g., downloadable mobile applications).

A secure software development life cycle ensures that Internet- and client-facing applications have the necessary security controls. The institution should ensure that all applications are securely developed. To verify the controls have been developed and implemented appropriately, management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications. Issues noted from tests should be remediated before launching applications or moving changes into production. At institutions that employ third parties to develop applications, management should ensure that the third parties meet the same controls.

Applications should provide the ability for management to do the following:

- Implement a prudent set of security controls (e.g., password and audit policies), audit trails of security and access changes, and user activity logs for all applications.
- Establish user and group profiles for applications if not part of a centralized identity access management system.

⁴⁹ See Federal Bureau of Investigation, [Alert I-012215-PSA](#).

- Change and disable default application accounts upon installation.
- Review and install patches for applications in a timely manner.
- Implement validation controls for data entry⁵⁰ and data processing.⁵¹
- Integrate additional authentication and encryption controls, as necessary, to ensure integrity and confidentiality of data and non-repudiation of transactions.
- Protect web or Internet-facing applications through additional controls, including web application firewalls, regular scanning for new or recurring vulnerabilities, mitigation or remediation of common security weaknesses, and network segregation to limit inappropriate access or connections to the application or other areas of the network.
- Mitigate risks from potential flaws in applications allowing remote access by customers and others through network, host, and application layer architecture considerations.
- Obtain attestation or evidence from third-party developers that the application acquired by the institution meets the necessary security requirements and that noted vulnerabilities or flaws are remediated in a timely manner.
- Perform ongoing risk assessments to consider the adequacy of application-level controls in light of changing threat, network, and host environments.
- Implement minimum controls recommended by the third-party service provider and consider supplemental controls as appropriate.
- Review available audit reports, and consider and implement appropriate control recommendations
- Collect data to build metrics and reporting of configuration management compliance, vulnerability management, and other measurable items as determined by management.

Whether the institution acquires or develops applications, management should establish security control requirements for new systems, system revisions, or new system acquisitions. Management should define the security control requirements based on its risk assessment process and evaluate the value of the information at risk and the potential impact of unauthorized access or damage within existing software development and acquisition processes. Management should have a process to determine risks posed by the system and necessary security requirements. Management may also refer to published, widely recognized industry standards as a starting point for establishing the institution's security requirements.

Information security personnel should be involved from the outset in the application development process to determine whether security controls are designed, tested, and implemented and information security needs are being met. Monitoring the development environment can help ensure that the implemented controls are functioning properly. Institutions that purchase applications typically rely on third-party service providers to develop applications with appropriate security built-in; management, however, should perform its own verification to

⁵⁰ Data entry validation controls include access controls over entry and changes to data, error checks, review of suspicious or unusual data, and dual entry or additional review and authorization for highly sensitive transactions or data.

⁵¹ Data processing controls include batch control totals, hash totals of data for comparison after processing, identification of any changes made to data outside the application (e.g., data-altering utilities), and job control checks to ensure programs run in correct sequence.

determine whether the application meets the institution's security requirements. Management should analyze the environment where the application will reside. As the environment changes, the security requirements and assurance needs for the application may also change. Management should leverage available resources⁵² to assist in risk identification and improve the institution's application security practices.

II.C.18 Database Security

Action Summary

Management should implement effective controls for databases and restrict access appropriately.

Databases are collections of information organized to be easily accessed, managed, and updated. Databases can be developed in-house or purchased from third parties and have their own controls and protective mechanisms configured to provide varying levels of protection. Along with many other security features, encryption helps to protect the stored information from theft or unauthorized viewing. Management should implement or enable controls commensurate with the sensitivity of the data stored in or accessed by the database.

Database users may be people (e.g., employees, customers, and contractors) or other applications. Users have different levels of access and authorization. Some users may have extensive privileges, including the ability to change the database configuration and access controls. Other users may have restrictions in what they can view, manipulate, or store. When a person is the database user, authorizations can be tailored to that person, greatly limiting the amount of information that could be exposed in a security incident. When an application is the database user, the access granted to the application can be more extensive than a person would require. Accordingly, an attack on a database through an application could expose a larger and more damaging collection of data. For application accounts, management should strengthen authentication and monitoring requirements to minimize the potential for unauthorized use.

Management should appropriately control user access and apply the principle of least privilege in assigning authorizations. The use and overall configuration of a database's security features should be part of a well-designed, layered security program.

II.C.19 Encryption

Action Summary

Management should implement the type and level of encryption commensurate with the sensitivity of the information.

⁵² Resources include software tools, industry resources, specific certifications, and education courses.

Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. Encryption can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols.

Encryption can be used as a preventive control, a detective control, or both. As a preventive control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow management to discover unauthorized changes to data. When prevention and detection are joined, encryption can be an important control in ensuring confidentiality, integrity, and availability.

Institution management should employ encryption strength sufficient to protect information from disclosure. Encryption methods should be reviewed periodically to ensure that the types and methods of encryption are still secure as technology and threats evolve. Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure and the costs of encryption. The need to encrypt data is determined by the institution's data classification and risk assessment.

Passwords should be hashed or encrypted in storage. Passwords that are hashed also should be salted.⁵³ Files containing encrypted or hashed passwords used by systems to authenticate users should be readable only with elevated (or administrator) privileges.

Key management⁵⁴ is crucial to the effective use of encryption. Effective key management systems rely on an agreed set of standards, procedures, and secure methods that address the following:⁵⁵

- Generating keys for different cryptographic systems and different applications.
- Generating and obtaining public keys.
- Distributing keys to intended users, including how keys should be activated when received.
- Storing keys, including how authorized users obtain access to keys.
- Changing or updating keys, including rules on when and how keys should be changed.
- Addressing compromised keys.
- Archiving, revoking, and specifying how keys should be withdrawn or deactivated.
- Recovering keys that are lost or corrupted as part of business continuity management.
- Logging the auditing of key management-related activities.
- Instituting defined activation and deactivation dates, and limiting the usage period of keys.

⁵³ In password protection, salt is a random string of data used to modify a password hash.

⁵⁴ Key management is the management of cryptographic keys. This includes dealing with the generation, exchange, storage, use, and replacement of keys.

⁵⁵ Refer to ISO/IEC 11770-1:2010, "Key Management—Part 1: Framework"; ISO/IEC 11770-2:2008, "Key Management—Part 2: Mechanisms Using Symmetric Techniques"; and ISO/IEC 11770-3:2015, "Key Management—Part 3: Mechanisms Using Asymmetric Techniques."

II.C.20 Oversight of Third-Party Service Providers

Action Summary

Management should oversee outsourced operations through the following:

- Appropriate due diligence in third-party research, selection, and relationship management.
- Contractual assurances for security responsibilities, controls, and reporting.
- Nondisclosure agreements regarding the institution's systems and data.
- Independent review of the third party's security through appropriate reports from audits and tests.
- Coordination of incident response policies and contractual notification requirements.
- Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported.

Management should conduct appropriate due diligence in selecting and monitoring third-party service providers. Management should be responsible for ensuring that such third parties use suitable information security controls when providing services to the institution. When indicated by the institution's risk assessment, management should monitor third-party service providers to confirm that they are maintaining appropriate controls. If the third-party service provider stores, transmits, processes, or disposes of customer information, management should require third-party service providers by contract to implement appropriate measures designed to meet the Information Security Standards.

Management should evaluate information security considerations of potential third-party service providers during initial due diligence. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

Management should verify that third-party service providers implement and maintain controls sufficient to appropriately mitigate risks. The institution's contracts should do the following:

- Include minimum control and reporting standards.
- Provide for the right to require changes to standards as external and internal environments change.
- Specify that the institution or an independent auditor has access to the service provider to perform evaluations of the service provider's performance against the Information Security Standards.

Refer to the "Third-Party Reviews of Technology Service Providers" section of the *IT Handbook's* "Audit" booklet for more information.

Additionally, as part of the oversight of third-party service providers, management should determine whether cyber risks are identified, measured, mitigated, monitored, and reported by such third parties as third-party cyber threats can have an impact on the institution. Information security reporting by the institution should incorporate an assessment of these third-party risks to

facilitate a comprehensive understanding of the institution's exposure to third-party cyber threats.

II.C.20(a) *Outsourced Cloud Computing*

As with other forms of outsourcing, information security implications are key in the cloud computing model. Management may need to revise information security policies, standards, and procedures to incorporate the activities related to a cloud computing service provider. Refer to the FFIEC's "Outsourced Cloud Computing" statement for more information.⁵⁶

II.C.20(b) *Managed Security Service Providers*

Management may rely on third parties to provide security services; management, however, remains responsible for ensuring the security of the institution's systems and information by overseeing the effectiveness of the services provided by the managed security services provider. Additional information is available in appendix D of the *IT Handbook's* "Outsourcing Technology Services" booklet.

II.C.21 Business Continuity Considerations

Action Summary

Management should do the following:

- Identify personnel who will have critical information security roles during a disaster, and train personnel in those roles.
- Define information security needs for backup sites and alternate communication networks.
- Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios.

Business continuity plans should be reviewed as an integral part of the security process. Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution if continuity plans must be implemented. Management should train personnel regarding their security roles during a disaster. Additionally, management should update technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of the business continuity plan.

Information security events may trigger activation of the business continuity plan. Therefore, the institution's plan should include steps that explicitly address information security incident response and resilience. Resilience testing should incorporate information security event scenarios identified by the institution.

Refer to the *IT Handbook's* "Business Continuity Planning" booklet for more information.

⁵⁶ See FFIEC, "[Outsourced Cloud Computing](#)," July 10, 2012.

II.C.22 Log Management

Network and host activities typically are recorded on the host and sent across the network to a central logging repository. The data that arrive at the repository are in the format of the software that recorded the activity. The logging repository may process the data and can enable timely and effective log analysis. Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs.

Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Intruders often attempt to conceal unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging repository. Considerations for securing the integrity of log files include the following:

- Encrypting log files that contain sensitive data or that are transmitted over the network.
- Ensuring adequate storage capacity to avoid gaps in data gathering.
- Securing backup and disposal of log files.
- Logging the data to a separate, isolated computer.
- Logging the data to read-only media.
- Setting logging parameters to disallow any modification to previously written data.
- Restricting access to log files to a limited number of authorized users.

Additionally, logging practices should be reviewed periodically by an independent party to ensure appropriate log management.

Logs are voluminous and challenging to read. They come from a variety of systems and can be difficult to manage and correlate. Security information and event management (SIEM) systems can provide a method for management to collect, aggregate, analyze, and correlate information from discrete systems and applications. Management can use SIEM systems to discern trends and identify potential information security incidents. SIEM systems can be used to gather information from the following:

- Network and security devices and systems.⁵⁷
- Identity and access management applications.
- Vulnerability management and policy compliance tools.
- Operating system, database, and application logs.
- Physical and environmental monitoring systems.
- External threat data.

Regardless of the method of log management, management should develop processes to collect, aggregate, analyze, and correlate security information. Policies should define retention periods for security and operational logs. Institutions maintain event logs to understand an incident or cyber event after it occurs. Monitoring event logs for anomalies and relating that information

⁵⁷ These can include intrusion detection and prevention systems, DLP solutions, and firewalls.

with other sources of information broadens the institution's ability to understand trends, react to threats, and improve reports to management and the board.

II.D Risk Monitoring and Reporting

Risk monitoring is a process by which the institution tracks information about its inherent risk profile and identifies gaps in the effectiveness of risk mitigation activities. Risk monitoring should address changing threat conditions in both the institution and the greater financial industry. Threats change frequently, particularly in terms of the threat's capabilities and intentions, as well as the vulnerabilities they may exploit. Vulnerabilities in software are continually announced, and other vulnerabilities may emerge as the institution's systems are modified or updated. External requirements, including the use of new third-party service providers, also may change the institution's inherent risk profile.

Risk reporting is a process that produces information systems reports that address threats, capabilities, vulnerabilities, and inherent risk changes. Risk reporting should describe any information security events that the institution faces and the effectiveness of management's response and resilience to those events. The reporting process should provide a method of disseminating those reports to appropriate members of management. The contents of the reports should prompt action, if necessary, in a timely manner to maintain appropriate levels of risk.

II.D.1 Metrics

A mature and effective information security program uses metrics to improve the program's effectiveness and efficiency. Management should develop metrics that demonstrate the extent to which the security program is implemented and whether the program is effective. Metrics are used to measure security policy implementation, conformance with the information security program, the adequacy of security services delivery, and the impact of security events on business processes. The measurement of security characteristics can allow management to increase control and drive improvements to the security process. Metrics generally are formed to measure conformance to the standards and procedures that are used to implement policies.

Management should utilize metrics to quantify and report risks of the information security program. Metrics should be gathered from external sources and internal data. The scope of metrics should be comprehensive and commensurate with the complexity of the institution's operations. Reports should incorporate metrics tailored for different audiences and stakeholders. These metrics and other monitoring reports of the information security program should feed into ITRM reporting.

III Security Operations

Action Summary

Management should design policies and procedures to effectively manage security operations with the following characteristics:

- Broadly scoped to address all ongoing security-related functions.
- Guided by defined processes.
- Integrated with lines of business and third parties.
- Appropriately staffed and supplied with technology for continual incident detection and response activities.

Security operations involve a wide range of activities. Those activities may be centralized in a security operations center, distributed within the information security department and business lines, or outsourced in whole or in part. Security operations activities can include the following:

- Security software and device management (e.g., maintaining the signatures on signature-based devices and firewall rules).
- Forensics (e.g., analysis of potentially compromised systems).
- Threat identification and assessment.
- Vulnerability identification (e.g., operation or supervision of vulnerability scans, self-assessments, penetration tests, and analysis of audit results).
- Vulnerability cataloging and remediation tracking.
- Physical security management (e.g., CCTV, guards, and badge systems).
- Law enforcement interface (e.g., data retention and lawful intercepts).
- Third-party integration (e.g., managed security services and incident detection services).
- Network, host, and application activity monitoring.
- Analysis of threat intelligence from external sources.
- Engagement with information sharing groups.
- Incident detection and management.
- Enforcement of access controls.

Management should establish defined processes and appropriate governance to facilitate the performance of security operations. Policies should address the timing and extent of the security operations activities, reporting, escalation triggers, and response actions. Many institutions use an issue tracking system⁵⁸ to record and manage requests and events. An issue tracking system can be a source of evidence, contain a variety of security information, and serve as a valuable tool to assist management when taking actions to strengthen the information security environment.

⁵⁸ An issue tracking system (also ITS, trouble ticket system, ticketing management system, support ticket system, request management system, or incident ticket system) is a computer software package that manages and maintains lists of security issues.

Management should coordinate security operation activities with the institution's lines of business and with third-party service providers. Regardless of how extensive the coordination is, the goal should be to maintain a sufficient security operation capability across the entire environment.

Sufficient technology and staff should be available to support continual incident detection and response activities. Some institutions may rely on or supplement their activities with third parties to gain the necessary scope and depth of coverage. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

III.A Threat Identification and Assessment

Action Summary

Management should do the following:

- Identify and assess threats.
- Use threat knowledge to drive risk assessment and response.
- Design policies to allow immediate and consequential threats to be dealt with expeditiously.

Threat identification and assessment involves discovering knowledge about threat sources and vulnerabilities and analyzing the potential for exploitation. This is much more focused than the risk identification process described in the "Risk Identification" section of this booklet.

Information gained from threat identification and assessment should be used in risk assessment and response to drive protective and detective strategies and tactics. Strategies involve the information security program's policies, standards, and procedures, and the implementing technologies. Examples of tactics include threat signatures used for incident identification and management of threat behaviors. NIST notes that types of threat sources include the following:

- Hostile cyber or physical attacks.
- Human errors of omission or commission.
- Structural failures of organization-controlled resources (e.g., hardware, software, and environmental controls).
- Natural and man-made disasters, accidents, and failures beyond the control of the organization.⁵⁹

Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information. The identification of threats involves the sources of threats, their capabilities, and their objectives. Information about threats generally comes from government (e.g., US-CERT), information-sharing organizations (e.g., FS-ISAC), industry sources, the institution, and third parties. Third-party information may be from organizations that specifically track and report on threats or from third-party reports of past activity. Some of those

⁵⁹ NIST SP 800-30, revision 1, "[Information Security: Guide for Conducting Risk Assessments](#)," September 2012.

reports compile knowledge from incidents reported by many organizations worldwide. Different types of information supporting an assessment may be available through the following:

- Incident data from reports published by security providers and others.
- Attack data from sources including FS-ISAC and managed security service providers.
- Threat data through reports available either free or for a fee.

The availability of threat information is often ad hoc, although some providers present threat information within a defined framework that readily lends itself to analytical operations. By using a threat taxonomy, the institution may greatly reduce the complexity of threat assessment and enable efficient understanding of reasonable risk mitigations. Specific factors in the threat assessment may include a description, context for operation, capabilities and intent, and, from the threat-source perspectives, benefits and negative consequences associated with an attack.

Knowledge of threat sources is especially important to help identify vulnerabilities. Vulnerabilities can occur in many areas, such as the system design, the system operation, security procedures, business line controls, and the implementation of the system and controls. Self-assessments, audits, scans, penetration tests, and reviews of SIEM reports can identify vulnerabilities. Additionally, external individuals or groups can identify vulnerabilities.

Tools for analyzing vulnerabilities in a layered security environment include attack trees, event trees, and kill chains. These tools attempt to model an attacker's actions to enable identification of the most effective and efficient remediation options.

Once a threat is identified and potential vulnerabilities are assessed, the significance of the threat should trigger a response. The response should be commensurate with the risk posed by the threat and should include remediation options. Management should design policies to allow for immediate and consequential threats to be dealt with expeditiously, while less significant threats are addressed as part of a broader risk management process. When management receives vulnerability information from external individuals or groups, management should have appropriate processes and procedures to evaluate the credibility of the information to appropriately address it.

III.B Threat Monitoring

Threat monitoring policies should provide for continual and ad hoc monitoring of threat intelligence communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal procedures. Management should establish the responsibility and authority of security personnel and system administrators for monitoring. Additionally, management should review and approve the tools used and the conditions for use.

Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies. Monitoring should address incoming and outgoing network traffic, seeking to identify malicious activity and data exfiltration. Additionally, the monitoring process should be established and documented to independently monitor administrators and other users with higher privileges.

III.C Incident Identification and Assessment

Action Summary

Management should have a process to enable the following:

- Identify indicators of compromise.
- Analyze the event associated with the indicators.
- Classify the event.
- Escalate the event consistent with the classification.
- Report internally and externally as appropriate.

Incident identification involves indicators and analysis. External indicators may arise through contact with customers, law enforcement, card organizations (e.g., credit or payment cards), other financial institutions, media, or others. Internal indicators may arise when internal users contact the help desk, IT operations follows up on anomalies, or security operations follows up on anomalies identified through security devices and network and systems activity. Indicators may also arise through the use of “hunt teams,” or dedicated analysts who actively search for indicators of compromise. Examples of technology-based intrusion identification systems and tools include the following:

- Threat intelligence data feeds (e.g., STIX/TAXII).⁶⁰
- Intrusion detection and prevention systems for networks and hosts.
- End-point visibility tools (tools that can identify the function of end points and which end points contain or have access to sensitive information).
- DLP tools.
- Log correlation and analysis tools.
- File integrity tools.
- Malware detection tools.
- Network behavior analysis systems.
- “Big data” tools and analytics that aggregate and allow pre-formed and ad hoc analysis.

Technology-based indicators of compromise generally are anomalies in host state, host activity, and network traffic. A few examples are unexpected (1) processes, (2) changes to files, (3) packet source or destination, (4) protocols, (5) ports, (6) encryption, (7) log-ins, and (8) packet content. Other indicators include alerts triggered by black lists in anti-virus and network-monitoring products.

Management should have a process for identifying indicators of compromise and rapidly reporting those indicators for investigation. The report should instigate an analysis that seeks to

⁶⁰ There are efforts to automate and structure operational cybersecurity information-sharing techniques across the globe. Of these, STIX (the Structured Threat Information eXpression) and TAXII (the Trusted Automated eXchange of Indicator Information) are two of the technical specifications that allow an automated exchange of threat source data using standardized language.

confirm whether a compromise took place and how that compromise should be classified. Investigation may require additional information from outside and inside the institution, such as a forensic review. Management should perform due diligence to identify external assistance in advance of incidents to ensure available resources. Classification of a compromise may require information on the specific hosts affected, data lost, and business processes affected. Information developed in the analysis may be useful to guide response activities.

Analysis should result in a classification of the event, implementation of escalation procedures, and reporting. Analysis should be guided by the following:

- Classification policies should be sufficiently clear to enable timely classification of incidents by level of severity, enabling the use of response teams and responses depending on the type and severity of events.
- Escalation, response, and reporting should be commensurate with the level of severity.
- Escalation policies should address when different personnel within the organization will be contacted and the responsibility those personnel have in incident analysis and response.
- Escalation policies should include when to request or obtain external assistance, from both third parties and the federal government.
- Reporting policies should address internal and external reporting, including coordination with third parties and reporting to external organizations (e.g., FS-ISAC).

Additionally, a policy should address who is empowered to declare an incident. A defined process should guide responses to incidents. The institution should develop procedures to test the incident escalation, response, and reporting processes.

The sharing of attack data through organizations, such as FS-ISAC, also has the potential to benefit the industry at large by enabling other institutions to better assess and respond to current attacks. Management should consider whether to include such information sharing as a part of its strategy to protect the institution.

Management should determine whether the institution's or its managed security service provider's analysts are sufficiently trained to appropriately analyze network, host, and application activity and to use the monitoring and analysis tools made available to them. Additionally, security analysts should coordinate and collaborate with others in the institution with knowledge and authority for specific types of malicious activity, such as fraud.

III.D Incident Response

Management should have an incident response program.⁶¹ The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate, containing the incident, coordinating with law

⁶¹ See also "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," supplementing the Information Security Standards.

enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the institution.

The response involves a combination of people and technologies. The quality of incident response is attributable to the institution's culture, policies, procedures, and training. Incident response is also a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS-ISAC), and others. Management should prepare for potential incidents by developing an incident response plan that is comprehensive, coordinated, and integrated with existing institution policies, procedures, and training. To validate the effectiveness of the institution's incident response program, management should periodically test it through different test types, including scenario planning and tabletop testing, and perform the tests with appropriate internal and external parties.

Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort. Additionally, management should define thresholds for reporting significant security incidents, and consider developing processes for when the institution should notify its regulators of incidents that may affect the institution's operations or compromise sensitive customer information. These incidents may include those that could affect the financial system. Primary considerations for incident response include the following:

- How to balance concerns regarding confidentiality, integrity, and availability for devices and data. This consideration is a key driver for a containment strategy and may involve legal and liability considerations. Management may decide that some systems must be disconnected or shut down at the first sign of intrusion, while others must be left on line.
- When and under what circumstances to invoke the incident response activities, and how to ensure that the proper personnel are notified and available.
- When to involve outside experts and how to ensure the proper expertise will be available when needed. This consideration addresses both containment and restoration.
- Protocols to define when and under what circumstances to notify and involve regulators, customers, and law enforcement, including names and contact information for each group.
- Which personnel have authority to perform specific actions in the containment of the intrusion and restoration of the system. This consideration affects the internal communications strategy, the commitment of personnel, and procedures that escalate involvement and decisions within the organization.
- How, when, and what to communicate outside of the institution, whether to law enforcement, regulatory agencies, information-sharing organizations, customers, third-party service providers, potential victims, or others.
- How to document and maintain the evidence, the decisions made, and the actions taken.
- What criteria must be met before compromised services, equipment, and software are returned to the network.
- How to learn from the intrusion and use lessons learned to improve the institution's security.
- How and when to prepare and file a Suspicious Activities Report.

Successful implementation of any response policy or procedure requires the assignment of responsibilities, training, and testing. Some institutions formalize the response program with the creation of a security incident response team (SIRT). The SIRT typically is tasked with performing, coordinating, and supporting responses to security incidents and intrusions. Because of the wide range of technical and nontechnical issues posed by an intrusion, typical SIRT membership includes individuals with a wide range of backgrounds and expertise from different areas within the institution. Those areas include management, legal, and public relations, as well as IT staff. Other organizations may outsource some of the SIRT functions (e.g., forensic examinations). When SIRT functions are outsourced, management should require the third-party service provider to follow the institution's policies and maintain the confidentiality of data.

Institutions should assess the adequacy of their preparation through testing. There are a variety of testing methods; therefore, management should consider the most applicable tests for its IT environment. Institutions can also participate with outside entities that provide testing activities (e.g., FS-ISAC).

While containment strategies between institutions can vary, they typically include the following broad elements:

- Isolation of compromised systems or enhanced monitoring of intruder activities.
- Search for additional compromised systems.
- Collection and preservation of evidence.
- Communication with affected parties and often the primary regulator, information-sharing organizations (e.g., FS-ISAC), or law enforcement.

Restoration and follow-up strategies should address the following:

- Elimination of an intruder's means of access.
- Restoration of systems, programs, and data to a known good state.
- Initiation of customer notification and assistance activities consistent with laws, regulations, and interagency guidance.
- Monitoring to detect similar or further incidents.

Management should periodically review the actions taken in response to intrusions to identify improvements and implement those improvements through changes in policy, standards, procedures, training, and practices.

IV Information Security Program Effectiveness

The information security program should be subject to periodic review to ensure continual improvement in the program's effectiveness. The review should address the program in the context of the environment in which the program now operates, both within the institution and outside. Lessons learned from experience, audit findings, and other indicators of opportunities for improvement should be identified and the program changed as appropriate.

IV.A Assurance and Testing

Action Summary

Management should ascertain that the information security program is operating securely, as expected, and reaching intended goals by doing the following:

- Testing and evaluating through self-assessments, tests, and audits with appropriate coverage, depth, and independence.
- Aligning personnel skills and program needs.
- Establishing and implementing a reporting process that includes the assembly and distribution of assurance reports that are timely, complete, transparent, and relevant to management decisions.

Assurance relates to the confidence that the information security program is mitigating risk as expected. Assurance targets two parts of the process: (1) the IT system's design and (2) the IT system's operation. The institution should carefully distinguish between the two because the former relates to risk decisions that change the security controls and the latter relates to the operation of the controls. Flaws in control design typically are corrected by a redesign, and flaws in operation typically are corrected through a compliance program.

The institution should have a documented testing and evaluation plan that addresses the integration of security controls, level of assurance desired, and strategies and activities performed in obtaining that assurance. The plan should identify specific components of the system to address, methods by which the components are to be addressed, timing and frequency of the tests and evaluations, and criteria used to ascertain whether the test and evaluation results are acceptable and provide assurance.⁶²

IV.A.1 Key Testing Factors

Management should consider the following key factors when developing and implementing independent tests:

- **Scope.** The tests and methods utilized, in the aggregate, should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling the risk from information security-related events.
- **Personnel.** Technical testing is only as good as the personnel performing and supervising the test. Management should review qualifications of testing personnel to verify testers' capabilities are adequate to support the test objectives.
- **Notifications.** Management should consider whom to inform within the institution about the timing and nature of the tests. The need for protection of institution systems and the potential for disruptive false alarms should be balanced against the need to test personnel reactions to unexpected activities.

⁶² See also Information Security Standards, section III.C.3, requiring each financial institution to test the key controls, systems, and procedures of its information security program using independent third parties or staff independent of those that develop or maintain the program.

- **Confidentiality, integrity, and availability.** Management should carefully control information security tests to limit the risks to confidentiality, integrity, and system availability. Because testing may uncover sensitive customer information, management should use appropriate safeguards to protect such information. Management should ensure that employee and contract personnel who perform the tests or have access to the test results have passed appropriate background checks and that contract personnel are appropriately bonded. Because certain tests may pose more risk to system availability than other tests, management should have personnel who perform those tests maintain logs of testing actions. Those logs are helpful if the systems react unexpectedly.
- **Confidentiality of test plans and data.** Because knowledge of test planning and results may facilitate a security breach, the institution should carefully limit the distribution of testing information. Management should restrict test plans and data only to those individuals involved in the testing. Results should be made available in a usable form only to those responsible for following up on tests. Additionally, management should require contractors to sign nondisclosure agreements and to return information they obtained in their testing to the institution.
- **Frequency.** The institution's ITRM process should determine the frequency of independent testing. Factors that may increase testing frequency include changes to network configurations, changes to or additions of systems and applications, significant changes in potential attacker profiles and techniques, and results of other testing. For instance, management should have a testing process for security and usability over the life cycle of testing (during development, before placing a new or modified system into production, and periodic testing of the production system or application).
- **Proxy testing.** Proxy testing refers to testing that is conducted on like systems and with like interfaces, rather than the actual system, to avoid disruptions on a system that may be too critical for a comprehensive continuity test. Proxy tests are conducted using the same hardware and operating software, are sometimes used as a replacement for actual tests, and should provide similar results. Independent testing of a proxy system is generally not effective in validating the effectiveness of a security process. Proxy testing, by its nature, does not test the operational system's policies and procedures or its integration with other systems. It also does not test the reaction of personnel to unusual events. Proxy testing may be the best choice, however, when management is unable to test the operational system without creating excessive risk.

IV.A.2 Types of Tests and Evaluations

Information security management may use several tools to gain confidence that the information security program is operating as expected and reaching the intended goals. The primary tools include self-assessments, penetration tests, vulnerability assessments, and audits. The coverage and depth of the various tools directly relates to the confidence gained in the information security program.

IV.A.2(a) *Self-Assessments*

Periodic self-assessments typically should be performed by the organizational unit being assessed. Self-assessments capture subjective opinions on the achievement of objectives.

Although they may provide valuable information related to perceived changes in the level of risk and effectiveness of controls, they are affected by the breadth and depth of the assessor's knowledge, the completeness and reliability of information used to complete the assessment, and the assessor's biases. Self-assessment frequency should be a function of the level of assurance needed by the institution, determined by the risk management process. Results from self-assessments can be informative to the overall test and evaluation process. Management should use the results to help strengthen the organizational unit's information security.

IV.A.2(b) *Penetration Tests*

A penetration test subjects a system to real-world attacks selected and conducted by the testers. A penetration test targets systems and users to identify weaknesses in business processes and technical controls. The test mimics a threat source's search for and exploitation of vulnerabilities to demonstrate a potential for loss. Some tests focus on only a subset of the institution's systems and may not accurately simulate a determined threat actor. There are many types of penetration tests (e.g., network, client-side, web application, and social engineering), and management should determine the level and types of tests employed to ensure effective and comprehensive coverage.

The frequency and scope of a penetration test should be a function of the level of assurance needed by the institution and determined by the risk assessment process. The test can be performed internally by independent groups, internally by the organizational unit, or by an independent third party. Management should determine the level of independence required of the test.

IV.A.2(c) *Vulnerability Assessments*

A vulnerability assessment is a process that defines, identifies, and classifies the vulnerabilities in a computer, network, or communications infrastructure. Technical vulnerabilities can be identified through the use of scanners and other tools. Scanners search for known vulnerabilities (e.g., Mitre's CVE) or for known vulnerability classes (e.g., Structured Query Language [SQL] injection and cross-site scripting). They also can search for compliance with approved configurations. Scanners identify vulnerabilities by inspecting network traffic or hosts. When inspecting hosts, they may require agents to be placed on the hosts with high-level access. If host agents are required, the security over the use of credentials in the scan should be a prime consideration for management.

Similar to penetration testing, the frequency of the performance of vulnerability assessments should be determined by the risk management process. Scanners and other tools can be run continuously, generating metrics that are reported and acted upon continuously. Alternatively, they can be run periodically. Vulnerability assessments can be performed internally or by external testers, but they are often run as part of internal testing processes.

IV.A.2(d) Audits

Independent internal departments or third parties typically perform audits. Audits should review every aspect of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the reasonableness and appropriateness of, and compliance with, policies, standards, and procedures; report on information security activity and control deficiencies to decision makers; identify root causes and recommendations to address deficiencies; and test the effectiveness of controls within the program. Internal audit should track the results and the remediation of control deficiencies reported in audits and additional technical reviews, such as penetration tests and vulnerability assessments.

Refer to the *IT Handbook's* "Audit" booklet for more information.

IV.A.3 Independence of Tests and Audits

Institutions frequently use independent organizations to test aspects of their information security programs. Independent tests have the potential to reduce bias, increase capabilities, and increase knowledge about threats and technologies. Independence gives credibility to the test results. To be considered independent, testing personnel should not be responsible for the design, installation, maintenance, and operation of the tested system, or the policies and procedures that guide its operation. The reports generated from the tests should be prepared by individuals who similarly are independent.

IV.A.4 Assurance Reporting

Reporting of self-assessments, penetration tests, vulnerability assessments, and audits supports management decision making. Those decisions may support a range of ITRM activities, including the prioritization and funding of resource allocations and improvement to existing information security policies and procedures.

Management should provide reports that are timely, complete, transparent, and relevant to management decisions. The reports should prioritize risk and findings in the order of importance, suggest options for remediation, and highlight repeat issues. Additionally, reports should address root causes. The reporting should be to individuals with authority and responsibility to act on the reports and to those accountable for the outcomes, as well as those responsible for advising or influencing risk decisions. Reporting should trigger appropriate, timely, and reliable escalation and response procedures. Summary reports should be made available to the board as appropriate.

Appendix A: Examination Procedures

Examination Objective

Determine the quality and effectiveness of the institution's information security. Examiners should use these procedures to measure the adequacy of the institution's culture, governance, information security program, security operations, and assurance processes. In addition, controls should be evaluated as additional evidence of program quality and effectiveness. Controls also should be evaluated for conformance with contracts, indicators of legal liability, and conformance with regulatory policy and guidance. Failure of management to implement appropriate controls may expose the institution to potential loss from fines, penalties, and customer litigation.

These examination procedures (commonly referred to as the work program) are intended to help examiners determine the effectiveness of the institution's information security process. Examiners may choose, however, to use only particular components of the work program based on the size, complexity, and nature of the institution's business. Examiners should also use these procedures to measure the adequacy of the institution's cybersecurity risk management processes.

Objective 1: Determine the appropriate scope and objectives for the examination.

1. Review past reports for outstanding issues or previous problems. Consider the following:
 - a. Regulatory reports of examination.
 - b. Internal and external audit reports.
 - c. Independent security tests.
 - d. Regulatory, audit, and security reports on service providers.
2. Review management's response to issues raised at, or since, the last examination. Consider the following:
 - a. Adequacy and timing of corrective action.
 - b. Resolution of root causes rather than just specific issues.
 - c. Existence of any outstanding issues.
3. Interview management and review responses to pre-examination information requests to identify changes to technology infrastructure or new products and services that might increase the institution's risk. Consider the following:
 - a. Products or services delivered to either internal or external users.
 - b. Network topology or diagram including changes to configuration or components and all internal and external connections.
 - c. Hardware and software inventories.
 - d. Loss, addition, or change in duties of key personnel.
 - e. Technology service providers and software vendor listings.

- f. Communication lines with other business units (e.g., loan review, credit risk management, line of business quality assurance, and internal audit).
 - g. Credit or operating losses primarily attributable (or thought to be attributable) to IT (e.g., system problems, fraud occurring due to poor controls, and improperly implemented changes to systems).
 - h. Changes to internal business processes.
 - i. Internal reorganizations.
4. Determine the complexity of the institution's information security environment.
 - a. Determine the degree of reliance on service providers for information processing and technology support, including security operation management.
 - b. Identify unique products and services and any required third-party access requirements.
 - c. Determine the extent of network connectivity internally and externally and the boundaries and functions of security domains.
 - d. Identify the systems that have recently undergone significant change, such as new hardware, software, configuration, and connectivity. Correlate the changed systems with the business processes they support, the extent of customer data available to those processes, and the effect of those changes on institution operations.

Objective 2: *Determine whether management promotes effective governance of the information security program through a strong information security culture, defined information security responsibilities and accountability, and adequate resources to support the program.*

1. Determine whether the institution has a culture that contributes to the effectiveness of the information security program.
 - a. Determine whether the institution's board and management understand and support information security and provide appropriate resources for the implementation of an effective security program.
 - b. Determine whether the information security program is integrated with the institution's lines of business, support functions, and management of third parties.
 - c. Review for indicators of an effective information security culture (e.g., method of introducing new business initiatives and manner in which the institution holds lines of business and employees accountable for promoting information security).
2. Determine whether the board, or a committee of the board, is responsible for overseeing the development, implementation, and maintenance of the institution's information security program.
3. Determine whether the board holds management accountable for the following:
 - a. Central oversight and coordination.
 - b. Assignment of responsibility.
 - c. Support of the information security program.

- d. Effectiveness of the information security program.
4. Determine whether the board approves a written information security program and receives a report on the effectiveness of the information security program at least annually. Determine whether the report to the board describes the overall status of the information security program and discusses material matters related to the program such as the following:
 - a. Risk assessment process, including threat identification and assessment.
 - b. Risk management and control decisions.
 - c. Service provider arrangements.
 - d. Results of security operations activities and summaries of assurance reports.
 - e. Security breaches or violations and management's responses.
 - f. Recommendations for changes or updates to the information security program.
 5. Determine whether management responsibilities are appropriate and include the following:
 - a. Implementation of the information security program by clearly communicating responsibilities and holding appropriate individuals accountable for carrying out these responsibilities.
 - b. Establishment of appropriate policies, standards, and procedures to support the information security program.
 - c. Participation in assessing the effect of security threats or incidents on the institution and its business lines and processes.
 - d. Delineation of clear lines of responsibility and communication of accountability for information security.
 - e. Adherence to risk thresholds established by the board relating to information security threats or incidents, including those relating to cybersecurity.
 - f. Oversight of risk mitigation activities that support the information security program.
 - g. Establishment of appropriate segregation of duties.
 - h. Coordination of both information and physical security.
 - i. Integration of security controls throughout the institution.
 - j. Protection of data consistently throughout the institution.
 - k. Definition of the information security responsibilities of third parties.
 - l. Facilitation of annual information security and awareness training and ongoing security-related communications to employees.
 6. Determine whether management has designated one or more individuals as an information security officer and determine appropriateness of the reporting line.
 7. Determine whether security officers and employees know, understand, and are accountable for fulfilling their security responsibilities.

8. Determine the adequacy of audit coverage and reporting of the information security program by reviewing appropriate audit reports and board or audit committee minutes. (For further questions, refer to the *IT Handbook's* "Audit" booklet examination procedures.)⁶³
9. Determine whether the board provides adequate funding to develop and implement a successful information security function. Review whether the institution has the following:
 - a. Appropriate staff with the necessary skills to meet the institution's technical and managerial needs.
 - b. Personnel with knowledge of technology standards, practices, and risk methodologies.
 - c. Training to prepare staff for their short- and long-term security responsibilities.
 - d. Oversight of third parties when they supplement an institution's technical and managerial capabilities.
10. Determine whether management has adequately incorporated information security into its overall ITRM process. (For further questions, refer to the *IT Handbook's* "Management" booklet examination procedures.)⁶⁴

Objective 3: Determine whether management of the information security program is appropriate and supports the institution's ITRM process, integrates with lines of business and support functions, and integrates third-party service provider activities with the information security program.

1. Determine whether the institution has an effective information security program that supports the ITRM process. Review whether the program includes the following:
 - a. Identification of threats and risks.
 - b. Measurement of risks.
 - c. Implementation of risk mitigation.
 - d. Monitoring and reporting of risks.
 - e. Methods to assess the program's effectiveness.
2. Determine whether management appropriately integrates the information security program across the institution's lines of business and support functions. Review whether management has the following:
 - a. Security policies, standards, and procedures that are designed to support and to align with the policies in the lines of business.
 - b. Incident response programs that include all affected lines of business and support units.
 - c. Common awareness and enforcement mechanisms between lines of business and information security.
 - d. Visibility to assess the likelihood of threats and potential damage to the institution.
 - e. The ability to identify and implement controls over the root causes of an incident.

⁶³ See the *IT Handbook's* "Audit" booklet examination procedures.

⁶⁴ See the *IT Handbook's* "Management" booklet examination procedures.

3. If the institution outsources activities to a third-party service provider, determine whether management integrates those activities with the information security program. Verify that the third-party management program evidences expectations that align with the institution's information security program.

Objective 4: As part of the information security program, determine whether management has established risk identification processes.

1. Determine whether management effectively identifies threats and vulnerabilities continuously.
2. Determine whether the risk identification process produces manageable groupings of information security threats, including cybersecurity threats. Review whether management has the following:
 - a. A threat assessment to help focus the risk identification efforts.
 - b. A method or taxonomy for categorizing threats, sources, and vulnerabilities.
 - c. A process to determine the institution's information security risk profile.
 - d. A validation of the risk identification process through audits, self-assessments, penetration tests, and vulnerability assessments.
 - e. A validation through audits, self-assessments, penetration tests, and vulnerability assessments that risk decisions are informed by appropriate identification and analysis of threats and other potential causes of loss.
3. Determine whether management has a means to collect data on potential threats to identify information security risks. Determine whether management uses threat modeling (e.g., development of attack trees) to assist in identifying and quantifying risk and in better understanding the nature, frequency, and sophistication of threats.
4. Determine whether management has continuous, established routines to identify and assess vulnerabilities. Determine whether management has processes to receive vulnerability information disclosed by external individuals or groups, such as security or vulnerability researchers.
5. Determine whether management adjusts the information security program for institutional changes and changes in legislation, regulation, regulatory policy, guidance, and industry practices. Review whether management has processes to do the following:
 - a. Maintain awareness of new legal and regulatory requirements or changes to industry practices.
 - b. Update the information security program to reflect changes.
 - c. Report changes of the information security program to the board.

Objective 5: Determine whether management measures the risk to guide its recommendations for and use of mitigating controls.

1. Determine whether management uses tools to perform threat analysis and analyzes information security events to help do the following:
 - a. Map threats and vulnerabilities.
 - b. Incorporate legal and regulatory requirements.
 - c. Improve consistency in risk measurement.
 - d. Highlight potential areas for mitigation.
 - e. Allow comparisons among different threats, events, and potential mitigating controls.

Objective 6: Determine whether management effectively implements controls to mitigate identified risk.

1. Determine whether policies, standards, and procedures are of sufficient scope and depth to guide information security-related decisions. Review whether policies, standards, and procedures have the following characteristics:
 - a. Are appropriately implemented and enforced.
 - b. Delineate areas of responsibility.
 - c. Are communicated in a clear and understandable manner.
 - d. Are reviewed and agreed to by employees.
 - e. Are appropriately flexible to address changes in the environment.
2. Determine whether the information security policy is annually reviewed and approved by the board.
3. Determine whether the institution continually assesses the capability of technology needed to sustain an appropriate level of information security based on the size, complexity, and risk appetite of the institution.
4. Determine whether management implements an integrated control system characterized by the use of different control types that mitigates identified risks. Review whether management does the following:
 - a. Implements a layered control system using different controls at different points in a transaction process.
 - b. Uses controls of different classifications, including preventive, detective, and corrective.
 - c. Verifies that compensating controls are used appropriately to compensate for weaknesses with the system or process.
5. Determine whether management implements controls that appropriately align security with the nature of the institution's operations and strategic direction. Specifically, review whether management does the following:

- a. Implements controls based on the institution's risk assessment to mitigate risk from information security threats and vulnerabilities, such as interconnectivity risk.
 - b. Evaluates whether the institution has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls.
 - c. Reviews and improves or updates the security controls, where necessary.
6. Determine whether management effectively maintains an inventory(ies) of hardware, software, information, and connections. Review whether management does the following:
 - a. Identifies assets that require protection, such as those that store, transmit, or process sensitive customer information, or trade secrets.
 - b. Classifies assets appropriately.
 - c. Uses the classification to determine the sensitivity and criticality of assets.
 - d. Uses the classification to implement controls required to safeguard the institution's assets.
 - e. Updates the inventory(ies) appropriately.
7. Determine whether management comprehensively and effectively identifies, measures, mitigates, monitors, and reports interconnectivity risk. Review whether management does the following:
 - a. Identifies connections with third parties.
 - b. Identifies access points and connection types that pose risk.
 - c. Identifies connections between and access across low-risk and high-risk systems.
 - d. Measures the risk associated with connections with third parties with remote access.
 - e. Implements and assesses the adequacy of appropriate controls to ensure the security of connections.
 - f. Monitors and reports on the institution's interconnectivity risk.
8. Determine whether management effectively mitigates risks posed by users. Review whether management does the following:
 - a. Develops and maintains a culture that fosters responsible and controlled access for users.
 - b. Establishes and effectively administers appropriate security screening in IT hiring practices.
 - c. Establishes and appropriately administers a user access program for physical and logical access.
 - d. Employs appropriate segregation of duties.
 - e. Obtains agreements from employees, contractors, and service providers covering confidentiality, nondisclosure, and authorized use.
 - f. Provides training to support awareness and policy compliance.
9. Determine whether management applies appropriate physical security controls to protect its premises and more sensitive areas, such as its data center(s).

10. Determine whether management secures access to its computer networks through multiple layers of access controls. Review whether management does the following:
 - a. Establishes zones (e.g., trusted and untrusted) according to risk with appropriate access requirements within and between each zone.
 - b. Maintains accurate network diagrams and data flow charts.
 - c. Implements appropriate controls over wired and wireless networks.
11. Determine whether management has a process to introduce changes to the environment (e.g., configuration management of IT systems and applications, hardening of systems and applications, use of standard builds, and patch management) in a controlled manner. Determine whether management does the following:
 - a. Maintains procedures to guide the process of introducing changes to the environment.
 - b. Defines change requirements.
 - c. Restricts changes to authorized users.
 - d. Reviews the potential impact changes have on security controls.
 - e. Identifies all system components affected by the changes.
 - f. Develops test scripts and implementation plans.
 - g. Performs necessary tests of all changes to the environment (e.g., systems testing, integration testing, functional testing, user acceptance testing, and security testing).
 - h. Defines rollback procedures in the event of unintended or negative consequences with the introduced changes.
 - i. Verifies the application or system owner has authorized changes in advance.
 - j. Maintains strict version control of all software updates.
 - k. Validates that new hardware complies with institution policies and guidelines.
 - l. Verifies network devices are properly configured and function appropriately within the environment
 - m. Maintains an audit trail of all changes.
12. Determine whether appropriate processes exist for configuration management (managing and controlling configurations of systems, applications, and other technology).
13. Determine whether management has processes to harden applications and systems (e.g., installing minimum services, installing necessary patches, configuring appropriate security settings, enforcing principle of least privilege, changing default passwords, and enabling logging).
14. Determine whether management uses standard builds, allowing one documented configuration to be applied to multiple computers in a controlled manner, to create hardware and software inventories, update or patch systems, restore systems, investigate anomalies, and audit configurations.
15. Determine whether management has a process to update and patch operating systems, network devices, and software applications, including internally developed software provided

to customers, for newly discovered vulnerabilities. Review whether patch management processes include the following:

- a. An effective monitoring process that identifies the availability of software patches.
- b. A process to evaluate the patches against the threat and network environment.
- c. A prioritization process to determine which patches to apply across classes of computers and applications.
- d. A process for obtaining, testing, and securely installing the patches.
- e. An exception process, with appropriate documentation, for patches that an institution decides to delay or not apply.
- f. A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment.
- g. A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied.
- h. Actions to ensure that patches do not compromise the security of the institution's systems.

16. Determine whether management plans for the life cycles of the institution's systems, eventual end of life, and any corresponding business impacts. Review whether the institution's life cycle management includes the following:

- a. Maintaining inventories of systems and applications.
- b. Adhering to an approved end-of-life or sunset policy for older systems.
- c. Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor.
- d. Planning for the update or replacement of systems nearing obsolescence.
- e. Outlining procedures for the secure destruction or wiping of hard drives being returned to vendors or donated to prevent the inadvertent disclosure of sensitive information.

17. Determine whether management has implemented defense-in-depth to protect, detect, and respond to malware.

18. Determine whether management maintains policies and effectively controls and protects access to and transmission of information to avoid loss or damage. Review whether management does the following:

- a. Requires secure storage of all types of sensitive information, whether on computer systems, portable devices, physical media, or hard-copy documents.
- b. Establishes controls to limit access to data.
- c. Requires appropriate controls over data stored in a cloud environment.
- d. Implements appropriate controls over the electronic transmission of information or, if appropriate safeguards are unavailable, restricts the type of information that can be transmitted.
- e. Has appropriate disposal procedures for both paper-based and electronic information.

- f. Maintains the security of physical media, including backup tapes, containing sensitive information while in transit, including to off-site storage, or when shared with third parties.
 - g. Has policies restricting the use of unsanctioned or unapproved IT resources (e.g., online storage services, unapproved mobile device applications, and unapproved devices).
- 19. Determine whether management identifies factors that may increase risk from supply chain attacks and responds with appropriate risk mitigation. Review whether management implements the following as appropriate:
 - a. Purchases are made only through reputable sellers.
 - b. Purchases are made through a third party to shield the institution's identity.
 - c. Hardware is reviewed for anomalies.
 - d. Software is reviewed through both automated software testing and code reviews.
 - e. Reliability of the items purchased is regularly reviewed post-implementation.
- 20. Determine whether management has an effective process to administer logical security access rights for the network, operating systems, applications, databases, and network devices. Review whether management has the following:
 - a. An enrollment process to add new users to the system.
 - b. An authorization process to add, delete, or modify authorized user access to operating systems, applications, directories, files, and specific types of information.
 - c. A monitoring process to oversee and manage the access rights granted to each user on the system.
 - d. A process to control privileged access.
 - e. A process to change or disable default user accounts and passwords.
- 21. As part of management's process to secure the operating system and all system components, determine whether management does the following:
 - a. Limits the number of employees with access to operating system and system utilities and grants only the minimum level of access required to perform job responsibilities.
 - b. Restricts and logs access to and activity on operating system parameters, system utilities (especially those with data-altering capabilities), and sensitive system resources (including files, programs, and processes), and supplements with additional security software, as necessary.
 - c. Restricts operating system access to specific terminals in physically secure and monitored locations.
 - d. Secures or removes external drives and portable media from system consoles, terminals, or PCs running terminal emulations, residing outside of physically secure locations.
 - e. Prohibits remote access to operating system and system utilities, where feasible, and, at a minimum, requires strong authentication and encrypted sessions before allowing such remote access.
 - f. Filters and reviews logs for potential security events and provides adequate reports and alerts.

- g. Independently monitors operating system access by user, terminal, date, and time of access.
22. Determine whether management controls access to applications. Review whether management does the following:
- a. Implements a robust authentication method consistent with the criticality and sensitivity of the application.
 - b. Manages application access rights by using group profiles.
 - c. Periodically reviews and approves the application access assigned to users for appropriateness.
 - d. Communicates and enforces the responsibilities of programmers, security administrators, and application owners in maintaining effective application access control.
 - e. Sets time-of-day or terminal limitations for some applications or for more sensitive functions within an application.
 - f. Logs access and events, defines alerts for significant events, and develops processes to monitor and respond to anomalies and alerts.
23. Determine whether management has policies and procedures to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner. Review whether management does the following:
- a. Provides remote access in a safe and sound manner.
 - b. Implements the controls necessary to offer remote access securely (e.g., disables unnecessary remote access, obtains approvals for and performs audits of remote access, maintains robust configurations, enables logging and monitoring, secures devices, restricts remote access during specific times, controls applications, enables strong authentication, and uses encryption).
24. Determine whether management effectively controls employees' use of remote devices. Review whether management does the following:
- a. Implements controls over institution owned and personally owned devices used by employees to access the network (e.g., disallows remote access without business justification, requires management approval, reviews remote access approvals, restricts access to authorized network areas, logs remote access, implements robust authentication, uses encryption, and uses application white-listing).
 - b. Implements controls over remote devices provided by the institution (e.g., securely configures remote access devices, protects devices against malware, patches and updates software, encrypts sensitive data, implements secure containers, audits device access, uses remote disable and wipe capabilities, and uses geolocation).
 - c. Uses an effective method to ensure personally owned devices meet defined institution security standards (e.g., such as operating system version, patch levels, and anti-malware solutions).

25. Determine whether management effectively provides secure customer access to financial services and plans for potential interruptions in service. Review whether management does the following:
- a. Develops and maintains policies and procedures to securely offer and ensure the resilience of remote financial services (e.g., using appropriate authentication, layered security controls, and fraud detection monitoring). (For additional questions, refer to the “Mobile Financial Services” examination procedures.)⁶⁵
 - b. Plans and coordinates with ISPs and third parties to minimize exposure to incidents and continue services when faced with an incident (e.g., monitors threat alerts, service availability, applications, and network traffic for indicators of nefarious activity, and ensures traffic filtering).
 - c. Develops and tests a response plan in conjunction with the institution’s ISPs and third-party service providers to mitigate the interruption of mobile or remote financial services.
26. Determine whether management develops customer awareness and education efforts that address both retail (consumer) and commercial account holders.
27. Determine whether management uses applications that were developed by following secure development practices and that meet a prudent level of security. Determine whether management develops security control requirements for applications, whether they are developed in-house or externally. Determine whether information security personnel are involved in monitoring the application development process to verify secure development practices. Review whether applications in use provide the following capabilities:
- a. Provide a prudent level of security (e.g., password and audit policies), audit trails of security and access changes, and user activity logs.
 - b. Have user and group profiles to manage user access for applications if they are not part of a centralized identity access management system.
 - c. Provide the ability to change and disable default application accounts upon installation.
 - d. Allow administrators to review and install patches for applications in a timely manner.
 - e. Use validation controls for data entry and data processing.
 - f. Integrate additional authentication and encryption controls, as necessary.
 - g. Protect web or Internet-facing applications through additional controls, including web application firewalls, regular scanning for new or recurring vulnerabilities, mitigation or remediation of common security weaknesses, and network segregation.
28. With respect to developed software, determine whether institution management does the following:
- a. Reviews mitigation of potential flaws in applications.
 - b. Obtains attestation or evidence from third-party developers that the applications acquired by the institution meet the necessary security requirements and that noted vulnerabilities or flaws are remediated in a timely manner.

⁶⁵ Refer to [appendix E](#) of the *IT Handbook*’s “Retail Payment Systems” booklet.

- c. Performs ongoing risk assessments to consider the adequacy of application-level controls in light of changing threat, network, and host environments.
 - d. Implements minimum controls recommended by third-party service providers and considers supplemental controls as appropriate.
 - e. Reviews available audit reports, and considers and implements appropriate control recommendations.
 - f. Collects data to build metrics and reporting of configuration management compliance, and vulnerability management.
29. For database security, determine whether management implemented or enabled controls commensurate with the sensitivity of the data stored in or accessed by the database(s). Determine whether management appropriately restricts access and applies the rule of least privilege in assigning authorizations.
30. Determine how and where management uses encryption and if the type and strength are sufficient to protect information appropriately. Additionally, determine whether management has effective controls over encryption key management.
31. Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. Review the due diligence involved, security controls to mitigate risk, and monitoring capabilities over the institution's third parties. Review the institution's policies, standards, and procedures related to the use of the following:
- a. Third-party service providers that facilitate operational activities (e.g., core processing, mobile financial services, cloud storage and computing, and managed security services).
 - b. Due diligence in research and selection of third-party service providers.
 - c. Contractual assurances from third-party service providers for security responsibilities, controls, and reporting.
 - d. Nondisclosure agreements with third-party service providers with access to the institution's systems and data (including before, during, and following termination of the contract).
 - e. Independent review of the third-party service provider's security through appropriate reports from audits and tests.
 - f. Coordination of incident response policies and contractual notification requirements.
 - g. Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported.
32. If the institution outsources cloud computing or storage to a third-party service provider, refer to the FFIEC's "Outsourced Cloud Computing" statement.⁶⁶

⁶⁶ See the FFIEC's "[Outsourced Cloud Computing](#)" statement.

33. If the institution outsources the management of security services to a third-party service provider, refer to the information available in appendix D of the *IT Handbook's* "Outsourcing Technology Services" booklet and the related examination procedures.⁶⁷
34. Determine whether management effectively manages the following information security considerations related to business continuity planning. Review management's ability to do the following:
 - a. Identify personnel with key information security roles during a disaster and training of personnel in those roles.
 - b. Define information security needs for backup sites and alternate communication networks.
 - c. Develop policies that address the concepts of information security incident response and resilience and test information security incident scenarios.
35. Determine whether management has an effective log management process that involves a central logging repository, timely transmission of log files, and effective log analysis. Review whether management has the following:
 - a. Log retention policies that meet incident response and analysis needs.
 - b. Processes for the security and integrity of log files (e.g., encryption of log files, adequate storage capacity, secure backup and disposal of logs, logging to a separate computer, use of read-only media, controlled log parameters, and restricted access to log files).
 - c. Independent review of logging practices.
 - d. Processes to effectively collect, aggregate, analyze, and correlate security event information from discrete systems and applications.

Objective 7: Determine whether management has effective risk monitoring and reporting processes.

1. Determine whether the institution has risk monitoring and reporting processes that address changing threat conditions in both the institution and the greater financial industry. Determine whether these processes address information security events faced by the institution, the effectiveness of management's response, and the institution's resilience to those events. Review whether the reporting process includes a method of disseminating those reports to appropriate members of management.
2. Determine whether the risk monitoring and reporting process is regular and prompts action, when necessary, in a timely manner.
3. Determine whether program monitoring and reporting instigate appropriate changes that are effective in maintaining an acceptable level of risk.

⁶⁷ Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for the [MSSP Examination Procedures](#).

4. Determine whether management develops and effectively uses metrics as part of the risk monitoring and reporting processes for the information security program. Review whether management does the following:
 - a. Uses metrics that are timely, comprehensive, and actionable to improve the program's effectiveness and efficiency.
 - b. Develops metrics that demonstrate the extent to which the information security program is implemented and whether the program is effective.
 - c. Uses metrics to measure security policy implementation, the adequacy of security services delivery, and the impact of security events on business processes.
 - d. Establishes metrics to measure conformance to the standards and procedures that are used to implement policies.
 - e. Uses metrics to quantify and report risks in the information security program.

Objective 8: *Determine whether management has security operations that encompass necessary security-related functions, are guided by defined processes, are integrated with lines of business and activities outsourced to third-party service providers, and have adequate resources (e.g., staff and technology).*

1. Determine whether the institution's security operations activities include the following:
 - a. Security software and device management (e.g., maintaining the signatures on signature-based devices and firewall rules).
 - b. Forensics (e.g., analysis of potentially compromised systems).
 - c. Vulnerability identification (e.g., operation or supervision of vulnerability scans, self-assessments, penetration tests, and analysis of audit results).
 - d. Vulnerability cataloging and remediation tracking.
 - e. Physical security management (e.g., CCTV, guards, and badge systems).
 - f. Law enforcement interface (e.g., data retention and lawful intercepts).
 - g. Third-party integration (e.g., managed security services and incident detection services).
 - h. Monitoring of network, host, and application activity.
 - i. Threat identification and assessment.
 - j. Incident detection and management.
 - k. Enforcement of access controls.
2. Determine whether management establishes defined processes and appropriate governance to facilitate the performance of security operations. Determine whether management coordinates security operations activities with the institution's lines of business and with the institution's third-party service providers.
3. Determine whether management has effective threat identification and assessment processes, including the following:
 - a. Maintaining procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information.

- b. Identifying and assessing threats (e.g., threat information is often ad hoc, although some providers present threat information within a defined framework that readily lends itself to analytical operations).
 - c. Using tools to assist in the analysis of vulnerabilities (e.g., design of system, operation of the system, security procedures, business line controls, and implementation of the system and controls).
 - d. Using threat knowledge to drive risk assessment and response.
 - e. Designing policies to allow immediate and consequential threats to be dealt with expeditiously.
 - f. Developing appropriate processes to evaluate and respond to vulnerability information from external groups or individuals.
4. Determine whether management has effective threat monitoring processes, including the following:
- a. Defining threat monitoring policies that provide for both continual and ad hoc monitoring of communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal proceedings.
 - b. Establishing responsibility and accountability for security personnel and system administrators for monitoring.
 - c. Appropriately reviewing and providing approval of the monitoring tools used.
 - d. Monitoring of indicators, including vulnerabilities, attacks, compromised systems, and suspicious users.
 - e. Monitoring both incoming and outgoing network traffic to identify malicious activity and data exfiltration.
 - f. Establishing and documenting a process to independently monitor administrators and other users with higher privileges.
5. Determine whether management has effective incident identification and assessment processes to do the following:
- a. Identify indicators of compromise.
 - b. Analyze the event associated with the indicators.
 - c. Classify the event.
 - d. Enable the use of response teams and responses depending on the type of event.
 - e. Escalate the event consistent with the classification.
 - f. Report internally and externally as appropriate.
 - g. Identify personnel empowered to declare an incident.
 - h. Develop procedures to test the incident escalation, response, and reporting processes.
6. Determine whether management has effective incident response processes, including the following:
- a. Protocols defined in the incident response policy to declare and respond to an incident once identified.

- b. Procedures to minimize damage through the containment of the incident, restoration of systems, preservation of data and evidence, and notification, as appropriate, to customers and others as needed.
- c. Appropriate balance of adequate people and technologies in the response.
- d. A plan that is comprehensive, coordinated, integrated, and periodically tested with appropriate internal and external parties.
- e. Policies and procedures to guide the response, assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort.
- f. Thresholds for reporting significant security incidents and processes to notify, as appropriate, the institution's regulators of those incidents that may affect the institution or the financial system.
- g. Assignment of responsibilities, training, and testing.
- h. Containment strategies.
- i. Restoration and follow-up strategies.

Objective 9: *Determine whether management has an effective information security program.*

1. Determine whether the information security program is subject to periodic review and whether management provides for continual improvement in the program's effectiveness. Verify whether that review does the following:
 - a. Addresses the program in its current environment.
 - b. Demonstrates that lessons learned from experience, audit findings, and other opportunities for improvement are identified and applied.

Objective 10: *Determine whether assurance activities provide sufficient confidence that the security program is operating as expected and reaching intended goals.*

1. Review whether management ascertains assurance through the following:
 - a. Testing and evaluations through a combination of self-assessments, penetration tests, vulnerability assessments, and audits with appropriate coverage, depth, and independence.
 - b. Alignment of personnel skills and program needs.
 - c. Reporting that is timely, complete, transparent, and relevant to management decisions.
2. Determine whether management considers the following key testing factors when developing and implementing independent tests:
 - a. Scope.
 - b. Personnel.
 - c. Notifications.
 - d. Confidentiality, integrity, and availability of the institution's information.
 - e. Confidentiality of test plans and data.
 - f. Frequency.

- g. Proxy testing.
3. Determine whether management uses the following types of tests and evaluations to determine the effectiveness of the information security program. Verify whether management ensures the following are done:
 - a. Periodic self-assessments performed by the organizational unit being assessed.
 - b. Penetration tests that subject a system to real-world attacks and identify weaknesses.
 - c. Vulnerability assessments that define, identify, and classify the security holes found in the system.
 - d. Audits performed by independent internal departments or third parties.
 4. Determine whether management uses independent organizations to test aspects of its information security programs.
 5. Determine whether management uses reporting of the results of self-assessments, penetration tests, vulnerability assessments, and audits to support management decision making.
 6. Determine whether the annual information security report is timely and contains adequate information.

Objective 11: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the examiner-in-charge regarding the following:
 - a. Violations of laws or regulations.
 - b. Significant issues warranting inclusion as matters requiring attention or recommendations in the report of examination.
 - c. The proposed Uniform Rating System for Information Technology management component rating and the potential impact of the conclusion on the composite or other component IT ratings.
 - d. Potential impact of conclusions on the institution's risk assessment.
2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.
3. Document conclusions in a memo to the examiner-in-charge that provides report-ready comments for all relevant sections of the report of examination and guidance to future examiners.
4. Organize work papers to ensure clear support for significant findings by examination objective.

Appendix B: Glossary

Acceptable use policy: A document that establishes an agreement between users and the enterprise and defines for all parties the ranges of use that are approved before users can gain access to a network or the Internet.

Access: The ability to physically or logically enter or make use of an IT system or area (secured or unsecured). The process of interacting with a system.

Administrator privileges: Computer system access to resources that are unavailable to most users. Administrator privileges permit execution of actions that would otherwise be restricted.

Air-gapped environment: Security measure that isolates a secure network from unsecure networks physically, electrically, and electromagnetically.

Anomalous activity: Activity that deviates from normal. The result of the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.

Antivirus/anti-malware software: A program that monitors a computer or network to identify all types of malware and prevent or contain malware incidents.

Asset: In computer security, a major application, a general-support system, a high-impact program, a physical plant, a mission-critical system, personnel, equipment, or a logically related group of systems.

Attack signature: A specific sequence of events indicative of an unauthorized access attempt.

Authentication: The process of verifying the identity of an individual user, machine, software component, or any other entity.

Availability: Whether or how often a system is available for use by its intended users. Because downtime is usually costly, availability is an integral component of security.

Baseline configuration: A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time and that can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, or changes.

Black holing: A method typically used by ISPs to stop a distributed denial-of-service (DDoS) attack on one of its customers. This approach to blocking DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic.

Border router: A device located at the organization's boundary to an external network.

Change management: The broad processes for managing organizational change. Change management encompasses planning, oversight or governance, project management, testing, and implementation.

Checksum: A mathematical value that is assigned to a file and used to “test” the file at a later date to verify that the data contained in the file has not been maliciously or erroneously changed.

Classification: Categorization (e.g., “confidential,” “sensitive,” or “public”) of the information processed by the service provider on behalf of the receiver company.

Cloud computing: Generally a migration from owned resources to shared resources in which client users receive IT services on demand from third-party service providers via the Internet “cloud.” In cloud environments, a client or customer relocates its resources—such as data, applications, and services—to computing facilities outside the corporate firewall, which the end user then accesses via the Internet.

Cloud storage: A model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.

Compensating control: A management, operational, and/or technical control (e.g., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

Computer security: Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

Confidentiality: Assuring information will be kept secret, with access limited to appropriate persons.

Configuration management: The management of security features and assurances through control of changes made to a system’s hardware, software, firmware, documentation, testing, test fixtures, and test documentation throughout the development and operational life of the system.

Consumer information: For purposes of the Information Security Standards, “consumer information” means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report that is maintained by or on behalf of a financial institution for a business purpose, such as information that an institution obtains about a loan applicant or a prospective employee from a consumer report.

Control: The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature.

Control requirements: Process used to document and/or track internal processes to determine that those established procedures and/or physical security policies are being followed.

Control self-assessment: A technique used to internally assess the effectiveness of risk management and control processes.

Corrective control: A mitigating technique designed to lessen the impact to the institution when adverse events occur.

Crisis management: The process of managing an institution's operations in response to an emergency or event that threatens business continuity. An institution's ability to communicate with employees, customers, and the media, using various communications devices and methods, is a key component of crisis management.

Critical system (infrastructure): The systems and assets, whether physical or virtual, that are so vital that the incapacity or destruction of them may have a debilitating impact.

Customer: For purposes of the Information Security Standards, "customer" means a consumer with whom a financial institution has a continuing relationship under which the institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes. In the case of a credit union, a customer relationship will exist between a credit union and certain consumers that are not the credit union's members.

Customer information: A term used in the Information Security Standards to mean any record containing non-public personal information about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of a financial institution.

Customer information systems: For purposes of the Information Security Standards, "customer information systems" means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

Cyber attack: An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an institution for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; destroying the integrity of the data; or stealing controlled information.

Cyber event: A cybersecurity change or occurrence that may have an impact on organizational operations (including mission or capabilities).

Cyber incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

Cyber resilience: The ability of a system or domain to withstand cyber attacks or failures and, in such events, to reestablish itself quickly.

Cyber threat: An internal or external circumstance, event, action, occurrence, or person with the potential to exploit technology-based vulnerabilities and to adversely affect (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Cybersecurity: The process of protecting consumer and bank information by preventing, detecting, and responding to attacks.

Data classification program: A program that categorizes data to convey required safeguards for information confidentiality, integrity, and availability, and establishes required controls based on value and level of sensitivity.

Data corruption: Errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data.

Data integrity: The property that data have not been destroyed or corrupted in an unauthorized manner; maintaining and assuring the accuracy and consistency of data over their entire life cycle.

Data loss prevention (DLP) program: A comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data while it is stored, used, or in transit over the network and at the perimeter.

Database: A collection of data that is stored on any type of computer storage medium and may be used for more than one purpose.

Defense-in-depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

Demilitarized zone (DMZ): A computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

Detection device: A device designed to recognize an event and alert management when events occur.

Detective control: A mitigating technique designed to recognize an event and alert management when events occur.

Device: A generic term for any machine or component that attaches to a computer or connects to a network.

Distributed denial of service (DDoS) attack: A type of attack that makes a computer resource or resources unavailable to its intended users. Although the means to carry out, motives for, and

targets of a DDoS attack may vary, it generally consists of the concerted efforts of a group that intends to affect an institution by preventing an Internet site, service, or application from functioning efficiently.

Due diligence for service provider selection: Technical, functional, and financial review to verify a third-party service provider's ability to deliver the requirements specified in its proposal. The intent is to verify that the service provider has a well-developed plan and adequate resources and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

End-of-life: All software products have life cycles. End-of-life refers to the date when a software development company no longer provides automatic fixes, updates, or online technical assistance for the product.

End-point security: Refers to a methodology of protecting the corporate network when accessed with remote devices, such as laptops, or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry (or exit) point for security threats.

End-to-end process flow: Document that details the flow of the processes, considering automated and manual control points, hardware, databases, network protocols, and real-time versus periodic processing characteristics.

Enterprise-wide: Across an entire organization, rather than a single business department or function.

Exploit: A technique or code that uses a vulnerability to provide system access to the attacker. An exploit is an intentional attack to affect an operating system or application program.

External connections: An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

File transfer protocol (FTP): A standard high-level protocol for transferring files from one computer to another, usually implemented as an application-level program.

Financial Services Information Sharing and Analysis Center (FS-ISAC): A nonprofit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information.

Firewall: A hardware or software link in a network that relays only data packets clearly intended and authorized to reach the other side.

Frame relay: A high-performance wide area network protocol that operates at the physical and data link layers of the Open Systems Interconnection reference model. Frame relay is an example

of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth.

Governance: In computer security, governance means setting clear expectations for the conduct (behaviors and actions) of the entity being governed and directing, controlling, and strongly influencing the entity to achieve these expectations. Governance includes specifying a framework for decision making, with assigned decision rights and accountability, intended to consistently produce desired behaviors and actions.

Gramm–Leach–Bliley Act: The act, also known as the Financial Services Modernization Act of 1999 (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999), required the federal banking agencies to establish information security standards for financial institutions.

Hardening: The process of securing a computer’s administrative functions or inactivating those features not needed for the computer’s intended business purpose.

Hardware: The physical elements of a computer system; the computer equipment as opposed to the programs or information stored in a machine.

Hash: A fixed-length cryptographic output of variables, such as a message, being operated on by a formula or cryptographic algorithm.

Hijacking: An attacker’s use of an authenticated user’s communication session to communicate with system components.

Homing beacons: Devices that send messages to the institution when they connect to a network and that enable recovery of the device.

Host: A computer that is accessed by a user from a remote location.

Incident management: The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible.

Incident response plan: A plan that defines the action steps, involved resources, and communication strategy upon identification of a threat or potential threat event, such as a breach in security protocol, power or telecommunications outage, severe weather, or workplace violence.

Information security: The process by which an organization protects the creation, collection, storage, use, transmission, and disposal of information.

Information systems: Electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information systems can include networks (computer systems, connections to business partners and the Internet, and the

interconnections between internal and external systems). Other examples are backup tapes, mobile devices, and other media.

Information technology (IT): Any services or equipment, or interconnected system(s) or subsystem(s) of equipment that compose the institution's IT architecture or infrastructure. IT can include computers; ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance); peripheral equipment designed to be controlled by the central processing unit of a computer; software; firmware and similar procedures; services (including cloud computing and help-desk services or other professional services that support any point of the life cycle of the equipment or service); and related resources.

Infrastructure: Describes what has been implemented by IT architecture and often includes support facilities such as power, cooling, ventilation, server and data redundancy and resilience, and telecommunications lines. Specific architecture types may exist for the following: enterprise, data (information), technology, security, and application.

Integrity: Assurance that information is trustworthy and accurate; ensuring that information will not be accidentally or maliciously altered or destroyed (see "Data integrity").

Interconnectivity: The state or quality of being connected together. The interaction of a financial institution's internal and external systems and applications and the entities with which they are linked.

Interdependencies: When two or more departments, processes, functions, or third-party service providers support one another in some fashion.

Internal "trusted" zone: A channel in which the end points are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include SSLIP security and a secure physical connection.

International Organization for Standardization (ISO): An independent, non-governmental, international organization that brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards.

Internet: The global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide.

Internet service provider (ISP): A company that provides its customers with access to the Internet (e.g., AT&T, Verizon, and CenturyLink).

Intrusion detection: Techniques that attempt to detect unauthorized entry or access into a computer or network by observation of actions, security logs, or audit data; detection of break-ins or attempts, either manually or via software expert systems that operate on logs or other information available on the network.

Intrusion detection system (IDS): Software or hardware product that detects and logs inappropriate, incorrect, or anomalous activity. It gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations). IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

Intrusion prevention system (IPS): A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its target.

IT system inventory: A list containing information about the information resources owned or operated by an organization.

Life-cycle process: The multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system.

Log: A record of information or events in an organized system, usually sequenced in the order in which the events occurred.

Logical access: Ability to interact with computer resources granted using identification, authentication, and authorization.

Logical access controls: The policies, procedures, organizational structure, and electronic access controls designed to restrict access to computer software and data files.

Malware: Software designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs.

Media: Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks.

Metric: A quantitative measurement.

Middleware: Software that connects two or more software components or applications. It is another term for an application programmer interface or API, and it allows programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services.

Mobile device: A portable computing and communications device with information-storage capability. Examples include notebook and laptop computers, cellular telephones and smart phones, tablets, digital cameras, and audio recording devices.

Multi-factor authentication: The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number); something you have (e.g., cryptographic identification device or token); and something you are (e.g., biometric).

National Institute of Standards and Technology (NIST): An agency of the U.S. Department of Commerce that works to develop and apply technology, measurements, and standards. NIST developed a voluntary cybersecurity framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructures.

Network: Two or more computer systems grouped together to share information, software, and hardware.

Network activity baseline: A base for determining typical utilization patterns so that significant deviations can be detected.

Network administrator: The individual responsible for the installation, management, and control of a network.

Network diagram: A description of any kind of locality in terms of its physical layout. In the context of communication networks, a topology describes pictorially the configuration or arrangement of a network, including its nodes and connecting communication lines.

Network security: The protection of computer networks and their services from unauthorized entry, modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and that there are no harmful side effects. Network security includes providing for data integrity.

Non-public personal information: For purposes of the Information Security Standards, non-public personal information means (i) “personally identifiable financial information”; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any “personally identifiable financial information” that is not publicly available.

Non-repudiation: Ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Operating system: A system that supports and manages software applications. Operating systems allocate system resources, provide access and security controls, maintain file systems, and manage communications between end users and hardware devices.

Out-of-band: Activity outside of the primary means of interfacing with the customer. For example, if a user is performing activity online, he or she may be authenticated through a one-time password sent via text message.

Outsourcing: The practice of contracting with another entity to perform services that might otherwise be conducted in-house; a contractual relationship with a third party to provide services, systems, or support.

Packet: The data unit that is routed from source to destination in a packet-switched network.

Patch: Software code that replaces or updates other code. Patches frequently are used to correct security flaws.

Penetration test: The process of using approved, qualified personnel to conduct real-world attacks against a system to identify and correct security weaknesses before they are discovered and exploited by others.

Personally identifiable financial information: For purposes of the Information Security Standards, personally identifiable financial information means information (i) a consumer provides to a financial institution to obtain a financial product or service; (ii) about a consumer resulting from any transaction involving a financial product or service between the financial institution and a consumer; or (iii) that a financial institution otherwise obtains about a consumer in connection with providing a financial product or service, such as account balance information, payment history, overdraft history, and credit or debit card purchase information; or the fact that an individual is one of the financial institution's customers.

Phishing: A digital form of social engineering that uses authentic-looking—but bogus—e-mail to request information from users or direct them to fake websites that request information.

Policy: A document that records a high-level principle or an agreed-upon course of action; overall intention and direction as formally expressed by management.

Port: Either an end point to a logical connection or a physical connection to a computer.

Positive pay: A technique that can reduce check fraud by requesting businesses to send electronic files of information to the financial institution on all checks the business has issued.

Preventive control: A mitigating technique designed to prevent an event from occurring.

Principle of least privilege: The security objective of granting users only the access needed to perform official duties.

Privilege: The level of trust with which a system object is imbued.

Privileged access: Individuals with the ability to override system or application controls.

Protocol: A format for transmitting data between devices.

Real-time network monitoring: Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.

Remote access: The ability to obtain access to a computer or network from a remote location.

Remote deletions: Use of a technology to remove data from a portable device without touching the device.

Removable media: Portable electronic storage media, such as magnetic, optical, and solid-state devices that can be inserted into and removed from a computing device and that are used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, pen drives, and similar storage devices.

Resource: Any enterprise asset that can help the organization achieve its objectives.

Retention requirement: Requirement established by a company or by regulation for the length of time and/or for the amount of information that should be retained.

Risk analysis: The process of identifying risks, determining their probability and impact, and identifying areas needing safeguards.

Risk assessment: A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.

Rogue wireless access: An unauthorized wireless node on a network.

Routing: The process of moving information from its source to the destination.

Sandbox: A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

Scenario analysis: The process of analyzing possible future events by considering alternative possible outcomes.

Secure shell: Network protocol that uses cryptography to secure communication, remote command line log-in, and remote command execution between two networked computers.

Secure Sockets Layer (SSL): A protocol that is used to transmit private documents through the Internet.

Security architecture: A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

Security audit: An independent review and examination of system records and activities to test for adequacy of system controls, ensure compliance with established policy and operational procedures, and recommend any indicated changes in control, policy, and procedures.

Security breach: A security event that results in unauthorized access of data, applications, services, networks, or devices by bypassing underlying security mechanisms.

Security event: An event that potentially compromises the confidentiality, integrity, availability, or accountability of an information system.

Security log: A record that contains log-in and logout activity and other security-related events and that is used to track security-related information on a computer system.

Security posture: The security status of an enterprise's networks, information, and systems based on information security and assurance resources (e.g., people, hardware, software, and policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

Security violation: An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information or system resources.

Sensitive customer information: A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log into or access the customer's account, such as user name and password or password and account number.

Server: A computer or other device that manages a network service. An example is a print server, which is a device that manages network printing.

Service level agreement (SLA): Formal documents between an institution and its third-party service provider that outline an institution's predetermined requirements for a service and establish incentives to meet, or penalties for failure to meet, the requirements. SLAs should specify and clarify performance expectations, establish accountability, and detail remedies or consequences if performance or service quality standards are not met.

Service provider: For purposes of the Information Security Standards, service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through its provision of services directly to a financial institution.

Shadow IT: A term used to describe IT systems or applications used inside institutions without explicit approval.

Sniffing: The passive interception of data transmissions.

Social engineering: A general term for trying to trick people into revealing confidential information or performing certain actions.

Spear phishing: An attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into the targeted network.

Spoofing: A form of masquerading in which a trusted IP address is used instead of the true IP address as a means of gaining access to a computer system.

SQL Injection Attack: An exploit of target software that constructs structured query language (SQL) statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended. SQL injection enables an attacker to talk directly to the database, thus bypassing the application completely. Successful injection can cause information disclosure as well as the ability to add or modify data in the database.

Stateful inspection: A firewall inspection technique that examines the claimed purpose of a communication for validity. For example, a communication claiming to respond to a request is compared to a table of outstanding requests.

System administration: The process of maintaining, configuring, and operating computer systems.

System resources: Capabilities that can be accessed by a user or program either on the user's machine or across the network. Capabilities can be services, such as file or print services, or devices, such as routers.

Third-party relationship: Any business arrangement between a financial institution and another entity, by contract or otherwise.

Third-party service provider: Any third party to whom a financial institution outsources activities that the institution itself is authorized to perform, including a technology service provider.

Threat intelligence: The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making.

Trojan horse: Malicious code hidden in software that has an apparently beneficial or harmless use.

Tunnel: The path that encapsulated packets follow in an Internet VPN.

U.S. Computer Emergency Readiness Team (US-CERT): US-CERT is part of the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center in the Office of Cybersecurity and Communications. US-CERT is a partnership between the Department of Homeland Security and the public and private sectors, established to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation.

User identification: The process, control, or information by which a user identifies himself or herself to the system as a valid user (as opposed to authentication).

Utility: A program used to configure or maintain systems, or to make changes to stored or transmitted data.

Virtual local area network (VLAN): Logical segmentation of a LAN into different broadcast domains.

Virtual machine: A software emulation of a physical computing environment.

Virtual private network (VPN): A computer network that uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Virus: Malicious code that replicates itself within a computer.

Vulnerability: A hardware, firmware, or software flaw that leaves an information system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to information or to disrupt critical processing.

Vulnerability assessment: Systematic examination of systems to identify, quantify, and prioritize the security deficiencies of the systems.

Worm: A self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network), possibly without any user intervention. This occurs primarily because of security vulnerabilities on the target computers.

Zero-day attack: An attack on a piece of software that has a vulnerability for which there is no known patch.

Appendix C: Laws, Regulations, and Guidance

Laws

- 12 USC 1861–1867, “Bank Service Company Act”
- 12 USC 1882, “Bank Protection Act”
- 15 USC 1681w, “Fair and Accurate Credit Transactions Act”
- 15 USC 6801 and 6805(b), “Gramm–Leach–Bliley Act”
- 18 USC 1030, “Fraud and Related Activity in Connection With Computers”

Consumer Financial Protection Bureau

Regulations

- 12 CFR 1005, “Electronic Fund Transfers (Regulation E)”
- 12 CFR 1016, “Privacy of Consumer Financial Information (Regulation P)”

Federal Deposit Insurance Corporation

Regulations

- 12 CFR 326, subpart A, “Minimum Security Procedures”
- 12 CFR 326, subpart B, “Procedures for Monitoring Bank Secrecy Act Compliance”
- 12 CFR 332, “Privacy of Consumer Financial Information”
- 12 CFR 353, “Suspicious Activity Reports”
- 12 CFR 364, appendix A, “Interagency Guidelines Establishing Standards for Safety and Soundness”
- 12 CFR 364, appendix B, “Interagency Guidelines Establishing Information Security Standards”

Guidance

- FIL-28-2015, “Cybersecurity Assessment Tool” (July 2, 2015)
- FIL-13-2015, “FFIEC Joint Statements on Destructive Malware and Compromised Credentials” (March 30, 2015)
- FIL-9-2015, “Business Continuity Planning Booklet Appendix J Update to FFIEC IT Examination Handbook Series” (February 23, 2015)
- FIL-49-2014, “Technology Alert GNU Bourne-Again Shell (Bash) Vulnerability” (September 29, 2014)
- FIL-16-2014, “Technology Alert OpenSSL Heartbleed Vulnerability” (April 11, 2014)
- FIL-11-2014, “Distributed Denial of Service (DDoS) Attacks” (April 2, 2014)
- FIL-10-2014, “ATM and Card Authorization Systems” (April 2, 2014)
- FIL-50-2011, “FFIEC Supplement to Authentication in an Internet Banking Environment” (June 29, 2011)

FIL-56-2010, “Guidance on Mitigating Risk Posed by Information Stored on Photocopiers, Fax Machines and Printers” (September 15, 2010)

FIL-6-2010, “Retail Payment Systems Booklet” (February 25, 2010)

FIL-30-2009, “Identity Theft Red Flags, Address Discrepancies, and Change of Address Regulations Frequently Asked Questions” (June 11, 2009)

FIL-105-2008, “Identity Theft Red Flags, Address Discrepancies, and Change of Address Regulations Examination Procedures” (October 16, 2008)

FIL-100-2007, “Identity Theft Red Flags—Interagency Final Regulation and Guidelines” (November 15, 2007)

FIL-32-2007, “FDIC’s Supervisory Policy on Identity Theft” (April 11, 2007)

FIL-77-2006, “Authentication in an Internet Banking Environment Frequently Asked Questions” (August 21, 2006)

FIL-103-2005, “FFIEC Guidance Authentication in an Internet Banking Environment” (October 12, 2005)

FIL-69-2005, “Guidance on the Security Risks of Voice Over Internet Protocol (VoIP)” (July 27, 2005)

FIL-66-2005, “Spyware—Guidance on Mitigating Risks From Spyware” (July 22, 2005)

FIL-64-2005, “Pharming”—Guidance on How Financial Institutions Can Protect Against Pharming Attacks” (July 18, 2005)

FIL-59-2005, “Identity Theft Study Supplement on ‘Account Hijacking Identity Theft’” (July 5, 2005)

FIL-27-2005, “Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice” (April 1, 2005)

FIL-7-2005, “Fair and Accurate Credit Transactions Act of 2003 Guidelines Requiring the Proper Disposal of Customer Information” (February 2, 2005)

FIL-132-2004, “Identity Theft Study on ‘Account Hijacking’ Identity Theft and Suggestions for Reducing Online Fraud” (December 14, 2004)

FIL-121-2004, “Computer Software Due Diligence—Guidance on Developing an Effective Software Evaluation Program to Assure Quality and Regulatory Compliance” (November 16, 2004)

FIL-114-2004, “Risk Management of Free and Open Source Software FFIEC Guidance” (October 21, 2004)

FIL-103-2004, “Interagency Informational Brochure on Internet ‘Phishing’ Scams” (September 13, 2004)

FIL-84-2004, “Guidance on Instant Messaging” (July 21, 2004)

FIL-62-2004, “Guidance on Developing an Effective Computer Virus Protection Program” (June 7, 2004)

FIL-27-2004, “Guidance on Safeguarding Customers Against E-Mail and Internet Related Fraud Schemes” (March 12, 2004)

FIL-63-2003, “Guidance on Identity Theft Response Programs” (August 13, 2003)

FIL-43-2003, “Guidance on Developing an Effective Software Patch Management Program” (May 29, 2003)

FIL-30-2003, “Federal Bank and Credit Union Regulatory Agencies Jointly Issue Guidance on the Risks Associated With Weblinking” (April 23, 2003)

FIL-8-2002, “Wireless Networks and Customer Access” (February 1, 2002)

FIL-69-2001, “Authentication in an Electronic Banking Environment” (August 24, 2001)

FIL-68-2001, “501(b) Examination Guidance” (August 24, 2001)
 FIL-39-2001, “Guidance on Identity Theft and Pretext Calling” (May 9, 2001)
 FIL-22-2001, “Security Standards for Customer Information” (March 14, 2001)
 FIL-77-2000, “Bank Technology Bulletin: Protecting Internet Domain Names” (November 9, 2000)
 FIL-67-2000, “Security Monitoring of Computer Networks” (October 3, 2000)
 FIL-68-99, “Risk Assessment Tools and Practices” (July 7, 1999)
 FIL-98-98, “Pretext Phone Calling” (September 2, 1998)
 FIL-131-97, “Security Risks Associated With the Internet” (December 18, 1997)
 FIL-124-97, “Suspicious Activity Reporting” (December 5, 1997)
 FIL-82-96, “Risks Involving Client/Server Computer Systems” (October 8, 1996)

Federal Reserve

Regulations

12 CFR 208.61, “Minimum Security Devices and Procedures”
 12 CFR 208.62, “Reports of Suspicious Activities”
 12 CFR 208.63, “Procedures for Monitoring Bank Secrecy Act Compliance”
 12 CFR 208, appendix D-1, “Interagency Guidelines Establishing Standards for Safety and Soundness”
 12 CFR 208, appendix D-2, “Interagency Guidelines Establishing Information Security Standards”
 12 CFR 211.5(l), “Interagency Guidelines Establishing Information Security Standards”
 12 CFR 211.9, “Interagency Guidelines Establishing Standards for Safeguarding Customer Information”
 12 CFR 211.24(i), “Interagency Guidelines Establishing Information Security Standards”
 12 CFR 225, appendix F, “Interagency Guidelines Establishing Information Security Standards”

Guidance

SR Letter 15-9, “FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors”
 SR Letter 05-19, “Interagency Guidance on Authentication in an Internet Banking Environment”
 SR Letter 04-17, “FFIEC Guidance on the Use of Free and Open Source Software”
 SR Letter 04-14, “FFIEC Brochure With Information on Internet ‘Phishing’”
 SR Letter 02-18, “Section 312 of the USA Patriot Act—Due Diligence for Correspondent and Private Banking Accounts”
 SR Letter 02-6, “Information Sharing Pursuant to Section 314(b) of the USA Patriot Act”
 SR Letter 01-15, “Safeguarding Customer Information”
 SR Letter 01-11, “Identity Theft and Pretext Calling”
 SR Letter 00-17, “Guidance on the Risk Management of Outsourced Technology Services”
 SR Letter 00-04, “Outsourcing of Information and Transaction Processing”
 SR Letter 99-08, “Uniform Rating System for Information Technology”

SR Letter 97-32, “Sound Practices Guidance for Information Security for Networks”

National Credit Union Administration

Regulations

- 12 CFR 716, “Privacy of Consumer Financial Information & Appendix”
- 12 CFR 721, “Federal Credit Union Incidental Powers Activities”
- 12 CFR 741, “Requirements for Insurance”
- 12 CFR 748, “Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance & Appendices”

Guidance

- NCUA Letter to Credit Unions 05-CU-20, “Phishing Guidance for Credit Unions and Their Members”
- NCUA Letter to Credit Unions 05-CU-18, “Guidance on Authentication in Internet Banking Environment” (November 2005)
- NCUA Letter to Credit Unions 04-CU-12, “Phishing Guidance for Credit Union Members” (September 2004)
- NCUA Letter to Credit Unions 04-CU-06, “E-Mail and Internet Related Fraudulent Schemes Guidance” (May 2004)
- NCUA Letter to Credit Unions 04-CU-05, “Fraudulent E-Mail Schemes” (May 2004)
- NCUA Letter to Credit Unions 03-CU-14, “Computer Software Patch Management” (September 2003)
- NCUA Letter to Credit Unions 03-CU-12, “Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to Be Credit Unions” (August 2003)
- NCUA Letter to Credit Unions 03-CU-08, “Weblinking: Identifying Risks & Risk Management Techniques” (April 2003)
- NCUA Letter to Credit Unions 03-CU-03, “Wireless Technology” (March 2003)
- NCUA Letter to Credit Unions 02-CU-13, “Vendor Information Systems & Technology Reviews—Summary Results” (July 2002)
- NCUA Letter to Federal Credit Unions 02-FCU-11, “Tips to Safely Conduct Financial Transactions Over the Internet—An NCUA Brochure for Credit Union Members” (July 2002)
- NCUA Letter to Credit Unions 02-CU-08, “Account Aggregation Services” (April 2002)
- NCUA Letter to Federal Credit Unions 02-FCU-04, “Weblinking Relationship” (March 2002)
- NCUA Letter to Credit Unions 01-CU-21, “Disaster Recovery and Business Resumption Contingency Plans” (December 2001)
- NCUA Letter to Credit Unions 01-CU-20, “Due Diligence Over Third-Party Service Providers” (November 2001)
- NCUA Letter to Credit Unions 01-CU-12, “E-Commerce Insurance Considerations” (October 2001)

NCUA Letter to Credit Unions 01-CU-11, “Electronic Data Security Overview” (August 2001)
 NCUA Letter to Credit Unions 01-CU-10, “Authentication in an Electronic Banking Environment” (August 2001)
 NCUA Letter to Credit Unions 01-CU-09, “Identity Theft and Pretext Calling” (September 2001)
 NCUA Regulatory Alert 01-RA-03, “Electronic Signatures in Global and National Commerce Act (E-Sign Act)” (March 2001)
 NCUA Letter to Credit Unions 01-CU-04, “Integrating Financial Services and Emerging Technology” (March 2001)
 NCUA Letter to Credit Unions 01-CU-02, “Privacy of Consumer Financial Information” (February 2001)
 NCUA Letter to Credit Unions 00-CU-11, “Risk Management of Outsourced Technology Services (With Enclosure)” (December 2000)
 NCUA Letter to Credit Unions 00-CU-07, “NCUA’s Information Systems & Technology Examination Program” (October 2000)
 NCUA Letter to Credit Unions 00-CU-04, “Suspicious Activity Reporting” (June 2000)
 NCUA Letter to Credit Unions 00-CU-02, “Identity Theft Prevention” (May 2000)
 NCUA Regulatory Alert 99-RA-3, “Pretext Phone Calling by Account Information Brokers” (February 1999)
 NCUA Regulatory Alert 98-RA-4, “Interagency Guidance on Electronic Financial Services and Consumer Compliance” (July 1998)
 NCUA Letter to Credit Unions 97-CU-05, “Interagency Statement on Retail On-Line PC Banking” (April 1997)
 NCUA Letter to Credit Unions 97-CU-01, “Automated Response System Controls” (January 1997)
 NCUA Letter to Credit Unions 109, “Information Processing Issues” (September 1989)

Office of the Comptroller of the Currency

Regulations

12 CFR 21, subpart A, “Minimum Security Devices and Procedures”
 12 CFR 21, subpart B, “Reports of Suspicious Activities”
 12 CFR 21, subpart C, “Procedures for Monitoring Bank Secrecy Act Compliance”
 12 CFR 30, appendix A, “Interagency Guidelines Establishing Standards for Safety and Soundness”
 12 CFR 30, appendix B, “Interagency Guidelines Establishing Information Security Standards”
 12 CFR 41.83, “Proper Disposal of Records Containing Customer Information”

Guidance

OCC Bulletin 2016-18, “Cybersecurity of Interbank Messaging and Wholesale Payment Networks: FFIEC Statement” (June 7, 2016)

- OCC Bulletin 2016-14, “FFIEC Information Technology Examination Handbook: Mobile Financial Services, New Appendix to the Retail Payment Systems Booklet” (April 29, 2016)
- OCC Bulletin 2015-44, “FFIEC Information Technology Examination Handbook: Revised Management Booklet” (November 10, 2015)
- OCC Bulletin 2015-40, “Cybersecurity: Joint Statement on Cyber Attacks Involving Extortion” (November 3, 2015)
- OCC Bulletin 2015-31, “FFIEC Cybersecurity Assessment Tool” (June 30, 2015)
- OCC Bulletin 2015-20, “Cybersecurity: Destructive Malware Joint Statement” (March 30, 2015)
- OCC Bulletin 2015-19, “Cybersecurity: Cyber Attacks Compromising Credentials Joint Statement” (March 30, 2015)
- OCC Bulletin 2015-9, “FFIEC Information Technology Examination Handbook: Strengthening the Resilience of Outsourced Technology Services, New Appendix for Business Continuity Planning Booklet” (February 6, 2015)
- OCC Bulletin 2014-53, “Cybersecurity Assessment General Observations and Statement” (November 3, 2014)
- OCC Bulletin 2014-17, “Information Security Vulnerability in OpenSSL Encryption Tool (Heartbleed): Joint Statement” (April 25, 2014)
- OCC Bulletin 2014-14, “Distributed Denial-of-Service Cyber Attacks, Risk Mitigation, and Additional Resources: Joint Statement” (April 3, 2014)
- OCC Bulletin 2014-13, “Cyber Attacks on Financial Institutions’ Automated Teller Machine and Card Authorization Systems: Joint Statement” (April 2, 2014)
- OCC Bulletin 2013-29, “Third-Party Relationships: Risk Management Guidance” (October 30, 2013)
- OCC Bulletin 2013-22, “Windows XP Operating System: Joint Statement” (October 7, 2013)
- OCC Bulletin 2011-26, “Authentication in an Internet Banking Environment: Supplement” (June 28, 2011)
- OCC Bulletin 2008-16, “Information Security: Application Security” (May 8, 2008)
- OCC Bulletin 2007-45, “Identity Theft Red Flags and Address Discrepancies: Final Rulemaking” (November 14, 2007)
- OCC Bulletin 2005-35, “Authentication in an Internet Banking Environment: Interagency Guidance” (October 12, 2005)
- OCC Bulletin 2005-24, “Threats From Fraudulent Bank Web Sites: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents” (July 1, 2005)
- OCC Bulletin 2005-13, “Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance: Interagency Guidance” (April 14, 2005)
- OCC Bulletin 2005-1, “Proper Disposal of Consumer Information: Final Rule” (January 12, 2005)
- OCC Bulletin 2001-35, “Examination Procedures to Evaluate Compliance With the Guidelines to Safeguard Customer Information: Examination Procedures” (July 18, 2001)
- OCC Bulletin 2001-8, “Guidelines Establishing Standards for Safeguarding Customer Information: Final Guidelines” (February 15, 2001)
- OCC Bulletin 2000-14, “Infrastructure Threats—Intrusion Risks: Message to Bankers and Examiners” (May 15, 2000)

OCC Bulletin 1999-20, "Certificate Authority Systems: Guidance for Bankers and Examiners" (May 4, 1999)
OCC Bulletin 1998-3, "Technology Risk Management: Guidance for Bankers and Examiners" (February 4, 1998)
OCC Alert 2001-4, "Network Security Vulnerabilities" (April 24, 2001)
OCC Alert 2000-9, "Protecting Internet Addresses of National Banks" (July 19, 2000)

Other References

Basel Committee on Banking Supervision, "Sound Practices for the Management and Supervision of Operational Risk" (February 2003)
ISACA Control Objectives for Enterprise IT Governance



FFIEC Information Technology Examination Handbook

Management

NOVEMBER 2015

Contents

INTRODUCTION	3
I GOVERNANCE.....	4
I.A IT Governance	4
I.A.1 Board of Directors Oversight	4
I.A.2 IT Management	6
I.A.3 Enterprise Architecture	9
I.B IT Responsibilities and Functions	10
I.B.1 IT Risk Management Structure.....	10
I.B.2 Information Security	10
I.B.3 Project Management	11
I.B.4 Business Continuity.....	12
I.B.5 Information Systems Reporting	12
I.B.6 Planning IT Operations and Investment	14
I.B.7 Other Functions.....	18
II RISK MANAGEMENT	20
II.A Operational Risk.....	20
III IT RISK MANAGEMENT	21
III.A Risk Identification	22
III.A.1 Ongoing Data Collection	22
III.B Risk Measurement	24
III.C Risk Mitigation.....	26
III.C.1 Policies, Standards, and Procedures	27
III.C.2 Personnel.....	27
III.C.3 Information Security	28
III.C.4 Business Continuity.....	30
III.C.5 Software Development and Acquisition.....	31
III.C.6 IT Operations	31
III.C.7 Insurance	32
III.C.8 Third-Party Management	34
III.D Monitoring and Reporting	36

III.D.1	Metrics	36
III.D.2	Performance Benchmarks.....	37
III.D.3	Service Level Agreements	37
III.D.4	Policy Compliance.....	37
III.D.5	Effectiveness of Controls	38
III.D.6	Quality Assurance and Quality Control	38
III.D.7	Reporting	38
APPENDIX A: EXAMINATION PROCEDURES		40
APPENDIX B: GLOSSARY		57
APPENDIX C: REFERENCES		63

Introduction

The “Management” booklet is one of 11 booklets that make up the *Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook)*. The “Management” booklet rescinds and replaces the June 2004 version. This booklet provides guidance to examiners and outlines the principles of overall governance and, more specifically, IT governance. Additionally, this booklet explains how risk management is a component of governance and how IT risk management (ITRM) is a component of risk management. This booklet describes the interaction of these components. The examination procedures in this booklet assist examiners in evaluating the following:

- IT governance as part of overall governance in financial institutions.
- Processes for ITRM as part of risk management in financial institutions.¹

IT supports most aspects of a financial institution’s business; therefore, effective ITRM is not limited to technology. The IT department typically manages back-office operations, network administration, and systems development and acquisition, and is involved in business continuity and resilience, and third-party management. IT management provides expertise in choosing and operating technology solutions for an institution’s lines of business (e.g., commercial credit and asset management) or for enterprise-wide activities (e.g., security and business continuity planning).

IT management is critical to the performance and success of a financial institution. ITRM involves more than containing costs and controlling operational risks and does not work in isolation. A financial institution capable of aligning its IT infrastructure to support its business strategy adds value to the institution and positions itself for sustained success. Financial institutions face many challenges in today’s marketplace, including cybersecurity threats, increasing the need for effective IT management and ITRM.

An institution’s IT systems may connect with affiliates, customers, internal lines of business, third parties (e.g., third-party providers²), and the public. IT creates interdependencies among infrastructure, applications, and Web content. These interdependencies affect the decision-making process necessary to support existing products and services and provide for the delivery of new products and services. Timely, accurate, and secure information is critical to meeting business requirements throughout the institution. Technology evolves rapidly, requiring enhancements to existing systems and prompting new investment in infrastructure, systems, and applications. New technology requires expertise, which creates competition for the necessary

¹ The term “financial institution” includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions, as well as technology service providers that provide services to such entities. The term is used interchangeably with “institution” in this booklet. This booklet may refer to technology service providers specifically in cases where the agencies do not mean to include financial institutions.

² Third-party providers, also called third-party service providers, include technology service providers or other third parties that perform critical business activities for or on behalf of an institution.

talent, knowledge, and skill sets. ITRM includes addressing new sources of risk that arise with new or evolving technology.

I Governance

Action Summary

Financial institution boards of directors should oversee, while senior management should implement, a governance structure that includes the following:

- Effective IT governance.
- Appropriate oversight of IT activities.
- Comprehensive IT management, including the various roles played by management.
- Effective enterprise architecture.

Governance refers to how financial institutions manage and control their institution. Governance provides the structure through which an institution sets and pursues objectives while taking into account the regulatory and market environment and culture of the institution. The governance structure specifies the responsibilities for the board of directors, managers, auditors, and other stakeholders and specifies the level of authority and accountability for decision making. Governance also includes mechanisms for monitoring actions and decisions enterprise-wide.

I.A IT Governance

IT governance is “an integral part of governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives.”³ IT governance objectives are to ensure that IT generates business value for the institution and to mitigate the risks posed by using technology.

I.A.1 Board of Directors Oversight

The board of directors sets the tone and direction for an institution’s use of IT. The board should approve the IT strategic plan, information security program, and other IT-related policies. To carry out their responsibilities, board members should understand IT activities and risks. The board or a board committee should perform the following:

- Review and approve an IT strategic plan that aligns with the overall business strategy and includes an information security strategy to protect the institution from ongoing and emerging threats, including those related to cybersecurity.

³ [Board Briefing on IT Governance](#), 2nd edition, IT Governance Institute, 2003.

- Promote effective IT governance.
- Oversee processes for approving the institution's third-party providers, including the third parties' financial condition, business resilience, and IT security posture.
- Oversee and receive updates on major IT projects, IT budgets, IT priorities, and overall IT performance. The board of directors may need to approve critical projects and activities, such as expanding the institution's product line to include mobile financial services.
- Oversee the adequacy and allocation of IT resources for funding and personnel.
- Approve policies to escalate and report significant security incidents to the board of directors, steering committee, government agencies, and law enforcement, as appropriate.
- Hold management accountable for identifying, measuring, and mitigating IT risks.
- Provide for independent, comprehensive, and effective audit coverage of IT controls.

The board may delegate the design, implementation, and monitoring of specific IT activities to management or a committee (e.g., IT steering committee). An IT steering committee⁴ generally comprises senior management and staff from the IT department and other business units. Committee members do not have to be department heads, but members should understand IT policies, standards, and procedures (collectively, policies⁵). Each member should have the authority to make and be held accountable for decisions within their respective business units. If the institution has a formal risk management function, risk management staff should participate in an advisory capacity.

The steering committee typically is responsible for reporting to the board on the status of IT activities. The reports enable the board to make decisions without having to be involved in routine activities. While the board may delegate the design, implementation, and monitoring of certain IT activities to the steering committee, the board remains responsible for overseeing IT activities and should provide a credible challenge⁶ to management. The steering committee is typically responsible for strategic IT planning, oversight of IT performance, and aligning IT with business needs. The steering committee should have a charter that defines its responsibilities.

The steering committee should receive appropriate information from IT, lines of business, and external sources. Additionally, it should coordinate and monitor the institution's IT resources. The steering committee should review and determine the adequacy of the institution's training, including cybersecurity training, for staff. The steering committee should also document meeting minutes and decisions and inform the board of directors of the committee's activities.

⁴ In smaller or less complex financial institutions that may not have steering committees, these functions would be performed by management, IT department personnel, the board, or a board committee.

⁵ For the purposes of this booklet, policies generally include policies, standards, and procedures, unless stated otherwise. When the booklet refers to policies and practices, it is the combination of the formal and approved policies, standards, and procedures and the actual practices in place.

⁶ A credible challenge involves being actively engaged, asking thoughtful questions, and exercising independent judgment.

I.A.2 IT Management

IT management is responsible for IT performance and administering the day-to-day operation of an institution. IT management should perform the following:

- Implement IT governance.
- Implement effective processes for ITRM, including those that relate to cybersecurity.
- Review and annually approve processes for ITRM.
- Assess the institution's inherent IT risks across the institution.
- Provide regular reports to the board on IT risks, IT strategies, and IT changes.
- Establish and coordinate priorities between the IT department and lines of business.
- Establish a formal process to obtain, analyze, and respond to information on threats and vulnerabilities⁷ by developing a repeatable threat intelligence and collaboration program.⁸
- Ensure that hiring and training practices are governed by appropriate policies to maintain competent and trained staff.

I.A.2(a) *Executive Management*

Executive management, including the chief executive officer (CEO), the chief operating officer (COO), and often the chief information officer (CIO), plays a significant role in IT management at a financial institution. Executive management develops the strategic plans and objectives for the institution and sets the budget for resources to achieve these objectives. To carry out its responsibilities, executive management should understand at a high level the IT risks faced by the institution and ensure that those risks are included in the institution's risk assessments. In the event that executive management is unable to implement an objective or agree on a course of action, executive management should escalate that matter to the board for more guidance.

I.A.2(b) *Chief Information Officer or Chief Technology Officer*

The CIO or chief technology officer (CTO) is responsible and should be held accountable for the development and implementation of the IT strategy to support the institution's business strategy in line with its risk appetite. In less complex institutions, the IT manager may take on these responsibilities. This position typically oversees the IT budget and maintains responsibility for performance management, IT acquisition oversight, professional development, and training. In addition, the CIO or CTO is responsible for implementing the IT architecture and participating in planning activities. The IT management reporting structure should enable this position to accomplish these activities and ensure accountability for security, business resilience, risk reporting, and alignment of IT with business needs. The CIO or CTO should play a key role in

⁷ See the [FFIEC's "Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement,"](#) November 3, 2014.

⁸ For example, a repeatable threat intelligence and collaboration program could include internal resources, such as audit reports and fraud detection tools, or external resources, such as information sharing networks like the Financial Services–Information Sharing and Analysis Center (FS-ISAC) and the Federal Bureau of Investigation's (FBI) InfraGard.

the strategic planning as well as supporting activities of peers in various lines of business. The position often has a leadership role on the steering committee.

I.A.2(c) *Chief Information Security Officer*

The chief information security officer (CISO) is responsible for overseeing and reporting on the management and mitigation of information security risks across the institution and should be held accountable for the results of this oversight and reporting. Often, the CISO is responsible for implementing an information security program satisfying the Interagency Guidelines Establishing Information Security Standards⁹ (Information Security Standards), which were issued pursuant to the Gramm–Leach–Bliley Act (GLBA). While in the past the office of the CISO was considered a technology function, the role has become a strategic and integral part of the business management team. The CISO should be an enterprise-wide risk manager rather than a production resource devoted to IT operations.

To ensure independence, the CISO should report directly to the board, a board committee, or senior management and not IT operations management. While cost and benefit decisions will always need to be made, IT security decisions and funding should not be unduly influenced by operational ease or budgetary constraints. The reporting structure should demonstrate that the CISO has the appropriate authority to carry out the responsibilities of that position and should avoid conflicts of interest that could interfere with the ability of the CISO to make decisions in line with the board’s risk appetite. The institution’s size and complexity plays a role in the reporting structure. A smaller or less complex institution may have an information security officer perform the responsibilities of the CISO and report to senior management. A larger or more complex institution may have additional reporting lines for the CISO into other independent functions, such as risk management.

The CISO is typically responsible for the following:

- Implementing the information security strategy and objectives, as approved by the board of directors, including strategies to monitor and address current and emerging risks.
- Engaging with management in the lines of business to understand new initiatives, providing information on the inherent information security risk of these activities, and outlining ways to mitigate the risks.
- Working with management in the lines of business to understand the flows of information, the risks to that information, and the best ways to protect the information.
- Monitoring emerging risks and implementing mitigations.
- Informing the board, management, and staff of information security and cybersecurity risks and the role of staff in protecting information.
- Championing security awareness and training programs.

⁹ 12 CFR 30, appendix B (Office of the Comptroller of the Currency (OCC)); 12 CFR 208, appendix D-2 (Board of Governors of the Federal Reserve System); 12 CFR 364, appendix B (Federal Deposit Insurance Corporation (FDIC)); and 12 CFR 748, appendix A (National Credit Union Administration (NCUA)). Refer to [appendix C](#) of this booklet for a listing of laws, regulations, and agency guidance.

- Participating in industry collaborative efforts to monitor, share, and discuss emerging security threats.
- Reporting significant security events to the board, steering committee, government agencies, and law enforcement, as appropriate.

I.A.2(d) *IT Line Management*

IT line managers supervise the resources and activities of a specific IT function, department, or subsidiary. They typically coordinate services between the data processing area and other departments. They report to senior IT management on the plans, projects, and performance of their specific systems or departments. Some IT functions that often rely on line managers include data center operations, network services, application development, systems administration, telecommunications, customer support, and disaster recovery. Frontline managers coordinate daily activities, monitor current production, ensure adherence to established schedules, and enforce appropriate policies and controls in their areas.

I.A.2(e) *Business Unit Management*

Managers in an institution's lines of business or business units also have IT responsibilities. Examples of these responsibilities include the following:

- Establishing processes for ongoing communication of business needs, information systems reporting needs, and product development plans to IT support or line management.
- Ensuring that IT development efforts are prioritized, funded, and aligned with business strategy in the business unit.
- Establishing processes to test compliance with IT-related control policies in the business unit.
- Ensuring that required backup IT resources are available.
- Documenting information flows throughout the business unit and notifying the CISO when business processes change.
- Performing due diligence reviews for prospective third-party providers and ongoing monitoring of third-party providers with which the institution has established relationships.
- Engaging with the CISO to discuss inherent information security risks of new business unit initiatives.

The specific technology roles in IT and business unit management may vary depending on the institution's approach to risk management and policy enforcement. Institutions can approach technology management using either a centralized or a decentralized strategy.

In a centralized IT environment, IT management typically acquires, installs, and maintains technology for the entire institution. IT management has a greater ability to control and monitor the institution's technology investment. A centralized approach may promote greater operational efficiencies. The business unit managers retain the responsibility for enforcing internal controls within their areas.

In a decentralized IT environment, IT management serves in an advisory role in some business units' acquisition, installation, and maintenance of technology. The decentralized approach is

more common in larger or more complex institutions, where IT management can expedite decisions on IT services by transferring decision-making authority to strategically significant departments. In this approach, business line management has a much greater responsibility for ensuring that technology investments are consistent with enterprise-wide strategic plans. Institutions should ensure system compatibility and enforcement of enterprise-wide policies in a decentralized environment. IT management should still have a role in defining the institution's control requirements, but enforcement of enterprise-wide policies may be more difficult.

I.A.3 Enterprise Architecture

Enterprise architecture (EA) is the overall design and high-level plan that describes an institution's operational framework and includes the institution's mission, stakeholders, business and customers, work flow and processes, data processing, access, security, and availability. An EA program facilitates the conceptual design and maintenance of the network infrastructure, related IT controls, and policies. Management of financial institutions with highly complex systems or those experiencing growing IT costs without corresponding benefits should consider using or adjusting an EA program. As EA has evolved, different methodologies to implement EA programs have been developed. The underlying principle for all EA programs is that business IT requirements follow a predefined process that begins with a business need and ends with an IT solution that conforms to the policies approved by senior management and the board of directors. An effective EA program can result in the following:

- Enhanced interoperability from using IT to drive business adaptability.
- Closer partnership between business and IT groups.
- Improved focus on the institution's goals.
- Reduced numbers of failed IT systems.
- Reduced complexity of IT systems.
- Improved agility of IT systems.
- Closer alignment between IT deliverables and business requirements.
- Assurance that all software, including operating systems, is current and vendor supported.
- Improved morale, as more staff members see a direct correlation between their work and the institution's success.

Key considerations when developing an EA program include security, business resilience, data management, external connectivity, and alignment with the institution's goals and objectives. To effectively implement an EA program, the institution should analyze the risks and potential impact of threats to all of the institution's activities. A comprehensive EA program based on prudent practices can help an institution better develop processes to manage IT issues and identify, measure, and mitigate technology-based risks and threats.

I.B IT Responsibilities and Functions

Action Summary

As part of the governance structure, financial institution management should ensure development, implementation, and maintenance of the following:

- An effective IT risk management structure.
- A comprehensive information security program.
- A formal project management process.
- An enterprise-wide business continuity planning function.
- An accurate and timely process for information systems reporting.

I.B.1 IT Risk Management Structure

The institution should have an adequate ITRM structure. Depending on the size and complexity of the financial institution, this structure can take different forms. In a large or complex institution, the ITRM function may be an independent business unit.¹⁰ In a small or less complex institution, ITRM may be integrated with functional areas, such as information security, business continuity planning, third-party management, and regulatory compliance. Internal audit, specifically IT audit, can provide independent assurance on the effectiveness of risk management, but should not be responsible for its implementation. Regardless of the structure used, management should ensure that lines of authority are established for enforcing and monitoring controls.

I.B.2 Information Security

The institution should have a comprehensive information security program that addresses all technology and information assets and that complies with the Information Security Standards; these standards and the GLBA are discussed in detail in the “[Protecting Sensitive Customer Information](#)” section of this booklet. The information security program should include appropriate administrative, technical, and physical safeguards based on the inherent risk profile and the individual activities, products, and services of the institution. The board should delegate responsibility to the CISO or other appropriate personnel for assessing whether IT operations conform with policies. The CISO should ensure appropriate consideration of risks involved with new products, emerging technologies, and information systems. Testing of the controls identified in the information security program should be delegated to an independent auditor.¹¹

¹⁰ Some agencies have guidance on ITRM for larger, more complex financial institutions.

¹¹ An independent audit function can include internal auditors with sufficient independence to perform an adequate review, outside consultants or auditors, or a combination of both.

The institution should separate information security program management and monitoring from the daily security duties of IT operations. The IT department should have personnel with daily responsibility for implementing the institution's security policy. Responsibility for making changes and granting exceptions to policy should be segregated from the enforcement of the controls. Refer to the *IT Handbook's* "Information Security" booklet for more information.

I.B.3 Project Management

An effective project management process is a key factor in a well-managed IT operation and includes applying knowledge, skills, tools, and techniques to achieve project objectives. The operational complexity of the institution dictates the degree of formality of project management practices. Generally, project management consists of initiating, planning, executing, controlling, and completing projects. The institution's ability to manage projects drives its ability to adapt to changes in its business requirements and satisfy its strategic objectives. Management uses project management techniques to control projects for systems acquisition and development, systems conversions, product enhancements, infrastructure upgrades, and system maintenance.

Project teams should balance resource investments of time, money, and expertise with a project's priority, risk, and requirements. Management should monitor projects closely to control costs and assure adherence to project management policies. A formal project management system, if used, should employ well-defined and proven techniques for managing projects at all stages. Regardless of the system used, management should include the following elements in its project management process:

- Oversight by experienced and skilled project managers, whether they are employees of the institution or consultants hired for specific projects.
- Accepted and standardized project management practices.
- Senior management support, including a review process around significant projects.¹²
- Defined and monitored institution-wide project risk assessment methodology.
- Approval processes to ensure that projects are defined, go through a risk assessment process, and meet requirements.
- Established project requirements with collaboration among stakeholders and project management staff for each phase of the project.
- Target completion dates to track each task or phase of the project.
- Timely project status updates to compare actual completion dates with target dates.
- Procedures to track and measure project performance against requirements.
- A defined change management process, including approval requirements.
- Sufficient testing at all appropriate stages of the project to ensure that the new system or process will not negatively impact existing systems.
- Training for end users and designated staff responsible for ongoing support.
- A well-managed process for transition in ownership from implementation teams to operational teams.

¹² The significance of projects will depend on the institution's activities and its size and complexity.

Based on an institution's size and complexity, an institution pursuing a more-than-moderate growth path should consider establishing a project management office to promote sound management practices and principles. Refer to the *IT Handbook's* "Development and Acquisition" booklet for more information.

I.B.4 Business Continuity

Business continuity is defined as the ability to maintain operations and services, both technology and business, in the event of a disruption to normal operations and services. The board of directors should oversee implementation and approve policies relating to business continuity planning. Senior management should establish and implement policies, standards, and procedures and define responsibilities for enterprise-wide business continuity planning. Because business continuity is important for both business processes as well as technology operations, business continuity planning should be approached on an enterprise-wide basis. Business continuity planners should assess the ability for all lines of business to remain resilient or recover from disruptions or degradations. The business continuity function often resides in the risk management organizational structure. A specific member of management should be assigned responsibility for the oversight of the business continuity function, and both business and technology departments should assign personnel to develop and maintain the individual business unit plans. Refer to the *IT Handbook's* "Business Continuity Planning" booklet for more information.

I.B.5 Information Systems Reporting

A variety of systems can provide management with the information necessary to manage an institution effectively. These systems are often referred to as management information systems, decision support systems, and risk control self-assessments, to name just a few. While the precise definitions vary, these information systems are used by management to assess the performance of the business, report on the risks and challenges it faces, and assist management in the successful operation of the business.

Management should design its information systems to do the following:

- Provide management with information that is timely, accurate, consistent, complete, and relevant.
- Provide an objective system for recording and aggregating information.
- Provide key risk performance trends and indicators; and measure performance against risk tolerances.
- Support the institution's strategic plan.
- Ensure the confidentiality, integrity, and availability of data.
- Reduce labor-intensive manual activities.
- Enhance communication among staff.

Information systems reporting supplies decision makers with facts, supports and enhances the overall decision-making process, and can improve job performance throughout an institution. At the most senior levels, information systems reporting provides the data and information to help

the board and management make strategic decisions. At other levels, information systems reporting allows management to monitor the institution's activities and distribute information to staff, customers, and members of management.

Advances in technology have increased the volume of data and information available to management and directors for planning and decision making. Because report generation systems can rely on manual data entry or extract data from many different financial and transaction systems, management should establish appropriate control procedures to ensure that data and information are correct and relevant. Because information systems reporting can originate from multiple technology platforms, the controls should be designed to maintain the integrity of the information and the processing environment.

To function effectively as a feedback tool for management and staff, information systems reporting should meet five essential elements:

- **Timeliness:** To facilitate prompt decision making, an institution's information systems should be capable of providing and distributing current information to appropriate management or staff.
- **Accuracy:** A sound system of automated and manual internal controls should exist to ensure the validity of the information and should include appropriate editing, balancing, and internal control checks.
- **Consistency:** To be reliable, data should be processed and compiled in a uniform manner. Variations in data collection and reporting methods can distort information and trend analysis.
- **Completeness:** Reports should contain the necessary information to inform decision makers without voluminous detail.
- **Relevance:** Information systems should provide current, applicable, and actionable information.

In a complex institution, information systems reporting can be highly structured and automated. In a less complex institution, it can be informal and less dependent on sophisticated technology systems. Institution management should adopt information systems reporting capabilities commensurate with the size and complexity of the institution.

I.B.6 Planning IT Operations and Investment

Action Summary

Financial institution boards should oversee, while senior management should implement, an IT planning process with the following elements:

- Long-term goals and the allocation of IT resources to achieve them, usually within a three- to five-year horizon.
- Alignment of the IT strategic plan with the enterprise-wide business plan.
- Identification and measurement of risk before changes or new investment in technology are made.
- An IT infrastructure to support current and planned business operations.
- Integration of IT spending into the budgeting process and weighing of direct and indirect benefits against the total cost of ownership of the technology.

Planning involves preparing for future activities by defining goals and the strategies used to achieve them. Future activities may include releasing a new product or service, planning mergers and acquisitions, or preparing for the end of service for an IT system. IT is an integral part of financial institution operations. Therefore, institution management should integrate consideration of IT resources and investments into the overall business planning process. Major investments in IT resources have long-term implications on both the delivery and performance of an institution's products and services.

Plans may vary significantly depending on institutions' size and structure. Management should strive to achieve a planning process that constantly adjusts for new risks or opportunities and maximizes IT's value. Management should document its plan; a written plan, however, does not guarantee an effective planning process. Management should measure the effectiveness of a specific plan by whether the plan meets the institution's business needs. A sound plan should involve the board of directors, senior management, and staff in the planning process. The board of directors should provide a credible challenge to management when the board reviews and approves the plan. Senior management participates in formulating and implementing the plan. The individual departments and functional areas identify specific business needs and, ultimately, implement the plan.

An institution that uses third-party providers should verify that the provider can continue to support the institution's plans and that the plans and actions of the provider do not negatively impact the institution. As part of the institution's ongoing monitoring process, management should participate in third-party provider client user groups. Institution management should also consider a review of client portals, news articles, provider newsletters, and press releases to maintain awareness of provider activities, changes in strategy and products, future plans, and potential or actual service or security issues.

I.B.6(a) *Strategic IT Planning*

Strategic IT planning should address long-term goals and the allocation of IT resources to achieve them. Strategic IT planning focuses on a three- to five-year horizon and helps ensure that the institution's technology plans are consistent and aligned with the institution's business plan. Effective strategic IT planning can ensure delivery of IT services that balance cost and efficiency, while enabling the business units to meet the competitive demands of the marketplace. The IT strategic plan should address the budget, periodic board reporting, and the status of risk management controls.

Tactical plans support the larger IT strategic plan by defining specific steps necessary to fulfill it. Tactical plans outline specific steps, personnel, tools, and timetables to achieve the goals laid out in the IT strategic plan, typically using a one-year time frame. These tactical plans typically address hardware and software architecture, end-user computing resources, and processing done by third-party providers. These plans are often created by mid-level managers.

The operational IT plan is used to achieve the goals and objectives of both the tactical plans and the larger strategic plan. It provides the detailed information to perform the tasks needed to implement the tactical plans of an institution. The operational IT plan includes the milestones and tasks that must be undertaken, the individuals who have responsibility for each milestone and task, the timelines in which they must be completed, the conditions for success, and the financial resources necessary to complete each milestone and task. Operational plans should flow logically from both the tactical plans and the larger IT strategic plan. Front-line management typically creates and revises operational plans as needed based on changes in the underlying business needs.

Strategic IT planning should consider a number of factors:

- Marketplace conditions.
- Customer demographics.
- Institution growth targets.
- Mergers and acquisitions.
- Technology standards.
- Regulatory requirements (e.g., privacy, security, consumer disclosures, and other reporting requirements).
- Cost containment.
- Process improvement and efficiency gains.
- Customer service and technology performance quality.
- Third-party relationship opportunities versus in-house expertise.
- Optimal infrastructure, including systems and software replacement.
- Ability to adopt and integrate new technology.

These factors should align with the institution's business plans. Well-implemented IT plans enable the institution to deliver business value in terms of market share, earnings, and capital growth. If used, the IT steering committee's cross-functional membership makes the committee well-suited for balancing or aligning the institution's IT investment with its strategic objectives.

Typically, institutions that align IT with changing business goals and objectives have more effective operations.

Technology expenditures should be commensurate with the financial condition of the institution. They should also be appropriate to meet the changing IT strategy, provide enterprise-wide value, support necessary growth, ensure appropriate security and business resilience, and mitigate technology incompatibilities. For example, delaying investments and spending too conservatively on infrastructure or new products may lead to ineffective operations and service levels. Without a full understanding of the available technology, the institution is not able to update processes and products or achieve productivity gains or increased revenues. To create the appropriate balance, institutions should link strategic and operational plans between IT and the business units.

Management should address the following four key factors of IT planning:

- **Senior management participation:** Senior management should understand and support the IT strategic plan and established priorities.
- **Role of IT:** Management should clarify the role of IT and determine whether the current IT planning process enables personnel to work toward achieving enterprise-wide goals and objectives.
- **Impact of IT infrastructure:** Management or the IT steering committee should understand the relationship between the IT infrastructure and applications and the business strategic and operating plans. The IT infrastructure should directly support the goals and objectives of these plans.
- **Accurate scorecard on past performance:** Management or the IT steering committee should monitor past IT projects and initiatives after implementation to determine whether the institution realized the anticipated costs and benefits. The scorecard should be based on a set of objective measures.

Management should also create and maintain an alignment between IT and enterprise-wide strategies by performing the following:

- Reviewing whether IT strategic plans are aligned with the business strategy.
- Reviewing whether IT performance supports the planned strategy.
- Ensuring that the IT department is delivering on time, within budget, and to specification.
- Balancing investments between systems that support current operations and systems that transform operations and enable business units to grow and compete in new areas.
- Focusing IT resource decisions on specific business objectives, such as entry into new markets, enhanced competitive position, revenue growth, improved customer satisfaction, or customer retention.

I.B.6(b) *IT Resources*

Management should provide IT resources that are adequate to meet the current operational needs of the institution. Operational planning should consider the impact of any changes on critical business processes. Business processes are the integration of people, technology, and procedures

used to accomplish a task or complete a transaction. Changes in business processes should be coordinated and aligned with available IT resources. IT resources include the following elements:

- **Infrastructure:** Power, telecommunications capacity, network architecture, and facilities.
- **Hardware:** Mainframes, network servers, personal computers, communications networks, mobile devices, storage devices, and peripherals.
- **Operating software:** Operating systems, compilers, and utilities designed to enable the equipment and applications software to function effectively, both internally and externally.
- **Application software:** Programs designed to permit application users to perform a specific task or function. Application software runs on top of operating system software.
- **Personnel:** Staff and training programs.

Management should consider sufficient capacity for current and future needs for each of these elements.

I.B.6(c) *Budgeting*

Budgeting is another step in the operational planning process. The board should assess management's plans and its success in defining and meeting budgetary goals as one means of evaluating management's performance. The budget is a coordinated financial plan used to estimate and control the institution's activities. By assessing future economic developments and conditions, management creates an action plan and records changes in the balance sheet accounts and profitability (predicated on implementation of the plan). The budget not only projects expected results, but also serves as an important check on management.

When considering new IT projects, management should look at the entry costs of the technology and the post-implementation support costs. Increasingly, institutions are demanding, and third-party providers are providing, information regarding the total cost of ownership (TCO) beyond initial entry costs. IT projects often have undocumented costs, including the resources required to configure, maintain, repair, support, upgrade, and manage the technology over its lifetime. Readily available TCO models, as well as historical data, provide management with tools to incorporate such costs into the selection and budgeting process.

Some institutions budget IT as a separate department. A financial analysis of an IT department should include a comparison of the cost-effectiveness of the in-house operation versus contracting with a third-party provider. The analysis may also include a peer group comparison of operating costs and ratios. Depending on its size and complexity, the institution may allocate costs to the institution's lines of business. When cost allocation is used, management should ensure equitable assignment of the costs to each line of business. Equitable assignment of the costs is often accomplished by use of a chargeback system that records usage of resources based on a performance metric such as central processing unit cycles.

In some instances, a separate subsidiary of the holding company manages the IT function. An IT subsidiary can provide essential services at costs below those of third-party providers or individual institutions. Some relationships, however, may not result in a cost savings. Any

transaction between the institution and its affiliates must comply with applicable laws and regulations.¹³ Refer to the *IT Handbook*'s "Outsourcing Technology Services" booklet for more information.

I.B.7 Other Functions

Action Summary

The IT function at a financial institution is influenced by several other functions, which should include the following:

- The human resources function should hire and maintain competent and motivated IT staff.
- The IT audit function should validate appropriate controls to mitigate IT risk.
- The compliance function should validate that systems and applications adhere to applicable laws and regulations.

I.B.7(a) Human Resources

Human resources (HR) supports the IT function's ability to hire and maintain a competent and motivated staff. IT management should integrate its management of HR with IT planning to ensure optimum development and availability of IT skills.

Components of an effective IT HR management process include compensation planning, performance reviews, knowledge transfer mechanisms (e.g., rotational assignments), training, and mentoring. The board should actively and effectively provide oversight of incentive compensation programs for IT management to ensure that the programs appropriately balance risk and reward and are compatible with effective controls and risk management.

An institution should have programs in place to ensure that staff members have the expertise necessary to perform their jobs and achieve company goals and objectives. The institution may need to look externally to find necessary expertise for specialized areas.

¹³ Sections 23A and 23B of the Federal Reserve Act, codified at 12 USC 371c and 12 USC 371c-1, govern transactions between certain financial institutions, such as Federal Reserve member banks, national banks, and federal savings associations, and the institutions' affiliates. Specifically, section 23B(a) states that an institution and its subsidiaries may engage in certain transactions with an affiliate, including the payment of money or the furnishing of services to an affiliate under contract, lease, or otherwise. The transactions must be on terms and under circumstances, including credit standards, that are substantially the same, or at least as favorable to such institution, as those prevailing at the time for comparable transactions with or involving other nonaffiliated companies. In the absence of comparable transactions, the statute requires that such transactions be on terms and under circumstances, including credit standards, that in good faith would be offered to, or would apply to, nonaffiliated companies. See 12 USC 371c-1(a).

Management should develop training programs for new technology and products before their deployment in the institution. The institution may use its own certification program or encourage employees to obtain an external certification to ensure that the staff maintains the necessary expertise to support the business.

The board and senior management should consider appropriate succession and transition strategies for key managers and staff members. Some strategies include the use of employment contracts, professional development plans, and contingency plans for interim staffing of key management positions. Management should have backup staff for key positions and should cross-train additional personnel. The objective is to provide for a smooth transition in the event of turnover in vital IT management or IT operations.

I.B.7(b) *IT Audit*

The audit department should send IT audit reports to appropriate management and directly to the board of directors or a designated board committee. The board of directors is responsible for overseeing the IT auditors' performance and compensation, including whether the IT auditors have the necessary expertise and the audit coverage is adequate, timely, and independent. Depending on the institution's size and complexity, the board of directors may completely outsource the IT audit function. In those cases, the outsourced auditor should be engaged by the board or audit committee.

IT auditors should validate that IT controls are designed appropriately to mitigate risk and are operating as management intended. IT audit should be completely independent, should have no role in designing or implementing controls, and should not have primary responsibility for enforcing policy. Management should have processes in place to monitor and enforce policy compliance. IT audit should verify that those processes function effectively and report the results to the board.

Senior management should ensure cooperation between business unit management and IT audit. Management should also ensure timely and accurate response to audit concerns and exceptions and ensure appropriate and timely corrective action.

Refer to the *IT Handbook's* "Audit" booklet for more information.

I.B.7(c) *Compliance*

Senior management should ensure that compliance staff reviews new products, systems, applications, or changes to ensure compliance with applicable laws and regulations. New implementations or changes can cause noncompliance through, for example, inaccurate interest rate calculations, inadequate or inaccurate disclosures, weak security controls over the creation, storage, or transmission of customer information, or poor customer verification procedures.

II Risk Management

Financial institution management should understand and evaluate risk across the institution, including the definitions and categories of risk. Risk is the potential that events, expected or unanticipated, may have an adverse effect on a financial institution's earnings or capital. For regulatory purposes, risk is categorized as operational, liquidity, interest rate, credit, price, strategic, and compliance (legal). Although financial institution management should be aware of all potential risks as part of its overall risk management program, operational risk is the primary risk associated with IT.

II.A Operational Risk

Operational risk is the risk of failure or loss resulting from inadequate or failed processes, people, or systems. Operational risks from IT are present not only in back-office operations and transaction processing but also in areas such as customer service, systems development and support, internal controls and processes, and capacity planning. Operational risk may cross all lines of business and can be caused by internal or external events. Operational risk from IT affects strategic, compliance, and other risks.

Management should be aware of the implications of operational risk from IT, including the following:

- Strategic risk can stem from inaccurate information or analysis that causes management to make poor IT strategic decisions.
- Compliance risk can result from an institution's inability to meet the regulatory and legal requirements associated with its products and services. Compliance risk can also result from an institution's dependence on products and services to meet its operations and reporting requirements.

Management should have a comprehensive view of operations and business processes that are supported by technology. IT management should maintain an active role in institution strategic planning to align IT with established business goals and strategies. Additionally, management should ensure that effective IT controls exist throughout the institution, either through direct oversight or by holding lines of business accountable for IT-related controls. From a control standpoint, management should participate in the ITRM process to identify and measure risk from the use of IT, support decisions on how to mitigate the risks, implement the mitigation decisions, and monitor and report on the resulting outcomes.

III IT Risk Management

Action Summary

Financial institution management should develop an effective ITRM process that supports the broader risk management process. As part of the ITRM process, management should perform the following:

- Identify risks to information and technology assets within the financial institution or controlled by third-party providers.
- Measure the level of risk.
- Mitigate the risks to an acceptable residual risk level in conformance with the board's risk appetite.
- Monitor changing risk levels and report the results of the process to the board and senior management.

The ITRM process supports the enterprise-wide risk management framework through four activities: (1) risk identification, (2) risk measurement, (3) risk mitigation, and (4) risk monitoring and reporting. Risk identification generally documents inventories of systems and information necessary to financial institution operations and defines the potential threats to the institution's systems and operations. Risk measurement is a process of determining the likelihood of an adverse event or threat occurring and the potential impact of such an event on the institution. Risk mitigation includes the implementation of appropriate controls to reduce the potential for risk and bring the level of risk in line with the board's risk appetite. Monitoring and reporting provide the board and senior management with regular updates demonstrating the effectiveness of the risk management process.

Management should identify, measure, mitigate, monitor, and report IT risks that threaten the safety and soundness of an institution. An effective ITRM process is regularly updated and aligns IT and business objectives. This process should have a higher level of formality in more complex institutions.

The ITRM process is not complete without consideration of the overall IT environment. Management may need to consider risks associated with IT environments from two different perspectives:

- A centralized IT environment supports lines of business across shared infrastructure.
- A decentralized IT environment supports lines of business with separately managed infrastructure.

The following sections detail the processes involved in each of the ITRM activities.

III.A Risk Identification

Action Summary

Financial institution management should maintain a risk identification process that is coordinated and consistent throughout the institution. Risk identification includes ongoing data collection from existing activities and new initiatives.

All activities within a financial institution present a degree of risk. The nature of such risk, before applying controls and other mitigations, is called inherent risk. Senior management should ensure that IT risk identification efforts at the enterprise-wide level are coordinated and consistent throughout the institution. Management should maintain inventories of assets (e.g., hardware, software, and information), event classes (e.g., natural disaster, cyber, and insider abuse or compromise), threats (e.g., theft, malware, and social engineering), and existing controls as an important part of effective risk identification. Inventories should include systems and information hosted or maintained externally. Comprehensive IT risk identification should include identification of cybersecurity risks as well as details gathered during information security risk assessments required under guidelines implementing the GLBA.¹⁴ Participation in an information-sharing forum, such as FS-ISAC,¹⁵ should be a component of the risk identification process because sharing information may help the institution identify and evaluate relevant cybersecurity threats and vulnerabilities.¹⁶

Senior management should make risk management decisions based on a full understanding of identified risks. Small institutions with less complex systems may have a more simplified risk identification process. Regardless of the complexity, the process should be formal and adapt to changes in the IT environment. The effectiveness of the risk identification process is demonstrated by management's understanding and awareness of risk, the adequacy of formal risk assessments, and the effectiveness of the risk mitigation, including policies and internal controls.

III.A.1 Ongoing Data Collection

Understanding an institution's environment is the first step in any risk identification process. In identifying risks, management should collect and compile the following information regarding the institution's IT environment:

¹⁴ Refer to the "Information Security" booklet of the *IT Handbook* for more information on the GLBA and the "Interagency Guidelines Establishing Information Security Standards."

¹⁵ Refer to "[FFIEC Releases Cybersecurity Assessment Observations, Recommends Participation in Financial Services Information Sharing and Analysis Center](#)," November 3, 2014.

¹⁶ Ibid.

- **IT systems inventories:** These are critical to understanding the institution's IT infrastructure, as well as identifying the access and storage points for confidential customer and institution information.
- **IT strategic plan:** Such a plan can provide insight into the institution's planning process. Review and analysis of the strategic plan as part of the risk identification process may highlight developing risk exposures or other deficiencies that limit the institution's ability to implement strategic priorities.
- **Interconnectivity:**¹⁷ Management should comprehensively identify connections with third-party providers, including other financial institutions and financial institution intermediaries, because of the potential for significant operational risk through these interdependencies. In addition, management should identify all access points and connection types that pose risk, such as local or wide area network (LAN/WAN) connections to other networks or Internet service providers, cloud services, Wi-Fi, and cellular connections.
- **Information flow:** Management should document the flows of information throughout the institution, including flows of sensitive customer information. This documentation is critical to understanding what information assets the institution owns, where they are stored and transmitted, and who has access to them.
- **Business continuity and disaster recovery plans:** These plans prioritize the availability of various lines of business and often encompass restoration and provision of control and customer service and support. These plans can offer insight into the institution's critical operations and control environment.
- **Third-party management program:** Due diligence and monitoring present valuable information on the third-party provider's control environment. This information is necessary to identify the risks in an institution's IT environment.
- **Call center:** Issue tracking reports can often indicate potential performance or control issues if the problem reports are aggregated and analyzed for repetitive or common issues.
- **Self-assessments:** Assessments specifically on IT-related controls can provide early identification of policy noncompliance or weaknesses in controls.
- **IT audit findings:** These findings provide insight into the effectiveness of internal controls and staff and management's commitment to policy compliance.
- **Threat intelligence information:** By working with industry forums and groups, institutions can obtain information about emerging threats and the ways other organizations manage those threats.

In the process of collecting and compiling this information, management should include the potential cybersecurity risks associated with these areas of the financial institution's IT environment.

¹⁷ This term refers to the connections between networks that are owned and operated by different entities.

III.B Risk Measurement

Action Summary

Financial institution management should develop risk measurement processes that include the following elements:

- Measuring risk using qualitative, quantitative, or a hybrid of methods.
- Recognizing that risks do not exist in isolation.
- Prioritizing the risks based on the results of risk measurement.

Risk measurement typically is performed according to policies governing the enterprise-wide risk management process. Measurement is helpful in estimating the likelihood of an adverse event and its potential impact across the institution. Measurement across the financial institution is particularly important when an event impacts shared services and infrastructure or a shared customer base.

Measurements may be qualitative, quantitative, or a hybrid of both. Qualitative measures rely on experience, judgment, and intuition and are subject to potential flaws due to bias and other factors. Types of qualitative assessments include questionnaires or surveys to measure risk. Quantitative measures, on the other hand, are based on numerical values, such as dollar amounts or number of systems out of compliance. Quantitative measurement methods may include top-down and all-encompassing measures as well as measures that are limited to discrete activities and management choices. Hybrid measurements are frequently used and typically combine qualitative and quantitative measures to provide a more comprehensive analytical approach. A hybrid assessment could include a survey of staff to gain individual insight combined with numerical data inputs. Important considerations when evaluating hybrid measures include those presented above for both qualitative and quantitative measures.

Regardless of the method used, management should estimate the likelihood of occurrence and severity of the impact of the identified risk. When analyzing the potential impact, management should consider financial or other impact to the institution. Organizational impacts are highly variable and not always easy to quantify. They include such considerations as lost revenue, data recovery and reconstruction expense, costs of litigation and potential judgments, loss of market share, and increases to premiums or denials of insurance coverage.

There are a variety of techniques, including the use of applications, to measure risk. Applications to provide measurement-related information may be developed in-house, acquired, or both. IT's role in development and acquisition should be consistent with the guidance in the *IT Handbook's* "Development and Acquisition" booklet.

The following are common types of risks that often have significant impact:

- **Security breaches:** Including internal and external breaches, weak program code used to perpetrate fraud, and computer viruses.
- **System failures:** Including telecommunication failures, LAN and WAN failures, hardware and software failures, interconnectivity failures, and backup system failures.
- **External events:** Including weather-related events, earthquakes, pandemics, terrorism, cyber attacks, cut utility lines (e.g., telecommunication, water, and power), or widespread power outages.
- **Insider events:** Including intentional or unintentional acts by staff, such as carelessness, social engineering that results in inappropriate access or the installation of malware, and improper changes to transactions, systems, or databases.
- **Development and acquisition issues:** Including strategic platform or supplier risk, inappropriate definition of business requirements, incompatibility with existing systems, inadequate project management, programming errors (internal or external), change management issues, failure to integrate and/or migrate systems or applications successfully, or obsolescence of software.
- **Capacity planning issues:** Including inadequate capacity planning or inaccurate forecasts of growth.
- **Third-party provider issues:** Including deficiencies in the oversight of third-party providers in areas such as reporting, breach notification, business continuity and resilience testing, and subcontracting (fourth-party) risk management.

The institution should recognize that no risk exists in isolation; there are interdependencies among risks. This reinforces the need for an integrated approach for risk management. To ensure accurate risk measurement, management should ensure that risk assessments are updated regularly, and as changes occur, to address new technologies, products, services, and connections before deployment.

The IT department can have a specialized and unique role in the measurement and prioritization of IT-related threats, based on its expertise in the development, application, and use of IT. Institution management should use that expertise, as well as the expertise provided by others (e.g., auditors, third-party providers, and other third parties), in the risk measurement process. Once management identifies and measures the institution's IT risk, it should rank the risks and prioritize its response.

III.C Risk Mitigation

Action Summary

Financial institution management should implement effective control and risk transfer practices as part of its overall IT risk mitigation strategy. These practices should include the following:

- Establishing, implementing, and enforcing IT policies, standards, and procedures.
- Documenting policies for hiring and training personnel.
- Implementing internal controls for information security risks.
- Establishing and implementing effective cybersecurity controls.
- Developing and testing formal business continuity plans.
- Establishing and implementing a well-managed and controlled software development and acquisition function.
- Controlling, managing, and monitoring an IT operations function.
- Reviewing insurance for IT operations, including cyber insurance.
- Developing an effective third-party management program.

Risk mitigation is the process of reducing risks through the introduction of specific controls. Risk mitigation decisions are implemented through the use of controls or risk transfer. Risk transfer can be accomplished through mechanisms such as insurance. After implementing controls or transferring the risk, management should determine the level of residual risk, or the risk that cannot be fully mitigated or avoided. Both controls and risk transfer should be considered when evaluating whether a residual risk is within the financial institution's risk appetite. Risk appetite is the amount of risk a financial institution is prepared to accept when trying to achieve its objectives.

Controls are implemented in financial institution activities and may be performed either manually by staff or through automated systems. Controls can be classified by timing (preventive, detective, corrective) or nature (administrative, technical, physical). Refer to the *IT Handbook's* "Information Security" booklet for more information. The IT department generally implements controls within the institution for assets that are under the IT department's control. Non-IT-related controls implemented elsewhere in the financial institution should be coordinated with the IT department to ensure their adequacy.

Controls should be evaluated for effectiveness against identified threats or vulnerabilities. Evaluation typically is accomplished by tools that supplement and complement assurance and audit activities. Two examples of tools used are control self-assessments and scenario analysis. Control self-assessments, used internally to assess the effectiveness of ITRM processes and related controls, typically are performed by departments or lines of business periodically testing and validating their controls. Scenario analysis is a process of analyzing possible future events by considering alternative outcomes. It can be a valuable tool for gaining an overall

understanding of the exposure to existing, expected, and plausible (including potentially severe) events, as well as the robustness of—or gaps in—controls or other risk mitigation.

Additionally, a control self-assessment should encompass external requirements, such as laws, regulations, and widely accepted control standards and practices.¹⁸ Failure to comply with external requirements, whether in law, regulation, or contract, can result in compliance risk as well as strategic or other risks. Conformance with widely accepted control standards and practices can demonstrate due care in the operation of IT and potentially reduce operational risk.

Conformance with external requirements alone is not sufficient to ensure that the overall ITRM process is adequate. The ITRM process encompasses risk posed by the operation of the financial institution in its specific internal and external environment. Accordingly, the ITRM process should consider whether the IT control structure, when combined with controls outside the IT systems, adequately mitigates risk associated with the use of IT.

III.C.1 Policies, Standards, and Procedures

In general, a policy is a governing principle that provides the basis for standards and is adopted by the board. The policy is an overall statement of the institution's philosophy or intent. Standards are mandatory criteria that ensure conformity with policy, government regulations, and acceptable levels of control. Procedures are typically documents that describe, in detail, the behavior or processes used to adhere to the criteria mandated by standards. Clearly written and frequently communicated policies can establish clear assignments of duties, help staff coordinate and perform their tasks effectively and consistently, and aid in training staff. Senior management should ensure that policies, standards, and procedures are current, well documented, and integrated with the institution's information security strategy.

Institution management should create, document, maintain, and adhere to policies, standards, and procedures to manage and control the institution's IT risk. The level of detail depends on the complexity of the IT environment but should enable management to monitor the identified risk posture. Review of adherence to documented policies, standards, and procedures may be performed internally, by a risk or compliance function in the institution, or through independent audit. This review often helps to identify problems early so they can be corrected before they become serious.

III.C.2 Personnel

The institution should mitigate risks posed by IT staff by performing appropriate background checks and screening of new staff. The controls in this section also are relevant for third-party provider staff, consultants, and temporary personnel who support the IT function. Typically, the minimum verification considerations should include the following:

¹⁸ Examples of widely accepted industry standards include National Institute of Standards and Technology (NIST) publications, the Control Objectives for Information and Related Technology (COBIT) framework, and the Information Technology Infrastructure Library (ITIL).

- Background checks, including confirmations of prior experience, academic credentials, professional qualifications, or criminal records.¹⁹
- Confirmation of identity from government-issued identification.
- Character references.

The institution should use job descriptions, employment agreements (usually for higher-level or higher-sensitivity positions), training, and awareness programs to promote understanding and increase individual accountability. The job descriptions should detail duties and responsibilities and be routinely updated by managers responsible for the positions with assistance from HR. Management should document and confirm access privileges for each staff member based on his or her job description. Additionally, management should establish a timely process to review, update, and remove access privileges associated with any party when appropriate. The lack of such a process may result in unauthorized or inappropriate activity. Failure to remove access privileges when appropriate, particularly for those individuals with high levels of privilege, represents significant risk.

The institution should protect the confidentiality of information about its customers and organization by having new hires sign agreements covering confidentiality, nondisclosure, and authorized use as a condition of their employment. Employment agreements set both the expectations and limits associated with the staff member's functions. Management should obtain signed confidentiality and nondisclosure agreements before granting new staff members, contractors, and temporary staff access to IT systems. In addition, management should require periodic acknowledgement of acceptable use policies for the network, software applications, Internet, e-mail, confidential data, and social media. Information security awareness and training programs help support information security and other management policies.

III.C.3 Information Security

Financial institutions are critically dependent on their information and technology assets—hardware, software, and data. Management should protect information and technology assets to ensure operational continuity, financial viability, and the trust of customers. The unauthorized loss, destruction, or disclosure of confidential information can adversely affect a financial institution's earnings and capital.

The board of directors is responsible for overseeing the development, implementation, management, and maintenance of the institution's information security program. This oversight includes assigning specific responsibility and accountability for the program's implementation and reviewing reports from management. The board should provide management with guidance, review the effectiveness of management's actions, and annually approval written information

¹⁹ Section 19 of the Federal Deposit Insurance Act prohibits, without the prior written consent of the Federal Deposit Insurance Corporation (FDIC), a person convicted of any criminal offense involving dishonesty or breach of trust or money laundering (covered offenses), or who has agreed to enter into a pretrial diversion or similar program in connection with a prosecution for such offense, from becoming or continuing as an institution-affiliated party, owning or controlling, directly or indirectly an insured depository institution (insured institution), or otherwise participating, directly or indirectly, in the conduct of the affairs of the insured institution, See 12 U.S.C. 1829.

security policies and a written information security program. Key elements that should be addressed in the information security program include the following:

- Central oversight and coordination.
- Areas of responsibility.
- Risk measurement.
- Implementation of controls.
- Monitoring and testing of effectiveness of controls.
- Reporting.
- Acceptable residual risk.

The information security program should be coordinated across the institution. To ensure the effectiveness of the information security program throughout the institution, management should have a process to hold staff accountable for complying with the information security program. Institution management should perform the following:

- Develop and implement processes to identify and protect against security events and incidents.
- Develop, implement, and periodically test incident response procedures, which should address escalation, remediation, and reporting of events and incidents.
- Develop and implement a threat intelligence and collaboration process to identify and respond to information on threats and vulnerabilities.
- Consider information security risks when developing, implementing, or updating products.
- Ensure that products are developed or updated in accordance with established information security policies and procedures.
- Perform penetration tests before launching or making significant changes to critical systems, including Internet- and client-facing applications. Management should review all findings and develop processes to ensure the timely remediation of issues identified by the tests.
- Conduct initial due diligence and ongoing monitoring to fully understand the types of connections and mitigating controls in place between the financial institution and its third-party providers. In conjunction with this, management should require by contract that the third-party providers notify the institution of the use of any subcontractors or changes to subcontractor relationships.²⁰
- Implement a governance process to establish, monitor, maintain, and test controls to mitigate interconnectivity risk.
- Develop a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulator based on thresholds defined by the financial institution and applicable legal requirements. Relevant thresholds could include significant financial impact, significant operational downtime, operational or system breach, or loss of critical infrastructure.

Refer to the *IT Handbook's* "Information Security" booklet for more information.

²⁰ Refer to the *FFIEC IT Handbook's* "[Outsourcing Technology Services](#)" booklet.

III.C.3(a) *Protecting Sensitive Customer Information*

The Information Security Standards require management to develop, and the board to approve, an information security program to protect the security and confidentiality of customer information. This program may be a component of the institution's overall information security program.

The institution should protect customer information from threats to security or integrity. The institution should also protect customer information from unauthorized access or use that would result in substantial harm or inconvenience to any customer. The board should also annually review a written report, prepared by management, regarding the financial institution's actions toward GLBA compliance.

III.C.3(b) *Cybersecurity*

Institutions should take a comprehensive approach to maintain the security and resilience of their IT infrastructure, including the establishment of cybersecurity controls. Although an institution is not required to have a separate cybersecurity policy or program, its information security program should identify, measure, mitigate, monitor, and report on the heightened risks associated with cybersecurity. To address cybersecurity risk, the information security program should consider the following:

- Cyber risk management and oversight.
- Threat intelligence and collaboration.
- Cybersecurity controls.
- External dependency management.
- Cyber incident management and resilience.

Additional information on these topics is available in the FFIEC Cybersecurity Assessment Tool.²¹

III.C.4 *Business Continuity*

The board should approve policies, while senior management should establish and implement policies, procedures, and responsibilities for the enterprise-wide business continuity program. The board should annually approve the institution's business continuity program. Management should document, maintain, and test the plans and backup systems periodically to mitigate the consequences of system interruptions, natural and other disasters, and unauthorized intrusions that could result in the loss, damage, or degradation of data, systems, or services. Management should also provide to the board on an annual basis a written report on the overall status of the business continuity program and the results of testing of the plan and backup systems. Refer to the *IT Handbook's* "Business Continuity Planning" booklet for more information.

²¹ Refer to the [FFIEC Cybersecurity Assessment Tool](#), June 2015. Use of the Cybersecurity Assessment Tool by institutions is optional.

III.C.5 Software Development and Acquisition

Management should assess and mitigate operational risks associated with the development or acquisition of software. Management should develop applicable policies that specify risk management controls for the development and acquisition of systems. Management should guide the development or acquisition of software by using a system development life cycle (SDLC) or similar methodology appropriate for the specific IT environment. The extent or use of the SDLC depends on the size and complexity of the institution and the type of development activities performed. If the institution primarily acquires software, management should verify the effective use of an SDLC by the third-party provider.

Each phase of the SDLC should have procedures that verify the maintenance and integrity of controls before the start of the next phase. When identifying the controls to be implemented in each phase, the institution should incorporate the fundamental principles of confidentiality, integrity, and availability. Audit should review the SDLC to ensure that appropriate controls are incorporated during development. Management should analyze the operational impact early in the process to identify any additional cost and support issues.

Management should test new technology, systems, and products thoroughly before deployment. Testing, which should include tests of security, validates that equipment and systems function properly and produce the desired results. As part of the testing process, management should verify whether new technology systems operate effectively with other technology components, including vendor-supplied technology. Pilot programs or prototypes can be helpful in developing new technology before management accepts the technology for use on a broad scale. Management should conduct retesting periodically to help manage risk exposure on an ongoing basis.

Institutions that outsource the development of software should have a process to review their third-party provider's control environment and capabilities. Institutions often employ structured acquisition methodologies similar to the SDLC when acquiring significant hardware and software products.

Refer to the *IT Handbook's* "Development and Acquisition" booklet for more information.

III.C.6 IT Operations

Management should be aware of and mitigate risks associated with IT operations. The institution and its service providers may have one or more IT operations groups. The number and types vary across institutions. Common examples of IT operations are data center or computer operations, network services, distributed computing, personal or desktop computing, change management, project management, security, resource management, and contingency and resiliency planning.

Many operations functions have significant risk factors that should be addressed through effective management and control. Rapidly evolving threats require an effective monitoring and response program to ensure that vulnerability remediation occurs in a timely manner. Ongoing

business-driven changes to applications should have effective change control programs to ensure that application updates are implemented in a timely manner. The institution should have controls over systems changes, including the following:

- Testing, authorization, and approval.
- Timing of implementation.
- Post-implementation review.
- Rollback or recovery of systems when changes are unsuccessful.

Refer to the *IT Handbook's* "Operations" booklet for more information.

III.C.7 Insurance

The institution may rely on insurance policies as part of a mitigation strategy. Traditional business insurance policies include coverage for errors and omissions, commercial general liability, and directors' and officers' liability policies. Management should understand the institution's insurance needs and the limitations of insurance coverage. These policies generally exclude, or may not include, liability for all areas of IT operations and cybersecurity.

In establishing an insurance program, management should recognize its exposure to loss, the extent to which insurance is available to cover potential losses related to information assets and technology, and the cost of such insurance. The insurance program should be commensurate with the size, complexity, and risk of the institution. Management should weigh these factors to determine how much risk the institution assumes directly. In assessing the extent of that residual risk, the institution should analyze the potential effect of an uninsured loss on itself and any affiliates or parent companies. Management should consider seeking the help of insurance consultants, attorneys, and other professionals, as necessary, to fully identify and measure the risk. Management should also review a company's financial condition or credit rating when deciding on an insurance company.

Management should understand that it cannot insure against all risks. Insurance complements, but does not replace, an effective system of controls. Thus, an overall appraisal of the control environment is important in assessing the adequacy of the insurance program.

Management can insure against risks covered in standard insurance policies. Insurance that covers physical disasters often specifically excludes computer hardware and software. To the extent that policies cover physical storage media, they generally omit the extra cost of reconstructing the recorded information found on the media. Management should clearly understand what is covered and document any gaps in coverage.

Before purchasing insurance, management should assess the costs of obtaining insurance. Estimates of these costs enable management to choose the types and amounts of insurance to carry. These estimates also allow management to determine to what extent the institution may choose to self-insure against certain losses.

Insurance policies provide a variety of coverage for events that could affect an institution's IT. The policies can be adapted to a particular institution's IT environment. The evolving threat environment is contributing to increasing interest in and purchase of insurance related to cyber risks. Insurance companies can provide coverage for items including the cost of conducting an investigation into a breach, notifying customers, crisis management, business interruption, credit monitoring for affected customers, and legal costs. Management should exercise appropriate due diligence in the review of such policies, including policy exclusions to ensure the coverage aligns with management's goals.

As part of the decision to purchase insurance, management should consider the institution's size and complexity and the level and efficacy of controls in place to mitigate risk. Types of insurance may include the following:

- **IT equipment and facilities:** Damage to the information assets and technology throughout the institution. Coverage should include leased equipment if the lessee is responsible for hazard coverage.
- **Media reconstruction:** Damage to IT media, such as magnetic tape and disks, if the institution owns and is liable for the media. Insurance is available for on-premises, off-premises, or in-transit situations. Insurance should cover the actual replacement and reproduction cost of the media or, if reproduction is not possible, the value of the media. Additional considerations to determine the amount of coverage should include programming costs and backup expense.
- **Extra expense:** The extra costs of continuing operations following damage or destruction to the institution's physical location.
- **E-banking activities:** Loss or liability arising from electronic banking activities such as Internet banking, bill payment services, and mobile financial services.
- **Business interruption:** Reimbursement for monetary losses resulting from suspension of operations because of the loss, damage, or degradation of data, systems, or services.
- **Valuable papers and records:** Cost to restore or replace papers and records (not defined as media) in case of direct physical loss or damage.
- **Errors and omissions:** Protection against claims arising from negligent acts, errors, or omissions that occur in performing IT services for others. These policies can contain the following exclusions:
 - Employee dishonesty.
 - Libel, slander, or defamation of character.
 - Liability of others assumed by the insured under contract or agreement.
 - Liability of loss or damage to property of others.
 - Personal or bodily injury or sickness.
 - Liability arising out of advice from third parties on methods, procedures, and practices, etc.
 - Liability for preparation of income tax returns.
 - Loss caused intentionally by, or at the direction of, the insured.

Once management has acquired appropriate insurance coverage, it customarily establishes procedures to review and ensure the adequacy of the coverage. These procedures should include an annual program review by the board of directors.

III.C.8 Third-Party Management

Action Summary

As part of a financial institution's third-party management program, management should ensure that third-party providers effectively provide support by doing the following:

- Negotiating clear and comprehensive contracts with appropriate terms that meet the institution's requirements.
- Ensuring receipt of audited financial statements from third-party providers at least annually.
- Reviewing results of independent audits of IT controls at third-party providers.
- Monitoring the responsiveness of third-party provider's customer service, including client user group support.

Financial institutions increasingly rely on third-party providers and software vendors. Larger or more complex institutions are more likely to have institution-wide third-party management programs that encompass all of these relationships. IT departments can contract with third-party providers for several services, including data processing, software development, equipment maintenance, business continuity, data storage, Internet access, and security management. In smaller or less complex institutions with less formal third-party management programs, the procurement of third-party services should be reviewed by institution staff familiar with the operational, financial, security, and compliance requirements for such relationships. The oversight of the relationship should be performed by staff with knowledge of the services provided.

The board of directors should hold senior management responsible for ensuring appropriate oversight of third-party relationships. Technology needed to support business objectives is often a critical factor in deciding to outsource. Managing such relationships is not just a technology issue; it is an enterprise-wide governance issue. An effective third-party management program should provide the framework for management to identify, measure, mitigate, monitor, and report risks associated with the use of third-party providers. Management should develop and implement enterprise-wide policies and procedures to govern the third-party management program, including establishing objectives and strategies, selecting a provider, negotiating the contract, and monitoring the outsourced relationship.

Management should evaluate the quality of service, control environment, and financial condition of the third parties providing the institution with critical IT services. Third parties can include financial institution affiliates, other financial institutions, and third-party service providers. As

appropriate, these third parties should support the responsibilities of their financial institution clients to adhere to all applicable laws, regulations, and supervisory guidance. Financial institution management should expect third-party support at a level consistent with the criticality of the services provided to the institution. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

When financial institution management contracts with third-party providers for some or all IT services, it should ensure that controls over outsourced activities provide the institution with the same level of assurance as controls over those activities performed in-house. Management should also consider additional oversight or controls over third-party providers that operate in foreign locations. Management should have mitigation strategies that address risks related to foreign-based third-party providers, if applicable. In the event that the financial institution locates any of its own operations offshore and develops third-party relationships at those locations, specific risk mitigation plans should be considered to address related foreign-based third-party risks.

Management should address exposures from third-party risks through an effective third-party management program. Some factors that management should consider or address include the following:

- Assessing whether each third-party relationship supports the institution's overall objectives and strategic plans.
- Evaluating prospective third-party providers based on the scope and importance of the services they provide.
- Tailoring the institution's third-party management program based on an initial and ongoing risk assessment of the institution's third parties and the services they provide.

The time and resources devoted to managing third-party relationships effectively depend on several factors, such as the critical nature of outsourced processes, staff knowledge, and complexity of systems. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information. Additionally, some agencies have specific guidance on third-party relationships and managing third-party relationship risk.²²

Refer to the *IT Handbook's* "Audit" booklet for more information on independent reviews of third-party providers and to the "Business Continuity Planning" booklet, appendix J, "Strengthening the Resilience of Outsourced Technology Services," for guidance focusing on cyber resilience.

²² "Third Party Risk: Guidance for Managing Third Party Risk," FDIC FIL-44-2008, June 6, 2008; OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," October 30, 2013; Federal Reserve Board Supervision and Regulation Letter 13-19 "Guidance on Managing Outsourcing Risk," December 5, 2013.

III.D Monitoring and Reporting

Action Summary

Financial institution management should ensure satisfactory monitoring and reporting of IT activities and risk. These practices should include the following:

- Developing metrics to measure performance, efficiency, and compliance with policy.
- Developing benchmarks for reviewing performance.
- Establishing and reviewing service level agreements (SLA) with critical third-party providers.
- Developing, implementing, and monitoring a process to measure IT compliance with established policies, standards, and practices.
- Evaluating the effectiveness of mitigation strategies and controls.
- Implementing a quality control or quality assurance program to monitor and test systems and applications.
- Implementing timely and effective reporting processes.

Risk monitoring provides information about the effectiveness of risk mitigation activity and should address changing threat conditions in both the financial industry and in organizations that use similar technology. Risk monitoring is ongoing within the lines of business and should include reviews of metrics (e.g., threat intelligence), performance benchmarks, SLAs, and compliance with internal policies. In addition, as part of the monitoring process, institution management should review the effectiveness of controls and ensure that quality assurance and control practices are appropriately included. Management should ensure that there is clear assignment of responsibilities and accountability for both monitoring and escalation procedures. Management should also develop an IT risk reporting process that includes defined reporting channels to ensure accurate, timely, and relevant reporting to appropriate levels of management.

III.D.1 Metrics

Metrics aid management in its ability to assess the overall IT environment. The specific metrics reported, and the frequency with which they are reported, depend on the institution's IT environment. The following are common examples:

- Number of risk issues identified for IT activities (updated regularly to reflect new or mitigated issues). This may include information gathered through the threat intelligence and collaboration process.
- Number of risk acceptance issues approved by senior management. This information may be maintained in a database or other repository of the descriptions, mitigation options, and documentation of management acceptance.

- Number of current and historical events or issues (external and internal events that deviate from the control standards).
- Number of current or outstanding (i.e., unresolved) issues identified by the business unit, internal audit, external audit, or regulator.

Many tools can be used to provide management with metrics to facilitate risk monitoring, such as key risk indicators²³ and key control indicators.²⁴ These are indicators that correlate with changes in risk and control effectiveness. When developed and monitored correctly, metrics can direct management's attention to areas of potential problems.²⁵ As appropriate, certain metrics or summary reports of metrics should be provided to the board.

III.D.2 Performance Benchmarks

Management should periodically review the institution's IT functions and determine whether plans, goals, and expectations are on target. Given the cost of and business reliance on IT functions, failure to perform such monitoring could put an institution at risk. Management should establish performance benchmarks or standards for IT functions and monitor them on a regular basis. Such monitoring can provide assurance that IT functions are meeting the defined benchmarks and can identify potential problem areas. Areas to consider include mainframe and network availability, data center availability, system reruns,²⁶ out-of-balance conditions, response time, error rates, data entry volumes, special requests, and problem reports. Management should evaluate outsourced relationships by measuring performance against SLAs.

III.D.3 Service Level Agreements

The institution should establish formal SLAs with its IT providers, including affiliates and third-party providers. Larger or more complex institutions should consider establishing SLAs for internally provided services, for example, by another division or department of the same institution. SLAs establish mutual expectations and provide a baseline for measuring IT performance. Management can tie SLAs to incentive and penalty actions. SLAs should be comprehensive to provide the institution with a high level of comfort in setting expectations. The use of performance benchmarks and outcome-based measurements could identify potential issues with attaining expectations set in the SLAs.

III.D.4 Policy Compliance

Management should develop, implement, and monitor a process to measure IT compliance with the institution's established policies. In addition to the traditional reliance on internal and third-

²³ A key risk indicator is a measure used to indicate the level of risk associated with an activity.

²⁴ A key control indicator is a metric that indicates the potential for a control to fail within an organization.

²⁵ Refer to the "Metrics" section of the *IT Handbook's* "Information Security" booklet for more information.

²⁶ A system rerun is a method of correcting an error that occurs during processing. An entire job or selection of jobs may have to be rerun to correct the error.

party audit functions, the institution should perform periodic self-assessments. The scope and frequency of self-assessments depend on the scale and historical performance of the IT function. Self-assessments provide management with an understanding of whether the institution is in compliance with the policies approved by the board.

III.D.5 Effectiveness of Controls

Control testing should include the effectiveness of control design and implementation and take into account the changing nature of the threats and the enforcement of control functions. Management should monitor risk mitigation activities and controls to ensure that identified risks are appropriately mitigated. Monitoring of the effectiveness of controls should be ongoing, and departments should provide periodic progress reports to management. Ongoing monitoring ensures that the risk management process is not a one-time or annual event.

III.D.6 Quality Assurance and Quality Control

Quality assurance (QA) is a process intended to ensure that a product or service under development meets specified requirements. Management should oversee the establishment of a QA process and update future planning with the results. QA may include internal performance measures, focus groups, and customer surveys. Management should assess whether QA testing is conducted on new or updated systems before implementation. Testing should be independent of any programming function and should incorporate user acceptance testing programs. The thorough QA testing of a new system can identify vulnerabilities or poor functionality.

Quality control (QC) is a procedure intended to ensure that a product or application adheres to a defined set of quality criteria that meet the requirements of the end user. QC includes activities that can be used to identify weaknesses or vulnerabilities in work products and to avoid the resource drain and expense of repeating a task. The traditional goal of QC activities is to ensure that a product conforms to specifications and is fit to use. QC helps to determine the following about a product:

- Whether the product works.
- Whether the product does what it is designed to do.
- Whether the product is fit for use.

QA and QC reports are valuable tools for management and help document the control process for the production environment.

III.D.7 Reporting

Management should develop an IT risk reporting process that assembles and reports IT risk information in a manner that is timely, complete, transparent, and relevant to management decisions. IT management should provide periodic reports based on risk to senior management or the board as well as to necessary stakeholders. Recipients of IT risk reports should have the authority and responsibility to act on the reported information, provide a credible challenge for information contained in the reports, and be held accountable for the outcomes. The reporting

should be appropriate to the decisions the individual reviewing the report is responsible for influencing. This reporting should be defined in accordance with the institution's enterprise-wide risk management program. Additionally, reporting should trigger appropriate, timely, and reliable escalation procedures.

Appendix A: Examination Procedures

Examination Objective

Examiners should use these procedures to determine the quality and effectiveness of the institution's management of IT. Examiners should also use these procedures to measure the adequacy of the institution's ITRM process, including management awareness and participation, risk assessment, policies and procedures, reporting, ongoing monitoring, and follow-up.

These examination procedures (also known as the work program) are intended to assist examiners in determining the effectiveness of the institution's IT management process. Examiners may choose, however, to use only particular work steps of the following examination procedures based on the size, complexity, and nature of the institution's business. Examiners should use these procedures to measure the adequacy of the institution's cybersecurity risk management processes.

Objective 1: Determine the appropriate scope and objectives for the examination.

1. Review past reports for outstanding issues or previous problems. Consider the following:
 - a. Regulatory reports of examination.
 - b. Internal and external audit reports.
 - c. Internal or independent tests or reviews of controls (e.g., penetration tests, business continuity reviews, and third-party management reviews).
 - d. Regulatory and audit reports on service providers.
2. Review management's response to issues raised during, or since, the last examination. Consider the following:
 - a. Adequacy and timing of corrective action.
 - b. Resolution of root causes rather than just specific issues.
 - c. Existence of any outstanding issues.
 - d. Whether management has taken positive action toward correcting exceptions reported in audit and examination reports.
 - e. Independent review of resolution and reporting of resolution to the audit committee.
3. Interview management and review responses to pre-examination information requests to identify changes to the technology infrastructure or new products and services that might increase the institution's risk. Consider the following:
 - a. Products or services delivered to either internal or external users.
 - b. Current network diagrams and data flow diagrams, including changes to configuration or components.
 - c. Hardware and software inventories.
 - d. Loss or addition of key personnel.
 - e. Inventories of third-party providers and software vendors.

- f. Organizational charts that include reporting relationships between business units and control functions (e.g., enterprise risk management, ITRM, and internal audit).
- g. Credit or operating losses primarily attributable (or thought to be attributable) to IT (e.g., system problems, inadequate controls, improperly implemented changes to systems, and fraud resulting from cybersecurity attacks, such as account takeover).
- h. Changes to internal business processes.
- i. Internal reorganizations.

Objective 2: Determine whether the board of directors oversees and senior management appropriately establishes an effective governance structure that includes oversight of IT activities.

1. Review the institution's governance structure to determine the oversight of IT activities and verify that it includes the following:
 - a. Board sets the tone and direction for the institution's use of technology.
 - b. IT risks are adequately identified, measured, and mitigated.
 - c. Board approval of the information security program and other IT-related policies.
 - d. Board members are familiar with IT activities.
2. Review the activities performed by the board or a committee of the board to determine the effectiveness of IT oversight. Specifically, review whether the board or a committee of the board appropriately does the following:
 - a. Reviews and approves an IT strategic plan that aligns with the overall business strategy and includes an information security strategy to safeguard against ongoing and emerging threats, including cybersecurity threats.
 - b. Oversees the institution's adoption of effective IT governance processes.
 - c. Oversees management processes for approving third-party providers that include an assessment of financial condition and IT security posture of the third party, including on cybersecurity.
 - d. Has an oversight process that includes receiving updates on major projects, IT budgets, IT priorities, and overall IT performance; and has an approval process for critical projects and activities.
 - e. Reviews the adequacy and allocation of IT resources in terms of funding and personnel.
 - f. Approves a policy to escalate and report significant security incidents to the board, steering committee, government agencies, and law enforcement, as appropriate.
 - g. Holds management accountable for the identification, measurement, and mitigation of IT risks.
 - h. Provides for independent, comprehensive, and effective audit coverage of the IT program.
3. Determine whether the board does the following:
 - a. Delegates monitoring for specific IT activities, as appropriate, to a steering committee.
 - b. Provides a credible challenge to management decisions.

- c. Receives regular reports regarding operations.
 - d. Directs management to maintain an institution-wide view of technology and the business processes supported by technology.
4. Review the membership list of board, steering committee, and/or relevant management committees established to review IT activities. Determine whether board, senior management, lines of business, audit, and IT personnel are represented appropriately, and whether regular meetings are held and minutes are maintained.
5. Review the minutes of the board of directors and relevant committee meetings for evidence of board support and supervision of IT activities.
6. If the board delegates certain activities regarding the oversight of IT to a committee, review the membership, responsibilities, and activities of the committee. Specifically, determine whether the committee does the following:
 - a. Maintains a charter that defines its responsibilities.
 - b. Has a defined mission to assist the board in IT oversight.
 - c. Has decision-making authority.
 - d. Receives appropriate management information from IT, lines of business, and external sources.
 - e. Coordinates and monitors IT resources.
 - f. Determines whether there is adequate training, including cybersecurity training, for institution staff.
 - g. Reports to the board on the status of IT activities to enable the board to make decisions.
 - h. Receives reports on IT to remain informed on risk.
 - i. Is responsible for effective strategic IT planning, oversight of IT performance, and aligning IT with business needs.
7. Review the board of directors and management oversight program for IT. Determine whether the board has effective oversight of IT. Determine whether the board oversees and management implements the following:
 - a. Processes and procedures that meet objectives of governing IT policies.
 - b. Appropriate policies for information security, including cybersecurity risk management processes, and other relevant IT policies.
 - c. Policies that result in compliance with applicable regulatory requirements.
 - d. Controls over risks associated with system development and acquisition.
 - e. Process for business continuity planning.
8. Review IT management and determine whether management performs the following:
 - a. Implements effective IT governance and IT risk management processes, including those that relate to cybersecurity.
 - b. Reviews, understands, approves, and provides for at least annual reviews of ITRM processes.

- c. Assesses the institution's inherent IT risks across lines of business and ensures IT risks are included in enterprise-wide risk assessments.
 - d. Provides regular reports to the board on IT risks, IT strategies, and IT changes.
 - e. Coordinates priorities between the IT department and lines of business.
 - f. Establishes a formal process to obtain, analyze, and respond to information on threats and vulnerabilities by developing a repeatable threat intelligence and collaboration program.
 - g. Ensures that hiring and training practices are governed by appropriate policies to maintain competent and trained staff.
9. Review the roles and responsibilities of all levels of management, including executive management, CIO or CTO, CISO, IT line management, and IT business unit management, to ensure that there is a clear delineation between management and oversight functions and operational duties.
10. Review the corporate and IT departmental organization charts to determine whether they show the following:
 - a. IT management reports directly to senior management, with appropriate reporting directly to the board, as needed.
 - b. The IT department's responsibilities are appropriately segregated from business processing activities.
11. Review the institution's structure to determine whether the board established the following:
 - a. The organizational structure provides for effective IT support throughout the institution, from IT management up through senior management and the board.
 - b. Defined roles and responsibilities for key IT positions, including executive management (CEO and COO, and often CIO or CTO), and CISO.
 - c. An appropriate and effective executive management team or positions, such as CEO and COO, to assist in the oversight and management of IT.
 - d. A defined and functioning role for the CIO or CTO to focus on strategic IT issues and the overall effectiveness of the IT function.
 - e. A CISO or information security officer position responsible for the management and mitigation of information security risks.
 - f. Involvement of frontline management in the IT oversight process.
 - g. Integration of business line managers into the IT oversight process.
12. Determine whether the reporting structure ensures that the CISO has the appropriate authority to carry out its responsibilities and that there are no conflicts of interest in the ability of the CISO to make decisions in line with the risk appetite.
13. Determine management's need for, or effectiveness in, selecting and implementing appropriate EA and assess whether the EA program serves the institution's needs, complexity, and future technology plans.

Objective 3: *As part of the ITRM structure, determine whether financial institution management has defined IT responsibilities and functions. Verify the existence of well-defined responsibilities and expectations between risk management and IT functional areas, such as information security, project management, business continuity, and information systems reporting.*

1. Review the institution's established lines of authority for enforcing and monitoring controls.
2. Determine whether management has a board-approved written information security program and verify that it is maintained and updated according to regulatory requirements.
3. Determine whether the institution has a project management function appropriate for the complexity of the institution, and verify that this function contains the appropriate elements.
4. Determine whether the institution maintains an adequate and up-to-date enterprise-wide business continuity plan. Determine whether the board oversees implementation and approves policies related to business continuity planning.
5. Determine whether the institution has a well-defined role for the implementation and use of information systems reporting and that it produces accurate and useful reports. Determine the effectiveness of the reports used by senior management or relevant management committees to supervise and monitor the following IT functions:
 - a. Management reports that provide the status of software development and maintenance activities.
 - b. Performance and problem reports prepared by internal user groups.
 - c. System use and planning reports prepared by operating managers.
 - d. Internal and external audit reports of IT activities.
6. Review information systems reports for management, and determine whether they provide the information necessary to help manage the institution effectively. Determine the following:
 - a. The information systems reports facilitate the management of the business.
 - b. The process and results are effective.
 - c. Data and information provided to the board and senior management allow them to make strategic decisions.
 - d. The information systems reports provide key risk and performance trends, indicators, and performance against risk tolerances.
 - e. The institution has effective controls procedures in place to ensure that information is correct and relevant.
 - f. The systems and reporting meet the five elements of effective reporting: timeliness, accuracy, consistency, completeness, and relevance.
 - g. The information systems reports are appropriate for the size and complexity of the institution.

Objective 4: *Determine the adequacy of the institution's IT operations planning and investment. Assess the adequacy of the risk assessment and the overall alignment with the institution's business strategy, including planning for IT resources and budgeting.*

1. Determine whether the board oversees and management considers the following when formulating the institution's overall business strategy:
 - a. Risk assessment, priority, and mitigation across the institution.
 - b. IT strategic plans.
 - c. Major projects in process or planned.
 - d. Third-party relationships, including the third party's current and future plans (e.g., changes in strategy and products offered) and service or security issues that may affect the institution.
 - e. Staffing levels sufficient to complete tasks as scheduled.
 - f. IT operating costs.
 - g. IT contingency planning and business recovery.
2. Review the strategic plan for IT activities. Determine whether the goals and objectives are consistent with the institution's overall business strategy. Document significant changes made since the previous examination that affect (or any planned changes that may affect) the institution's organizational structure, hardware or software configuration, and overall operational goals. Determine the following:
 - a. Business needs are realistic.
 - b. IT has the ability to meet business needs.
 - c. The plan addresses long-term (three- to five-year horizon) goals and allocation of resources.
 - d. The plan incorporates the entire IT environment.
 - e. The plan lists strategic initiatives and considers all necessary factors around those initiatives.
 - f. The plan includes tactical plans to achieve strategic goals.
 - g. The plan explains trends and issues of potential impact.
 - h. The plan incorporates clearly defined goals and metrics.
 - i. The planning process adjusts for new or changing risks.
 - j. IT Management participates in the development of the IT strategic plan.
 - k. There is review of and credible challenge to the plan.
3. Determine whether the institution has adequate tactical and operational IT plans to support the larger IT strategic plan.
4. Determine whether the board or board committee reviews and approves the following:
 - a. Information security risk assessment, including cybersecurity.
 - b. Short- and long-term IT tactical, operational, and strategic plans.
 - c. Resource allocation (e.g., major hardware or software acquisition and project priorities).
 - d. Reported status of major projects.

- e. IT budgets and current operating cost and the allocation of IT resources.
5. Determine the effectiveness of management's process to fund IT resources to meet the current operational needs of the institution. Assess whether management considers the following IT resources:
 - a. Infrastructure.
 - b. Hardware.
 - c. Operating software.
 - d. Application software.
 - e. Personnel.
6. Determine whether the board reviews management's budget plans. Determine the effectiveness of the budget process to estimate and control the institution's activities.
7. If the institution uses third-party providers, determine whether management:
 - a. Verifies that the third-party providers can continue to support current contract requirements and future changes (e.g., that the third party has a satisfactory financial condition).
 - b. Has a process to assess whether a third party's actions may negatively affect the institution (e.g., a review of the third-party plans to continue offering the necessary products or services contracted by the institution).
 - c. Has an effective ongoing monitoring process of its third-party providers.

Objective 5: Along with the IT audit and compliance departments, the HR department can serve as an influencing function for IT. Determine the adequacy of the institution's HR function to ensure its ability to attract and retain a competent workforce.

1. Determine the institution's ability to attract and retain a competent workforce and the ability of HR management to effectively meet the requirements for IT and the lines of business that IT supports.
2. Identify key IT positions, review biographical data (e.g., résumés and training and development records), and determine the following:
 - a. Job descriptions are reasonable and represent actual practice.
 - b. Employees have appropriate qualifications.
 - c. Staffing levels are appropriate.
 - a. There are provisions for management succession that provide for an acceptable transition in the event of the loss of a key IT manager or staff member.
 - b. Backup personnel are identified and trained.
3. Review and evaluate written job descriptions to ensure that management performs the following:

- a. Clearly defines the authority, responsibility, and technical skills required.
 - b. Maintains updated job descriptions in writing.
4. Determine whether the HR function has processes for compensation planning, performance reviews, knowledge transfer mechanisms, training, and mentoring.
5. Determine whether the financial institution has a process to ensure that staff has the requisite expertise to fulfill its roles. Review the adequacy of the process.
6. Determine the adequacy of the institution's training programs. Determine whether the institution has or supports the following:
 - a. Internal or external training programs.
 - b. Certification programs.
 - c. Training processes that support the goals and objectives of the institution.
7. Review turnover rates of IT staff and discuss staffing and retention issues with IT management, or review turnover rates of IT management and discuss with senior management. Identify root causes of any staffing or expertise shortages, including compensation plans or other retention practices.
8. If IT staff members have duties in other departments, determine the following:
 - a. Management is aware of the potential conflicts such duties may cause.
 - b. Conflicting duties are subject to appropriate supervision and compensating controls.

Objective 6: Evaluate management's review and oversight of IT controls, including the other influencing functions of IT audit and compliance.

1. Consult with the examiner reviewing audit or IT audit to determine the adequacy of IT audit coverage and management's responsiveness to identified weaknesses.
2. Determine whether the board provides for the necessary expertise in the audit department and that audit coverage is comprehensive, timely, and independent. Assess whether the board requires audit reporting directly to the board or a designated committee.
3. Determine whether the board, or its committee, has appropriate oversight of audit through the following:
 - a. Audit risk assessment and audit plan.
 - b. Audit review activities.
 - c. Audit reports with identified weaknesses.
 - d. Management's responses and corrective actions to audit issues.
 - e. Updates on any audit concerns and the status of issues.

4. Determine whether the board, or a board committee, is responsible for overseeing performance and compensation for the audit department.
5. Determine whether the compliance function has involvement in the institution's review oversight process, and assess the adequacy of its involvement.
6. Determine whether compliance staff reviews new products, systems, applications, or changes to evaluate compliance with applicable laws and regulations.

Objective 7: Determine whether the institution's risk management program facilitates effective risk identification and measurement and provides support for risk decisions within ITRM.

1. Determine whether the institution has a risk management program and whether the program includes an integrated approach for enterprise-wide risk management, including identification, measurement, mitigation, monitoring, and reporting of risk. If applicable, determine whether the structure conforms to regulatory requirements.
2. Determine the effectiveness of the risk management program by reviewing whether it receives appropriate direction and support from the board and senior management.
3. Determine the following:
 - a. The board of directors has defined its risk appetite and the institution's risk tolerance levels.
 - b. The board of directors has applied sufficient resources to achieve its risk appetite and remain within the institution's risk tolerance levels.
 - c. Management has committed to support the board's risk decisions.
4. Determine whether the institution maintains a risk assessment process to perform the following:
 - a. Identify risks and threats from both internal and external sources.
 - b. Develop or update policies within the risk management function to guide risk measurement activities.
 - c. Ensure the existence of a process to promote sound understanding and analysis of threats, events, assets, and controls.
 - d. Maintain processes within the risk management function to help make risk mitigation decisions.
 - e. Determine the entities that should have involvement in that decision-making process.
 - f. Ensure that the board and management understand the risk categories.

Objective 8: Determine whether the board of directors oversees and senior management proactively mitigates operational risk.

1. Review the institution's management of operational risk, and verify that the risk management process includes aspects of operational risk across the institution, including the following:
 - a. Back-office operations and transaction processing.
 - b. Customer service.
 - c. Systems development and support.
 - d. Internal controls and processes.
 - e. Capacity planning.
2. Determine whether the institution's management of operational risk incorporates an enterprise-wide view of IT and business processes that are supported by technology.
3. Assess whether IT management maintains an active role in the institution's strategic planning to align IT with established business goals and strategies. Assess whether effective IT controls exist throughout the institution, either through direct oversight or by holding lines of business accountable for IT-related controls.
4. Determine whether IT management participates in the enterprise-wide risk management process to identify and measure risk from the use of IT, support decisions on how to mitigate the risks, implement the mitigation decisions, and monitor and report on the resulting outcomes.

Objective 9: Determine whether management implements an ITRM process that supports the overall enterprise-wide risk management process.

1. Review the role of IT management in the risk management process and identify whether it is supportive and collaborative to the overall process.
2. Determine whether the ITRM process includes the following:
 - a. A risk identification process to identify risks to information assets within the institution and information assets controlled by third-party providers.
 - b. A risk measurement process using an evidence-based approach to measure the level of risk and determine if it is in line with the board's risk appetite.
 - c. A risk mitigation process to ensure that management mitigates the risks to an acceptable residual risk level.
 - d. A risk monitoring and reporting process to monitor changing risk levels and report the results of the process to the board and senior management.
3. Determine whether the ITRM process includes the following:
 - a. Is regularly updated with a frequency appropriate for the pace of change.
 - b. Aligns IT and business objectives.

- c. Has formality appropriate to the complexity of the institution.
- d. Considers the overall IT environment, regardless of the design and management of the IT environment.

Objective 10: Determine whether the institution maintains a risk identification process that is coordinated and consistent across the enterprise.

1. Determine whether the institution has a comprehensive IT risk identification process that includes the identification of cybersecurity risks. Specifically, determine whether management performs the following:
 - a. Maintains an inventory of assets, event classes, threats, and existing controls.
 - b. Participates in an information sharing forum (such as FS-ISAC).
 - c. Has a process to identify internal and external threats.
 - d. Considers existing controls—including governance of controls, their limitations, and their effectiveness—in a comprehensive control assessment.
 - e. Has a risk identification process that is formal yet flexible enough to adapt to changes in the IT environment.
 - f. Incorporates a measurement and assessment of outsourced relationships in the risk identification process.
 - g. Considers the information security risk assessments completed in accordance with the Information Security Standards in management oversight of IT operations.
2. Determine whether the institution's risk identification process includes the ongoing collection of information on the IT environment, including the following:
 - a. IT systems inventories.
 - b. IT strategic plans.
 - c. Interconnectivity documentation.
 - d. Information flow diagrams.
 - e. Business continuity and disaster recovery plans.
 - f. Third-party management program.
 - g. Call center data.
 - h. Department self-assessments.
 - i. IT audit findings.
 - j. Threat intelligence information.

Objective 11: Determine whether institution management maintains a risk measurement process that is coordinated and consistent across the enterprise.

1. Determine whether management's risk measurement process includes the determination of risk factors (such as adverse events, threats, and controls) and the affected assets. Determine whether management develops inventories of those risk factors. Specifically, determine whether management does the following in the risk measurement process:
 - a. Identifies reasonable threats to financial institution assets.

- b. Performs a threat analysis.
 - c. Estimates the probability of occurrence of adverse events.
 - d. Determines the potential impacts of events and threats, internal and external.
 - e. Analyzes the institution's technical and organizational vulnerabilities.
 - f. Measures risk through qualitative, quantitative, or hybrid measurement approaches.
 - g. Measures and assesses risks posed by third-party relationships.
 - h. Considers the information security risk assessments completed in accordance with the Information Security Standards in management oversight of IT operations.
 - i. Risk ranks information assets according to a rigorous and consistent methodology.
2. Determine whether the risk measurement process is comprehensive and includes the following types of risks that affect the institution:
 - a. Security breaches.
 - b. System failures.
 - c. External or insider events.
 - d. Development and acquisition issues.
 - e. Capacity planning issues.
 - f. Third-party provider issues.
 3. Identify whether the institution has a proactive process in place to effectively update its measurement of risk before implementing system changes, rolling out new products or services, or confronting new external conditions.

Objective 12: Determine whether financial institution management effectively implements satisfactory risk mitigation practices.

1. Determine whether the institution has processes within enterprise-wide risk management to assist IT management in making risk mitigation decisions, and determine which entities should be involved in the decision-making process.
2. Determine whether management has adequate methods and tools, including control self-assessments and scenario analysis, to evaluate controls for effectiveness against identified threats.
3. Determine whether the ITRM process addresses risks with an effective IT control structure in the institution's IT environment and through conformance with external legal and regulatory requirements.
4. Determine whether IT management has developed adequate policies, standards, and procedures to manage the risk from technology and that they are current, documented, and appropriately communicated. Policies, standards, and procedures should address the following:
 - a. Risk assessment.
 - b. Personnel administration.

- c. Development and acquisition, including secure development.
 - d. Computer operations.
 - e. Third-party risk management.
 - f. Computer and information security, including cybersecurity.
 - g. Business continuity and resilience planning.
 - h. IT audit.
5. Determine whether management has effective hiring and training practices that include the following:
 - a. Performing appropriate background checks on new staff, contractors, and third-party provider personnel, as necessary.
 - b. Confirming identity.
 - c. Obtaining character references.
 - d. Requiring periodic acknowledgement of acceptable-use policies.
 - e. Obtaining signed confidentiality and nondisclosure agreements.
 - f. Providing information security awareness and training programs.
6. Determine whether the board has appropriate oversight and management has appropriate responsibility for the implementation of the institution's information security program.
7. For the information security program, verify that the board is responsible for the following:
 - a. Overseeing the development, implementation, and maintenance of the program.
 - b. Assigning specific responsibility for its implementation.
 - c. Providing management with guidance and reviewing the effectiveness of management's actions.
 - d. Annually reviewing and approving a formal, written information security program.
 - e. Overseeing management steps to safeguard the information assets of the bank and its customers.
 - f. Annually reviewing management's report on the status of the bank's actions to achieve or maintain compliance with the Information Security Standards.
8. Determine whether, as part of the institution's information security program, the board of directors oversees and management establishes a control structure that is intended to specifically address cybersecurity risks and includes the following:
 - a. Developing and implementing processes to identify, protect against, detect, respond to, and recover from security events and incidents.
 - b. Developing, implementing, and periodically testing incident response procedures.
 - c. Using a threat intelligence and collaboration process to identify and respond to information on threats and vulnerabilities.
 - d. Including information security risks when developing, implementing, or updating products.
 - e. Assigning "business owner" responsibility in product development or update processes.

- f. Performing penetration tests before launching new or making significant changes to existing Internet- and client-facing applications and remediating findings from the tests.
 - g. Conducting initial due diligence and ongoing monitoring to fully understand the connections and mitigating controls in place between the financial institution and its third-party providers.
 - h. Implementing a governance process to establish, monitor, maintain, and test controls to mitigate interconnectivity risk.
 - i. Developing a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulators based on thresholds defined by the financial institution.
9. Determine whether the board of directors approved policies and management established and implemented policies, procedures, and responsibilities for an enterprise-wide business continuity program, including the following:
 - a. Annual review and approval of the business continuity program by the board of directors.
 - b. Management responsibility to document, maintain, and test the plan and backup systems periodically according to risk.
 - c. Annual reports by management of the results of the business continuity and disaster recovery tests to the board of directors.
10. Determine whether management assesses and mitigates the operational risks associated with the development or acquisition of software. Appropriate management of the risks should include the following:
 - a. Policies documenting risk management controls for the development and acquisition of systems.
 - b. System development life cycle or similar methodology based on the complexity and type of development performed.
 - c. Tests of new technology, systems, and products before deployment to validate functionality, controls, and interoperability.
 - d. Penetration tests of new or updated applications, particularly for Internet- or client-facing applications, to detect and correct security flaws.
11. Review major acquisitions of hardware and software to determine if the acquisitions are within the limits approved by the board of directors.
12. Determine whether management is aware of and mitigates operational risks associated with IT operations, including the following:
 - a. Data center or computer operations.
 - b. Network services.
 - c. Distributed computing.
 - d. Desktop computing.
 - e. Change management.
 - f. Project management.

- g. Security.
 - h. Resource management.
 - i. Contingency and resiliency planning.
13. Review the financial institution's insurance program and determine whether it is commensurate with the size, complexity, risks, and mitigation strategy of the institution. Determine the adequacy of insurance coverage (if applicable) for the following:
- a. Employee fidelity.
 - b. IT equipment and facilities.
 - c. Media reconstruction.
 - d. Extra expenses, including backup site expenses.
 - e. E-banking activities.
 - f. Business interruption.
 - g. Valuable papers and records.
 - h. Errors and omissions.
 - i. Items in transit.
 - j. Other probable risks (unique or specific risks for a particular institution).
14. Review the financial institution's third-party management program to ascertain the extent and effectiveness of the oversight by the board of directors and management of risks involved in the financial institution's outsourced relationships. An effective third-party management program should incorporate the following:
- a. A framework for management to identify, measure, mitigate, and monitor the risks associated with third-party relationships.
 - b. Board oversight and senior management development and implementation of enterprise-wide policies to govern the third-party management program.
 - c. A review process of third-party providers to ensure that each relationship supports the institution's overall business objectives and strategic plans.
 - d. Evaluation of prospective third-party providers based on the scope and criticality of services provided.
 - e. Tailoring of the monitoring program based on the initial and ongoing risk assessment of the third party and the services provided.
15. As part of the examiner's review of the institution's third-party management program, analyze the third party's financial condition and note any potential weaknesses, including measures to improve those weaknesses.
16. When reviewing information provided by the institution's third-party providers, determine whether the third-party provider enables adequate financial institution client access to relevant information. Consider the following:
- a. The third party's method of communication with financial institution clients.
 - b. Timeliness of third-party reporting to financial institution clients.
 - c. Quality of financial information, as determined by internal or external auditor reports.

17. When reviewing information provided by the institution's third-party providers, determine the adequacy of third-party provider audit reports in terms of scope, independence, expertise, frequency, and corrective actions taken on identified issues. Work with the examiner reviewing the third-party management program to determine its adequacy.
18. When reviewing information provided by the institution's third-party providers, determine the quality of management's follow-up and resolution of customer concerns and problems with its third-party providers.

Objective 13: Determine whether IT management develops satisfactory measures for defining and monitoring metrics, performance benchmarks, service level agreements, compliance with policies, effectiveness of controls, and quality assurance and control. Determine whether management developed satisfactory reporting of ITRM activities.

1. Determine whether management develops and uses metrics to help assess the overall IT environment. Determine whether the metrics used and the frequency and monitoring of those metrics are useful to direct management's attention to emerging issues. Additionally, determine whether necessary metrics or summary reports of metrics are provided to the board.
2. Determine whether there are established performance benchmarks and standards for the IT function and whether they serve to help management identify problem areas, particularly in system or data center availability, operating conditions, response times, and error rates.
3. Review whether the institution has formal service level agreements with all of its third-party providers. Determine whether the agreements provide the institution with assurance of continued service.
4. Determine the effectiveness of management's communication and monitoring of IT policy compliance across the institution.
5. Determine whether management has an adequate method of testing the effectiveness of control design and implementation and whether management and the board appropriately monitor risk mitigation activities. Determine whether management considers all forms of controls, including governance of controls, their limitations, and their effectiveness in a comprehensive control assessment.
6. Determine whether management has QA and QC procedures defined for significant IT activities and whether those procedures are performed internally or externally. Specifically, review whether management:
 - a. Has a process to assist it in determining whether products or services meet specified requirements (QA).
 - b. Has procedures to ensure that a product or application adheres to a defined set of quality criteria to meet end-user requirements (QC),

- c. Performs tests associated with QA and QC independent of the programming function, and whether the QA and QC procedures incorporate user acceptance testing programs.
 - d. Receives effective reports on the results of QA and QC testing.
- 7. Review the monitoring and reporting specific to the institution's ITRM activities. Specifically, determine whether the institution has developed the following:
 - a. A process to adequately identify and monitor relevant external threats and vulnerabilities.
 - b. Effective risk monitoring that provides tangible feedback on the quality of the implementation of controls and risk mitigation strategies.
 - c. A reporting process that assembles and reports IT risk-related information in a timely, complete, transparent, and relevant manner.
 - d. Appropriate escalation procedures in place depending on the content of the reporting.

Objective 14: Discuss corrective action and communicate findings.

- 1. Review preliminary conclusions with the examiner-in-charge (EIC) regarding:
 - a. Violations of laws and regulations.
 - b. Significant issues warranting inclusion as matters requiring attention or recommendations in the report of examination.
 - c. Proposed Uniform Rating System for Information Technology management component rating and the potential impact of the examiner's conclusions on composite or other component IT ratings.
 - d. Potential impact of the examiner's conclusions on the institution's risk assessment.
- 2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.
- 3. Document conclusions in a memorandum to the EIC that provides report-ready comments for all relevant sections of the report of examination and guidance to future examiners.
- 4. Organize work papers to ensure clear support for significant findings by examination objective.

Appendix B: Glossary

Access: The ability to physically or logically enter or make use of an IT system or area (secured or unsecured). The process of interacting with a system.

Administrator privileges: Computer system access to resources that are unavailable to most users. Administrator privileges permit execution of actions that would otherwise be restricted.

Agility: In IT systems, the ability to rapidly incorporate new technologies or changes to technologies allowing an organization to adapt to changing business needs.

Application development: The process of designing and building code to create a computer program (software) used for a particular type of job.

Benchmark: A standard, or point of reference, against which things may be compared or assessed.

Confidentiality: Assuring that information will be kept secret, with access limited to appropriate persons.

Control self-assessment: A technique used to internally assess the effectiveness of risk management and control processes.

Corrective control: A mitigating technique designed to lessen the impact to the institution when adverse events occur.

Cyber attack: An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an institution for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cybersecurity: The process of protecting consumer and bank information by preventing, detecting, and responding to attacks.

Data center: A facility that houses an institution's most important information systems components, including computer systems, telecommunications components, and storage systems.

Detective control: A mitigating technique designed to recognize an event and alert management when events occur.

Disaster recovery: The process of recovering from major processing interruptions.

Due diligence: Technical, functional, and financial review to verify a service provider's ability to deliver the requirements specified in its proposal. The intent is to verify that the service

provider has a well-developed plan and adequate resources and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

Enterprise Architecture: The overall design and high-level plan that describes an institution's operational framework and includes the institution's mission, stakeholders, business and customers, work flow and processes, data processing, access, security, and availability.

Enterprise-wide: Across an entire organization, rather than a single business department or function.

External connections: An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

Financial Services Information Sharing and Analysis Center (FS-ISAC): A nonprofit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information.

Gramm–Leach–Bliley Act: The Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999 (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999), required the Federal banking agencies to establish information security standards for financial institutions.

Incident management: The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible.

Information security: The process by which an organization protects the creation, collection, storage, use, transmission, and disposal of information.

Information systems: Electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information systems can include networks (computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems). Other examples are backup tapes, mobile devices, and other media.

Information technology: Any services or equipment, or interconnected system(s) or subsystem(s) of equipment that comprise the institution's IT architecture or infrastructure. It can include computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources.

Infrastructure: Describes what has been implemented by IT architecture and often include support facilities such as power, cooling, ventilation, server and data redundancy and resilience, and telecommunications lines. Specific architecture types may exist for the following: enterprise, data (information), technology, security, and application.

Interconnectivity: The state or quality of being connected together. The interaction of a financial institution's internal and external systems and applications and the entities with which they are linked.

Interdependencies: Where two or more departments, processes, functions, and/or third parties affect or support one another.

Internet: A worldwide network of computer networks, governed by standards and protocols developed by the Internet Engineering Task Force (IETF).

Interoperability: The ability of a system to work with or use the parts or equipment of another system.

IT architecture: A subset of enterprise architecture, with detail to support data processing and access, including fundamental requirements for centralized or distributed computing, real or virtual servers, devices and workstations, and networking design. Architecture plans may also exist for data (information), security, and applications.

IT governance: An integral part of governance that consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

IT strategic plan: A comprehensive blueprint that guides the organization's technology management and contains high-level goals and plans for all areas of information technology that affect the business, not just the infrastructure. The plan should include areas that impact technology management, including cost management, human capital management, hardware and software management, third-party management, risk management, and all other considerations in the enterprise IT environment.

IT system inventory: A list containing information about the information resources owned or operated by an organization.

Malware: Software designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs.

Metric: A quantitative measurement.

Milestone: Major project event.

Mobile device: A portable computing and communications device with information-storage capability. Examples include notebook and laptop computers, cellular telephones and smart phones, tablets, digital cameras, and audio recording devices.

Mobile financial services: A financial institution's use of mobile devices to provide products and services to its customers.

National Institute of Standards and Technology (NIST): An agency of the U.S. Department of Commerce that works to develop and apply technology, measurements, and standards. NIST developed a voluntary cybersecurity framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructures.

Network: Two or more computer systems that are connected to share information, software, and hardware.

Operating system: A system that supports and manages software applications. Operating systems allocate system resources, provide access and security controls, maintain file systems, and manage communications between end users and hardware devices.

Operational IT plan: Typically, the plans that are made by front-line, or low-level, IT managers. Operational IT plans are focused on the specific procedures and processes that implement the larger strategic plan.

Operational risk: The risk of failure or loss resulting from inadequate or failed processes, people, or systems.

Penetration test: The process of using approved, qualified personnel to conduct real-world attacks against a system to identify and correct security weaknesses before they are discovered and exploited by others.

Preventive control: A mitigating technique designed to prevent an event from occurring.

Principle of least privilege: The security objective of granting users only the access needed to perform official duties.

Project: A task involving the acquisition, development, or maintenance of a technology product.

Project management: Planning, monitoring, and controlling an activity.

Residual risk: The amount of risk remaining after the implementation of controls.

Resilience: The ability of an institution to recover from a significant disruption and resume critical operations.

Risk: The potential that events, expected or unanticipated, may have an adverse effect on a financial institution's earnings or capital.

Risk identification: The process of determining risks and existing safeguards. It generally includes inventories of systems and information necessary to operations and defines the potential threats to systems and operations.

Risk management: The total process required to identify, control, and minimize the impact of uncertain events. The objective of a risk management program is to reduce risk and obtain and maintain appropriate management approval at pre-defined stages in the life cycle.

Risk measurement: A process of determining the likelihood of an adverse event or threat occurring and the potential impact of such an event on the institution. The result of risk measurement is the prioritization of potential risks based on severity and likelihood of occurrence.

Risk mitigation: The process of reducing risks through the introduction of specific controls and risk transfer. It includes the implementation of appropriate controls to reduce the potential for risk and bring the level of risk in line with the board's risk appetite.

Scenario analysis: The process of analyzing possible future events by considering alternative possible outcomes.

Scorecard: A dashboard of performance measures.

Security breach: A security event that results in unauthorized access of data, applications, services, networks, or devices by bypassing underlying security mechanisms.

Security event: An event that potentially compromises the confidentiality, integrity, availability, or accountability of an information system.

Security posture: The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, and policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

Sensitive customer information: A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as user name and password or password and account number.

Service level agreement (SLA): Formal documents between an institution and its third-party provider that outline an institution's predetermined requirements for a service and establish

incentives to meet, or penalties for failure to meet, the requirements. SLAs should specify and clarify performance expectations, establish accountability, and detail remedies or consequences if performance or service quality standards are not met.

Social engineering: A general term for trying to trick people into revealing confidential information or performing certain actions.

Systems administration: The process of maintaining, configuring, and operating computer systems.

Tactical plan: Typically, a short-term plan that establishes the specific steps needed to implement a company's strategic plan.

Telecommunications: The exchange of information over significant distances by electronic means.

Third-party provider: Any type of company, including affiliated entities, nonaffiliated entities, and alliances of companies providing products and services to a financial institution. Other terms used to describe service providers include subcontractors, external service providers, application service providers, and outsourcers. Also called a third-party service provider.

Third-party relationship: Any business arrangement between a financial institution and another entity, by contract or otherwise.

Threat intelligence: The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision-making.

Total cost of ownership (TCO): The true cost of ownership of a computer or other technology system that includes: original cost of the computer and software; hardware and software upgrades; maintenance; technical support; and training.

Virus: Malicious code that replicates itself within a computer.

Vulnerability: A hardware, firmware, or software flaw that leaves an information system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to information or to disrupt critical processing.

Appendix C: References

Laws

- 12 USC 1464(d), Home Owners' Loan Act
- 12 USC 1867(c), Bank Service Company Act
- 12 USC 1882, Bank Protection Act
- 15 USC 6801 and 6805(b), Gramm–Leach–Bliley Act
- 18 USC 1030, Computer Fraud and Abuse Act

Federal Reserve

Regulations

- 12 CFR 208, appendix D-2, “Interagency Guidelines Establishing Information Security Standards”
- 12 CFR 211.5 and 211.24 (i), Protection of Customer and Consumer Information
- 12 CFR 225, appendix F, “Interagency Guidelines Establishing Information Security Standards”

Guidance

- SR Letter 13-19, “Guidance on Managing Outsourcing Risk” (December 5, 2013)
- SR Letter 11-9, “Interagency Supplement to Authentication in an Internet Banking Environment” (June 29, 2011)
- SR Letter 05-23, “Unauthorized Access to Customer Information” (December 1, 2005)
- SR Letter 05-19, “Interagency Guidance on Authentication in an Internet Banking Environment” (October 13, 2005)
- SR Letter 01-15, “Standards for Safeguarding Customer Information” (May 31, 2001)
- SR Letter 00-17, “Guidance on the Risk Management of Outsourced Technology Services” (November 30, 2000)
- SR Letter 99-8, “Uniform Rating System for Information Technology” (March 31, 1999)
- SR Letter 98-9, “Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations” (April 20, 1998)

Federal Deposit Insurance Corporation

Regulations

- 12 CFR 364, appendix A, “Interagency Guidelines Establishing Standards for Safety and Soundness”
- 12 CFR 364, appendix B, “Interagency Guidelines Establishing Information Security Standards”

Guidance

FIL-13-2015, “FFIEC Joint Statements on Destructive Malware and Compromised Credentials” (March 30, 2015)
FIL-21-2014, “Webinar on Senior Management’s Role in Cybersecurity” (April 25, 2014)
FIL-11-2014, “Distributed Denial of Service Attacks” (April 2, 2014)
FIL-13-2014, “Technology Outsourcing Information Tools for Community Bankers” (April 7, 2014)
FIL-46-2012, “Supervision of Technology Service Providers and Outsourcing Technology Services” (November 6, 2012)
FIL-44-2008, “Third Party Risk: Guidance for Managing Third Party Risk” (June 6, 2008)
FIL-6-2008, “Interagency Statement on Pandemic Planning: Guidance for Minimizing a Pandemic’s Potential Adverse Effect” (February 6, 2008)
FIL-52-2006, “Foreign-Based Third Party Service Providers: Guidance on Managing Risks in These Outsourcing Relationships” (June 21, 2006)
FIL-25-2006, “Influenza Pandemic: Interagency Advisory” (March 15, 2006)
FIL-121-2004, “Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance” (November 16, 2004)
FIL-103-2004, “Interagency Information Brochure on Internet Phishing Scams” (Sept 13, 2004)
FIL-43-2003, “Computer Software Patch Management” (May 29, 2003)
FIL-50-2001, “Bank Technology Bulletin on Outsourcing” (June 4, 2001)
FIL-49-99, “Required Notification for Compliance with the Bank Service Company Act” (June 3, 1999)

National Credit Union Administration

Regulations

12 CFR 721, “Federal Credit Union Incidental Powers Activities”
12 CFR 748, “Security Program, Report of Crime and Catastrophic Act, Bank Secrecy Act Compliance,” and appendix A, “Guidelines for Safeguarding Member Information”
12 CFR 741, “Requirements for Insurance”
12 CFR 740, “Advertising”

Guidance

NCUA Letter to Credit Unions 02–CU–17, “E-Commerce Guide for Credit Unions” (December 2002)
NCUA Letter to Credit Unions 01–CU–20, “Due Diligence Over Third–Party Service Providers” (November 2001)
NCUA Letter to Credit Unions 00–CU–11, “Risk Management of Outsourced Technology Services (with Enclosure)” (December 2000)

Office of the Comptroller of the Currency

Regulations

- 12 CFR 30, appendix A, “Interagency Guidelines Establishing Standards for Safety and Soundness”
- 12 CFR 30, appendix B, “Interagency Guidelines Establishing Information Security Standards”

Guidance

- OCC Bulletin 2015–20, “Cybersecurity: Destructive Malware Joint Statement” (March 30, 2015)
- OCC Bulletin 2015–19, “Cybersecurity: Cyber Attacks Compromising Credentials Joint Statement” (March 30, 2015)
- OCC Bulletin 2015–9, “FFIEC Information Technology Examination Handbook: Strengthening the Resilience of Outsourced Technology Services, New Appendix for Business Continuity Planning Booklet” (February 6, 2015)
- OCC Bulletin 2014-45, “Heightened Standards for Large Banks; Integration of 12 CFR 30 and 12 CFR 170: Final Rules and Guidelines”
- OCC Bulletin 2014–53, “Cybersecurity: Cybersecurity Assessment General Observations and Statement” (November 3, 2014)
- OCC Bulletin 2013–29, “Third-Party Relationships: Risk Management Guidance” (October 30, 2013)
- OCC Bulletin 2006–26, “Disaster Planning: Hurricane Katrina—Lessons Learned” (June 15, 2006)
- OCC Bulletin 2006–12, “Influenza Pandemic: Interagency Advisory” (March 15, 2006)
- OCC Bulletin 2004–47, “FFIEC Guidance: Risk Management for the Use of Free and Open Source Software” (October 27, 2004)
- OCC Bulletin 2003–14, “Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System” (April 8, 2003)
- OCC Bulletin 1998–3, “Technology Risk Management: Guidance for Bankers and Examiners” (February 4, 1998)

Other References

- FDIC FIL-28-2015 “Cybersecurity Assessment Tool” (July 2, 2015)
- SR Letter 15-9, “FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors” (July 2, 2015)
- OCC Bulletin 2015-31, “FFIEC Cybersecurity Assessment Tool” (June 30, 2015)
- Basel Committee on Banking Supervision, “[Sound Practices for the Management and Supervision of Operational Risk](#)” (February 2003)
- [ISACA](#) Control Objectives for Enterprise IT Governance (CoBIT)



Federal Financial Institutions Examination Council

FFIEC

Outsourcing
Technology Services

OT

June 2004

IT EXAMINATION

Handbook

Table of Contents

Introduction	1
Board and Management Responsibilities	2
Risk Management	3
Risk Assessment and Requirements	4
Quantity of Risk Considerations	5
Requirements Definition	6
Service Provider Selection	9
Request for Proposal	9
Due Diligence	10
Contract Issues	11
Service Level Agreements (SLAs)	15
Pricing Methods	15
Bundling	16
Contract Inducement Concerns	16
Ongoing Monitoring	18
Key Service Level Agreements and Contract Provisions	18
Financial Condition of Service Providers	19
General Control Environment of the Service Provider	20
Potential Changes due to the External Environment	21
Related Topics	22
Business Continuity Planning	22
Outsourcing the Business Continuity Function	23
Information Security/Safeguarding	25
Multiple Service Provider Relationships	25
Outsourcing to Foreign Service Providers	26
Appendix A: Examination Procedures	A-29
Appendix B: Laws, Regulations, and Guidance	B-1

Appendix C: Foreign-Based Third-Party Service Providers	C-1
Appendix D: Managed Security Service Providers	D-1

Introduction

The financial services industry has changed rapidly and dramatically. Advances in technology enable institutions to provide customers with an array of products, services, and delivery channels. One result of these changes is that financial institutions increasingly rely on external service providers for a variety of technology-related services. Generally, the term "outsourcing" is used to describe these types of arrangements.

The Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) "Outsourcing Technology Services Booklet" (booklet) provides guidance and examination procedures to assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships.

The ability to contract for technology services typically enables an institution to offer its customers enhanced services without the various expenses involved in owning the required technology or maintaining the human capital required to deploy and operate it. In many situations, outsourcing offers the institution a cost effective alternative to in-house capabilities. Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines that use it. Risks such as loss of funds, loss of competitive advantage, improper disclosure of information, and regulatory action remain. Because the functions are performed by an organization outside the financial institution, the risks may be realized in a different manner than if the functions were inside the financial institution resulting in the need for controls designed to monitor such risks.

Financial institutions can outsource many areas of operations, including all or part of any service, process, or system operation. Examples of information technology (IT) operations frequently outsourced by institutions and addressed in this booklet include: the origination, processing, and settlement of payments and financial transactions; information processing related to customer account creation and maintenance; as well as other information and transaction processing activities that support critical banking functions, such as loan processing, deposit processing, fiduciary and trading activities; security monitoring and testing; system development and maintenance; network operations; help desk operations; and call centers. The booklet addresses an institution's responsibility to manage the risks associated with these outsourced IT services.

Management may choose to outsource operations for various reasons. These include:

- Gain operational or financial efficiencies;
- Increase management focus on core business functions;
- Refocus limited internal resources on core functions;
- Obtain specialized expertise;
- Increase availability of services;
- Accelerate delivery of products or services through new delivery channels;

- Increase ability to acquire and support current technology and avoid obsolescence; and
- Conserve capital for other business ventures.

Outsourcing of technology-related services may improve quality, reduce costs, strengthen controls, and achieve any of the objectives listed previously. Ultimately, the decision to outsource should fit into the institution's overall strategic plan and corporate objectives.

Before considering the outsourcing of significant functions, an institution's directors and senior management should ensure such actions are consistent with their strategic plans and should evaluate proposals against well-developed acceptance criteria. The degree of oversight and review of outsourced activities will depend on the criticality of the service, process, or system to the institution's operation.

Financial institutions should have a comprehensive outsourcing risk management process to govern their technology service provider (TSP) relationships. The process should include risk assessment, selection of service providers, contract review, and monitoring of service providers. Outsourced relationships should be subject to the same risk management, security, privacy, and other policies that would be expected if the financial institution were conducting the activities in-house. This booklet primarily focuses on how the bank regulatory agencies review the risk management process employed by a financial institution when considering or executing an outsourcing relationship.

To help ensure financial institutions operate in a safe and sound manner, the services performed by TSPs are subject to regulation and examination. ^[1] The federal financial regulators have the statutory authority to supervise all of the activities and records of the financial institution whether performed or maintained by the institution or by a third party on or off of the premises of the financial institution. Accordingly, the examination and supervision of a financial institution should not be hindered by a transfer of the institution's records to another organization or by having another organization carry out all or part of the financial institution's functions. ^[2]

Many of the general principles on effective management of outsourcing relationships discussed in this booklet can and should be applied to managing the outsourcing of software development. Outsourcing of activities related to software development is addressed in the IT Handbook's, "Development and Acquisition Booklet."

This booklet rescinds and replaces Chapter 22 of the 1996 FFIEC Information Systems Examination Handbook, IS Servicing - Provider and Receiver.

Board and Management Responsibilities

Action Summary

The financial institution's board and senior management should establish and

approve risk-based policies to govern the outsourcing process. The policies should recognize the risk to the institution from outsourcing relationships and should be appropriate to the size and complexity of the institution.

The responsibility for properly overseeing outsourced relationships lies with the institution's board of directors and senior management. Although the technology needed to support business objectives is often a critical factor in deciding to outsource, managing such relationships is more than just a technology issue; it is an enterprise-wide corporate management issue. An effective outsourcing oversight program should provide the framework for management to identify, measure, monitor, and control the risks associated with outsourcing. The board and senior management should develop and implement enterprise-wide policies to govern the outsourcing process consistently. These policies should address outsourced relationships from an end-to-end perspective, including establishing servicing requirements and strategies; selecting a provider; negotiating the contract; and monitoring, changing, and discontinuing the outsourced relationship.

Factors institutions should consider include:

- Ensuring each outsourcing relationship supports the institution's overall requirements and strategic plans;
- Ensuring the institution has sufficient expertise to oversee and manage the relationship;
- Evaluating prospective providers based on the scope and criticality of outsourced services;
- Tailoring the enterprise-wide, service provider monitoring program based on initial and ongoing risk assessments of outsourced services; and
- Notifying its primary regulator regarding outsourced relationships, when required by that regulator. ^[3]

The time and resources devoted to managing outsourcing relationships should be based on the risk the relationship presents to the institution. To illustrate, outsourcing processing of a small credit card portfolio will require a different level of oversight than outsourcing processing of all loan applications. Additionally, smaller and less complex institutions may have less flexibility than larger institutions in negotiating for services that meet their specific needs and in monitoring their service providers.

Risk Management

Risk management is the process of identifying, measuring, monitoring, and managing risk. Risk exists whether the institution maintains information and technology services internally or elects to outsource them. Regardless of which alternative they choose, management is responsible for managing risk in all outsourcing relationships. Accordingly, institutions should establish and maintain an effective risk management process for initiating and overseeing all outsourced operations.

An effective risk management process involves several key factors:

- Establishing senior management and board awareness of the risks associated with outsourcing agreements in order to ensure effective risk management practices;
- Ensuring that an outsourcing arrangement is prudent from a risk perspective and consistent with the business objectives of the institution;
- Systematically assessing needs while establishing risk-based requirements;
- Implementing effective controls to address identified risks;
- Performing ongoing monitoring to identify and evaluate changes in risk from the initial assessment; and
- Documenting procedures, roles/responsibilities, and reporting mechanisms.

Typically, this process incorporates the following activities:

- Risk assessment and requirements definition;
- Due diligence in selecting a service provider;
- Contract negotiation and implementation; and
- Ongoing monitoring.

The preceding comments focus on risk elements specifically associated with outsourcing. For a broader perspective on IT transactional and operational risk, refer to the IT Handbook's "Supervision of Technology Service Providers (TSP) Booklet," which addresses outsourcing risk from the service provider perspective.

Risk Assessment and Requirements

<i>Action Summary</i>

Management should:

- Assess the risk from outsourcing;
- Involve stakeholders in creating risk-based written requirements to control an outsourcing action; and
- Use the written requirements to guide and manage the remainder of the outsourcing process.

Outsourced IT services can contribute to operational risks (also referred to as transaction risks). Operational risk may arise from fraud, error, or the inability to deliver products or services, maintain a competitive position, or manage information. It exists in each process involved in the delivery of the financial institutions' products or services. Operational risk not only includes operations and transaction processing, but also areas such as customer service, systems development and support, internal control processes, and capacity and contingency planning. Operational risk also may affect other risks such as interest rate, compliance, liquidity, price, or strategic risk as described below.

- Strategic risk - Inadequate management experience and expertise can lead to a lack of understanding and control of key risks. Additionally, inaccurate information from TSPs can cause the management of serviced financial institutions to make poor strategic decisions.
- Compliance (legal) risk - Outsourced activities that fail to comply with legal or regulatory requirements can subject the institution to legal sanctions. For example, inaccurate or untimely consumer compliance disclosures or unauthorized disclosure of confidential customer information could expose the institution to civil money penalties or litigation. TSPs often agree to comply with banking regulations, but their failure to track regulatory changes could increase compliance risk for their serviced financial institutions.
- Interest rate, liquidity, and price (market) risk - Processing errors related to investment income or repayment assumptions could lead to unwise investment or liquidity decisions thereby increasing market risks.

Quantity of Risk Considerations

The quantity of risk associated with an outsourced IT service is subject to the function outsourced, the service provider, and the technology used by the service provider. Management should consider the following factors in evaluating the quantity of risk at the inception of an outsourcing decision.

- Risks pertaining to the function outsourced include:
 - Sensitivity of data accessed, protected, or controlled by the service provider;
 - Volume of transactions; and
 - Criticality to the financial institution's business.

- Risks pertaining to the service provider include:
 - Strength of financial condition;
 - Turnover of management and employees;
 - Ability to maintain business continuity;
 - Ability to provide accurate, relevant, and timely Management Information Systems (MIS);
 - Experience with the function outsourced;
 - Reliance on subcontractors;
 - Location, particularly if cross-border (See Appendix C, Foreign-Based Third-Party Service Providers); and
 - Redundancy and reliability of communication lines.
- Risks pertaining to the technology used include:
 - Reliability;
 - Security; and
 - Scalability to accommodate growth.

Requirements Definition

The definition of business requirements sets the stage for all outsourcing actions and forms the basis for subsequent management of the outsourced activity. The requirements are developed through a process that identifies the functions or activities to be outsourced, assesses the risk of outsourcing those functions or activities, and establishes a baseline from which appropriate control measures can be identified. These requirements provide a basis for an understanding between the financial institution and the service provider as to what the risks are and how they will be managed and controlled.

Key Practices

Sound practices for the development of requirements include:

- **Stakeholder involvement**-All organizational groups who will be directly involved with the service provider or in using the contracted service should be represented in the development of product and service requirements.
- **Integration**-The development should result in requirements that support the subsequent steps of solicitation, selection, contracting, and monitoring.
- **Documentation**-Documentation will greatly assist in ensuring that the service contracted and delivered meets the institution's requirements. Documentation will also allow for subsequent reviews of the processes' adequacy and integrity.

Components

The requirements definition phase should result in a detailed document containing descriptions of the institution's expectations relative to the outsourced service. The requirements document may consider, but is not limited by, the following high level topical components:

- Scope and nature
 - Service description;
 - Technology; and
 - Customer support.
- Standards and service levels
 - Availability and performance;
 - Change management;
 - Financial reporting;
 - Quality of service;
 - Security; and
 - Business continuity.
- Minimum acceptable service provider characteristics
 - Industry experience;
 - Management experience;
 - Technology and systems architecture;
 - Process controls;
 - Financial condition;
 - Degree of reliance on third parties, subcontractors, or partners;
 - Legal, regulatory, and compliance history; and
 - Ability to meet future needs.
- Monitoring and reporting
 - Measurements and reporting criteria;
 - Right to audit;
 - Third-party reports; and
 - Coordination of responses to security events.
- Transition requirements
 - Initial migration of data to the service provider;

- Implementation of necessary communications mechanisms;
- Migration of data from the service provider at termination of contract; and
- Staff training.
- Contract duration, termination, and assignment
 - Start and term;
 - Conditions and right to cancel;
 - Ownership of data;
 - Timely return of data in machine-readable format;
 - Costs of transition;
 - Limitations, as appropriate, governing assignment to third party;
 - Dispute resolution; and
 - Confidentiality of institution data.
- Contractual protections against liability
 - Indemnification;
 - Limitation of liability; and
 - Insurance.

When outsourcing to a subsidiary or affiliate is considered, management must assure that the components outlined above evidence an arms-length transaction. An arrangement between a financial institution and an affiliate or subsidiary should be on terms that are substantially the same, or at least as favorable to the institution, as those prevailing at the time for comparable transactions with a non-affiliated third party.

Service Provider Selection

Action Summary

Management should:

- Evaluate service provider proposals in light of the institution's needs, including any differences between the institution's solicitation and the service provider proposal;
- Perform due diligence on the prospective service providers;
- Ensure that selection of affiliated parties as service providers is done at arms length in accordance with regulations and guidance issued by the institution's primary regulator; and
- Evaluate foreign-based third-party service providers in light of the guidance found in this section and in Appendix C, Foreign-Based Third-Party Service Providers.

After identifying the work to be performed and the necessary controls, a financial institution solicits responses from prospective service providers. The primary tool for the solicitation is the Request for Proposal (RFP). The RFP also supports subsequent contract negotiations.

Request for Proposal

A financial institution should generate the RFP from the information developed during the requirements definition phase. While the level of detail may vary for any particular procurement, the RFP should describe the institution's objectives; the scope and nature of the work to be performed; the expected production service levels, delivery timelines, measurement requirements, and control measures; and the financial institution's policies for security, business continuity, and change control. It also requests responses addressing those requirements as well as the fees each service provider will charge.

Once management distributes the RFPs and receives responses, it should evaluate the service provider proposals against the institution's needs. When the institution evaluates the proposals, it may find that the proposals do not completely agree with the RFP. For example, the service the service provider proposes may include different processing workflows or reporting schemes, pricing formulas or techniques, or the response to information requests may not be complete. If the institution considers proposals that differ from the RFP, the institution should evaluate the differences against its requirements and clearly understand how the changes will affect the institution's objectives and service expectations. The institution should evaluate material differences using a process similar to the one used to develop the requirements initially. An institution should negotiate a resolution to any differences between the RFP and the service provider proposal before contracting with a service provider.

Due Diligence

A financial institution should perform due diligence on the service provider's response to an RFP as well as the service provider itself. Due diligence should serve as a verification and analysis tool, providing assurance that the service provider meets the institution's needs. Due diligence should confirm and assess the following information regarding the service provider:

- Existence and corporate history;
- Qualifications and backgrounds of company principals, including criminal background checks where appropriate;
- Other companies using similar services from the provider that may be contacted for reference;
- Financial status, including reviews of audited financial statements;
- Strategy, service delivery capability, status, and effectiveness;
- Technology and systems architecture;
- Internal controls environment, security history, and audit coverage;
- Legal and regulatory compliance including any complaints, litigation, or regulatory actions;
- Reliance on and success in dealing with third party service providers;
- Insurance coverage; and
- Ability to meet disaster recovery and business continuity requirements.

Other important elements include probing for information on intangibles, such as the third party's service philosophies, quality initiatives, and management style. The culture, values, and business styles should fit those of the financial institution. When a foreign-based service provider is considered, the evaluation should assess the relationship in light of the above items as well as the information discussed in Appendix C, Foreign-Based Third-Party Service Providers.

Financial institutions may perform due diligence on one or more of the service providers that respond to the RFP. The depth and formality of the due diligence performed may vary according to the risk of the outsourced relationship, the institution's familiarity with the prospective service providers, and the stage of the provider selection process.

Once institutions issue RFPs, receive and evaluate responses, and perform due diligence, they enter into contract negotiations with one or more of the service providers they have determined can best meet their needs.

Contract Issues

Action Summary

Before signing a contract, management should:

- Ensure the contract clearly defines the rights and responsibilities of both parties;
- Ensure the contract contains adequate and measurable service level agreements;
- Ensure contracts with affiliates clearly reflect an arms-length relationship and costs and services are at least as favorable to the institution as those available from a non-affiliated provider;
- Choose the most appropriate pricing method for the financial institution's needs;
- Ensure the contract does not contain provisions or inducements that may have a significant, adverse affect on the institution;
- Engage legal counsel to review the contract; and
- Evaluate foreign-based third-party service providers in light of the guidance found in this section and in Appendix C, Foreign-Based Third-Party Service Providers.

After selecting a service provider, management should negotiate a contract that meets their requirements. The RFP and the service provider's response can be used as inputs to this process. The contract is the legally binding document that defines all aspects of the servicing relationship. A written contract should be present in all servicing relationships. This includes instances where the service provider is affiliated with the institution. When contracting with an affiliate, the institution should ensure the costs and quality of services provided are commensurate with those of a nonaffiliated provider. The contract is the single most important control in the outsourcing process. Because of the importance of the contract, management should:

- Verify the accuracy of the description of the outsourcing relationship in the contract;
- Ensure the contract is clearly written and contains sufficient detail to define the rights and responsibilities of each party comprehensively; and
- Engage legal counsel early in the process to help prepare and review the proposed contract.

Examples of contract elements that should be considered include:

Scope of Service. The contract should clearly describe the rights and responsibilities of the parties to the contract. Considerations should include:

- Descriptions of required activities, timeframes for their implementation, and assignment of responsibilities. Implementation provisions should take into consideration other existing systems or interrelated systems to be developed by different service providers (e.g., an Internet banking system being integrated with existing core applications or systems customization);
- Obligations of, and services to be performed by, the service provider including software support and maintenance, training of employees, or customer service;
- Obligations of the financial institution;
- The contracting parties' rights in modifying existing services performed under the contract; and
- Guidelines for adding new or different services and for contract re-negotiation.

Performance Standards. Institutions should include performance standards that define minimum service level requirements and remedies for failure to meet standards in the contract. For example, common service level metrics include percent system uptime, deadlines for completing batch processing, or number of processing errors. Industry standards for service levels may provide a reference point. The institution should periodically review overall performance standards to ensure consistency with its goals and objectives. Also see the Service Level Agreements section in this booklet.

Security and Confidentiality. The contract should address the service provider's responsibility for security and confidentiality of the institution's resources (e.g., information, hardware). ^[4] The agreement should prohibit the service provider and its agents from using or disclosing the institution's information, except as necessary to or consistent with providing the contracted services, and to protect against unauthorized use (e.g., disclosure of information to institution competitors). If the service provider receives nonpublic personal information regarding the institution's customers, the institution should verify that the service provider complies with all applicable requirements of the privacy regulations. Institutions should require the service provider to fully disclose breaches in security resulting in unauthorized intrusions into the service provider that may materially affect the institution or its customers. The service provider should report to the institution when intrusions occur, the effect on the institution, and corrective action to respond to the intrusion, based on agreements between both parties.

Controls. Management should consider implementing contract provisions that address the following controls:

- Service provider internal controls;
 - Compliance with applicable regulatory requirements;
 - Record maintenance requirements for the service provider;
 - Access to the records by the institution;
 - Notification requirements and approval rights for any material changes to services, systems, controls, key project personnel, and service locations;
 - Setting and monitoring parameters for financial functions including payments processing or extensions of credit on behalf of the institution; and
 - Insurance coverage maintained by the service provider.
-

Audit. The institution should include in the contract the types of audit reports it is entitled to receive (e.g., financial, internal control, and security reviews). The contract should specify the audit frequency, any charges for obtaining the audits, as well as the rights of the institution and its regulatory agencies to obtain the results of the audits in a timely manner. The contract may also specify rights to obtain documentation of the resolution of any deficiencies and to inspect the processing facilities and operating practices of the service provider. Management should consider, based upon the risk assessment phase, if it can rely on internal audits or if there is a need for external audits and reviews.

For services involving access to open networks, such as Internet-related services, management should pay special attention to security. The institution should consider including contract terms requiring periodic control reviews performed by an independent party with sufficient expertise. These reviews may include penetration testing, intrusion detection, reviews of firewall configuration, and other independent control reviews. The institution should receive sufficiently detailed reports on the findings of these ongoing audits to assess security adequately without compromising the service provider's security.

Reports. Contractual terms should include the frequency and type of reports the institution will receive (e.g., performance reports, control audits, financial statements, security, and business resumption testing reports). The contracts should also outline the guidelines and fees for obtaining custom reports.

Business Resumption and Contingency Plans. The contract should address the service provider's responsibility for backup and record protection, including equipment, program and data files, and maintenance of disaster recovery and contingency plans. The contracts should outline the service provider's responsibility to test the plans regularly and provide the results to the institution. The institution should consider interdependencies among service providers when determining business resumption testing requirements. The service provider should provide the institution a copy of the contingency plan that outlines the required operating procedures in the event of business disruption. Contracts should include specific provisions for business recovery timeframes that meet the institution's business requirements. The institution should ensure that the contract does not contain any provisions that would excuse the service provider from implementing its contingency plans.

Sub-contracting and Multiple Service Provider Relationships. Some service providers may contract with third parties in providing services to the financial institution. Institutions should be aware of and approve all subcontractors. To provide accountability, the financial institution should designate the primary contracting service provider in the contract. The contract should also specify that the primary contracting service provider is responsible for the services outlined in the contract regardless of which entity actually conducts the operations. The institution should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors.

Cost. The contract should fully describe the calculation of fees for base services, including any development, conversion, and recurring services, as well as any charges based upon volume of activity or for special requests. Contracts should also address the responsibility and additional cost for purchasing and maintaining hardware and software. Any conditions under which the cost structure may be changed should be addressed in detail including limits on any cost increases. Also see the Pricing Methods and Bundling sections in this booklet.

Ownership and License. The contract should address the ownership, rights to, and allowable use of the institution's data, equipment/hardware, system documentation, system and application software, and other intellectual property rights. Ownership of the institution's data must rest clearly with the institution. Other intellectual property rights may include the institution's name and logo, its trademark or copyrighted material, domain names, web sites designs, and other work products developed by the service provider for the institution. Additional information regarding the development of customized software to support outsourced services can be found in the IT Handbook's "Development and Acquisition Booklet."

Duration. Institutions should consider the type of technology and current state of the industry when negotiating the appropriate length of the contract and its renewal periods. While there can be benefits to long-term technology contracts, certain technologies may be subject to rapid change and a shorter-term contract may prove beneficial. Similarly, institutions should consider the appropriate length of time required to notify the service provider of the institutions' intent not to renew the contract prior to expiration. Institutions should consider coordinating the expiration dates of contracts for inter-related services (e.g., web site, telecommunications, programming, network support) so that they coincide, where practical. Such coordination can minimize the risk of terminating a contract early and incurring penalties as a result of necessary termination of another related service contract.

Dispute Resolution. The institution should consider including a provision for a dispute resolution process that attempts to resolve problems in an expeditious manner as well as a provision for continuation of services during the dispute resolution period.

Indemnification. Indemnification provisions should require the service provider to hold the financial institution harmless from liability for the negligence of the service provider. Legal counsel should review these provisions to ensure the institution will not be held liable for claims arising as a result of the negligence of the service provider.

Limitation of Liability. Some service provider standard contracts may contain clauses limiting the amount of liability that can be incurred by the service provider. If the institution is considering such a contract, management should assess whether the damage limitation bears an adequate relationship to the amount of loss the financial institution might reasonably experience as a result of the service provider's failure to perform its obligations.

Termination. Management should assess the timeliness and expense of contract termination provisions. The extent and flexibility of termination rights can vary depending upon the service. Institutions should consider including termination rights for a variety of conditions including change in control (e.g., acquisitions and mergers), convenience, substantial increase in cost, repeated failure to meet service levels, failure to provide critical services, bankruptcy, company closure, and insolvency. The contract should establish notification and timeframe requirements and provide for the timely return of the institution's data and resources in a machine readable format upon termination. Any costs associated with conversion assistance should also be clearly stated.

Assignment. The institution should consider contract provisions that prohibit assignment of the contract to a third party without the institution's consent. Assignment provisions should also reflect notification requirements for any changes to material subcontractors.

Foreign-based service providers. Institutions entering into contracts with foreign-based service providers should consider a number of additional contract issues and provisions. See Appendix C included in this booklet.

Regulatory Compliance. Financial institutions should ensure that contracts with service providers include an agreement that the service provider and its services will comply with

applicable regulatory guidance and requirements. The provision should also indicate that the service provider agrees to provide accurate information and timely access to the appropriate regulatory agencies based on the type and level of service it provides to the financial institution.

Service Level Agreements (SLAs)

Service level agreements are formal documents that outline the institution's pre-determined requirements for the service and establish incentives to meet, or penalties for failure to meet, the requirements. Financial institutions should link SLAs to provisions in the contract regarding incentives, penalties, and contract cancellation in order to protect themselves against service provider performance failures.

Management should develop SLAs by first identifying the significant elements of the service. The elements can be related to tasks (i.e., processing error rates, system up-time, etc.) or they can be organizational (i.e., employee turnover). Once it has identified the elements, management should devise ways to measure the performance of those elements objectively. Finally, institutions should determine the frequency of the measurements and an acceptable range of results to determine when a service provider violates the SLA benchmarks.

Although the specific performance standards may vary with the nature of the service delivered, management should consider SLAs to address the following issues:

- Availability and timeliness of services;
- Confidentiality and integrity of data;
- Change control;
- Security standards compliance, including vulnerability and penetration management;
- Business continuity compliance; and
- Help desk support.

SLAs addressing business continuity should measure the service provider's or vendor's contractual responsibility for backup, record retention, data protection, and the maintenance of disaster recovery and contingency plans. The SLAs can also test the contingency plan's provisions for business recovery timeframes or conducting periodic tests of the plan. Neither contracts nor SLAs should contain any extraordinary provisions that would excuse the vendor or service provider from implementing its contingency plans (outsourcing contracts should include clauses that discuss unforeseen events for which the institution would not be able to adequately prepare).

Pricing Methods

Financial institutions should have several choices when it comes to pricing an outsourcing venture. Management should consider all available pricing options and choose the most appropriate for the specific contract. Examples of different pricing methods include:

- Cost plus-The service provider receives payment for its actual costs, plus a

predetermined profit margin or markup (usually percentage of actual costs). For example, the service provider builds a website at a cost of \$5,000 plus a 10% markup; the institution pays \$5,500.

- Fixed price-The service provider price is the same for each billing cycle for the entire contract period. The advantage of this approach is that institutions know exactly what the provider will bill each month. Problems may arise if the institution does not adequately define the scope or the process. Often, with the fixed price method, the service provider labels services beyond the defined scope as additional or premium

services. For example, if a service provider bills an institution \$500 per month for maintaining a website, and the institution decides it wants to add another link, the service provider may charge more for that service if it is not clearly defined in the original contract.

- Unit pricing-The service provider sets a rate for a particular level of service, and the institution pays based on usage. For example, if an institution pays \$.10 per hit on a website, and the site has 5,000 hits for the month, the institution pays \$500 for the month.
- Variable pricing-The service provider establishes the price of the service based on a variable such as system availability. For example, the provider bills the institution \$500, \$600, or \$800 per month for service levels of 99.00, 99.50, or 99.75 percent system availability, respectively. If a website was available 99.80 percent of the time in a billing period, the institution would pay \$800.
- Incentive-based pricing-Incentives encourage the service provider to perform at peak level by offering a bonus if the provider performs well. This plan can also require the provider to pay a penalty for not performing at an acceptable level. For example, the institution wants a service provider to build a website. The service provider agrees to do so within 90 days for \$5,000. The institution offers the provider \$6,500 if the website is ready within 45 days, but states that it will only pay \$3,500 if the provider fails to meet its 90 day deadline.
- Future price changes-Service providers typically include a provision that will increase costs in the future either by a specified percentage or per unit. Some institutions may also identify circumstances under which price reductions might be warranted (i.e., reduction in equipment costs).

Bundling

The provider may entice the institution to purchase more than one system, process, or service for a single price - referred to as "bundling." This practice may result in the institution getting a single consolidated bill that may not provide information relating to pricing for each specific system, process, or service. Although the bundled services may appear to be cheaper, the institution cannot analyze the costs of the individual services. Bundles may include processes and services that the institution does not want or need. It also may not allow the institution to discontinue a specific system, process, or service without having to renegotiate the contract for all remaining services.

Contract Inducement Concerns

Financial institutions should not sign servicing contracts that contain provisions or inducements that may adversely affect the institution. Such contract provisions may

include extended terms (up to 10 years), significant increases in costs after the first few years, and/or substantial cancellation penalties. In addition, some service contracts improperly offer inducements that allow an institution to retain or increase capital by deferring losses on the disposition of assets or avoiding expense recognition. These inducements may attract institutions wanting to mask capital problems.

Inducements can take several forms including the following examples:

- The service provider purchases certain assets (e.g., computer equipment or foreclosed real estate) at book value (which exceeds market value) or purchases capital stock from the institution.
- The service provider offers cash bonuses to the institution upon completion of the conversion.
- The service provider offers up-front cash to the institution. The provider states that the institution acquires the right to future cost savings or profit enhancements that will accrue to the institution because of greater operational efficiencies. These improvements are usually without measurable benchmarks.
- The institution defers expenses for conversion costs or processing fees under the terms of the contract.
- Low installation and conversion costs in exchange for higher future systems support and maintenance costs.

These inducements may offer a short-term benefit to the institution. However, the provider usually recoups the costs by charging a premium for the processing services. These excessive fees may adversely affect an institution's financial condition over the long-term. Furthermore, institutions should account for such inducements in accordance with generally accepted accounting principles (GAAP) and regulatory reporting requirements.

Accordingly, when negotiating contracts, an institution should ensure the provider furnishes a level of service that meets the needs of the institution over the life of the contract. The institution must ensure it accounts for contracts in accordance with GAAP. Contracting for excessive servicing fees and/or failing to account properly for such transactions is an unsafe and unsound practice. In entering into service agreements, institutions must ensure accounting under such agreements reflects the substance of the transaction and not merely the form.

Ongoing Monitoring

Action Summary

Management should monitor service provider performance and potential changes in institution requirements throughout the life of the contract. Monitoring should encompass:

- Key service level agreements (SLAs) and contract provisions;
- Financial condition of the service provider;

General control environment of the service provider through the receipt and review of audit reports and other internal control reviews; and

- Potential changes due to the external environment.

Financial institutions should have an oversight program to ensure service providers deliver the quantity and quality of services required by the contract. The monitoring program should target the key aspects of the contracting relationship with effective monitoring techniques. The program should monitor the service provider environment including its security controls, financial strength, and the impact of any external events. The resources to support this program will vary depending on the criticality and complexity of the system, process, or service being outsourced.

To increase monitoring effectiveness, management should periodically rank service provider relationships according to risk to determine which service providers require closer monitoring. Management should base the rankings on the residual risk of the relationship after analyzing the quantity of risk relative to the controls over those risks. Relationships with higher risk ratings should receive more frequent and stringent monitoring for due diligence, performance (financial and/or operational), and independent control validation reviews. Personnel responsible for provider oversight should have the necessary expertise to assess the risks and should maintain suitable documentation. Management should use the oversight documentation when renegotiating contracts as well as developing contingency planning requirements.

User groups are another mechanism financial institutions can use to monitor and influence their service provider. User groups can participate and influence service provider testing (i.e., security, disaster recovery, and systems) as well as promote client issues. Independent user groups can monitor and influence a service provider better than its individual clients. Collectively, the group will constitute a significant portion of the service provider's business.

Key Service Level Agreements and Contract Provisions

Management should include SLAs in its outsourcing contracts to specify and clarify performance expectations, as well as establish accountability. These SLAs formalize the performance criteria against which the quantity and quality of service should be measured. Management should closely monitor the service provider's compliance with key service level agreements. To ensure an effective oversight program, the institution

should develop:

- A formal policy that defines the SLA program;
- An SLA monitoring process;
- A recourse process for non-performance;
- An escalation process;
- A dispute resolution process; and
- A termination process.

Financial Condition of Service Providers

Institutions should have on-going monitoring of the financial condition of their provider(s). To fulfill its fiduciary responsibility, an institution involved in an outsourcing arrangement should determine the financial viability of its provider(s) on an annual basis. However, if the financial condition of the provider is declining or unstable, more frequent financial reviews are warranted. Once the financial review is complete, management should report the results to the board of directors or to a designated committee. At a minimum, management's review should contain a careful analysis of the provider's annual financial statement. Institution management may also use other forms of information to determine a provider's condition, such as independent auditor reports. These reports may contain information that can be vital in determining a provider's financial condition. Managers also can use information provided by public media (trade magazines, newspapers, television, etc.).

If the institution becomes aware that the provider's financial condition is unstable or deteriorating, the institution should implement its contingency plan. Even if the provider remains in operation, its financial problems may jeopardize the quality of its service and possibly the integrity of the data in its possession. Institutions should consider a provider's failure to provide adequate financial data as a potential red flag that there may be serious financial stability issues.

Termination of services due to the bankruptcy of the service provider can have a devastating effect on a serviced institution's operations. There may not be sufficient advance notice of termination, an effective contingency plan, or adequate access to provider personnel. In such a situation, the serviced institution is put into the position of having to find an alternate processing site with little advance notice.

At this point, a serviced institution has several alternatives including:

- Paying off the servicer's creditor(s) and hiring outside specialists to operate the center;
- Obtaining required equipment and software for in-house processing; and
- Transferring data files to another provider.

Most options are costly and may cause harmful operating delays.

In some instances, the provider owns the programs and documentation required to process the institution's files. Unless the contract contains an escrow agreement for

source code, the program and documentation are unavailable to the institution. These programs are often the TSPs only significant assets. Therefore, a creditor of a bankrupt TSP, in an attempt to recover outstanding debts, might seek to attach those assets and further limit their availability to institutions. The bankruptcy court may provide remedies to the institution, but only after adjudicating substantive matters.

General Control Environment of the Service Provider

To oversee the risks associated with the use of external providers effectively, the institution should evaluate the adequacy of a provider's internal and security controls. Management should ensure the provider develops and adheres to appropriate policies, procedures, and standards. When conducting its evaluation, the institution should consider the results of internal audits conducted by institution staff or a user group, as well as external audits and control reviews conducted by qualified sources. The IT Handbook's "Audit Booklet" provides additional details on the various types of external audit engagements for third-party audits of a service provider.

The institution's review of the audit should include an assessment of the following factors in order to determine the adequacy of a service provider's internal and security controls:

- The practicality of the service provider having an internal auditor, and the auditor's level of training and experience;
- The service providers external auditors' training and background; and
- Internal IT audit techniques of the service provider.

Financial institutions should conduct a regular, comprehensive audit of their service provider relationships. The audit scope should include a review of controls and operating procedures that help protect the institution from losses due to irregularities and willful manipulations.

Third-party review reports generated on external providers typically identify certain internal control measures that client institutions are responsible for implementing in order for the provider's accounting systems to be effective. These client institution internal control measures are essential. Financial institution management and audit personnel should verify that the recommended institution internal controls are working effectively, and that the controls effectively complement the accounting system controls described in the provider's third-party review.

Because of the need for an effective internal control program, designated personnel should periodically perform "around-the-computer" audit techniques that:

- Develop data controls (proof totals, batch totals, document counts, number of accounts, and pre-numbered documents) at the institution before submission to the provider. The auditor should sample the controls periodically to ensure their accuracy.
- Include spot-checking reconciliation procedures to ensure output totals agree with input totals, less any rejects.
- Sample rejected, un-posted, holdover, and suspense items to determine why they did not process and how they are addressed (to assure they are properly corrected and reentered on a timely basis).

- Verify selected master file information (such as service charge codes), review exception reports, and crosscheck loan extensions and deposit account entries to source documents.
- Spot-check computer calculations, such as loan rebates, interest on deposits, late charges, service charges, and past-due loans.
- Trace transactions to final disposition to ensure there are adequate audit trails.
- Review source input to ensure sensitive master-file change requests have the required prior approval by appropriate staff or management.
- Visit the provider periodically to assess the status of controls.
- Review other provider audits.

In addition, "through-the-computer" audit techniques allow the auditor to use the computer to check processing steps. These techniques use audit software programs to test extensions and footings and to prepare direct verification statements. These audit software programs often can invoke statistical sampling routines in generating their audit confirmations. If a serviced institution has audit software, it should make arrangements with the provider to allow its use.

Regardless of whether the information processing is internal or outsourced, the financial institution's board of directors should ensure adequate audit coverage. If the institution has no technical audit expertise, the non-technical audit methods can provide minimum coverage. The institution should supplement the internal audit with comprehensive outside IT audits.

Potential Changes due to the External Environment

The contract between the institution and the service provider should be written to encompass the institution's requirements at the time the contract is formed. Over time, the institution's needs may change due to changes in regulation, the economic environment, competition, and other factors outside the contract. Although the contract should provide for flexibility to meet those changing needs, the institution should monitor for changes and update its contract accordingly.

Related Topics

Business Continuity Planning

Action Summary

Financial institutions should:

- Establish ongoing and effective business continuity and information security monitoring programs;
- Effectively manage multiple service provider relationships; and
- Assess, monitor, and effectively control cross-border risks when foreign service providers are used.

Each financial institution should have an effective business continuity plan as outlined in the IT Handbook's "Business Continuity Planning Booklet." The financial institution should also establish ongoing effective business continuity monitoring programs to ensure TSPs adequately control the risks, including information security aspects, associated with the technology services provided. The financial institution has responsibility not only for those portions of the business continuity program performed in-house, but for any portions of the plan developed by a service provider or otherwise outsourced. Financial institutions should consider TSP-related business continuity programs when developing internal plans and programs.

The outsourcing risk management program should identify, for Business Continuity Planning (BCP) purposes, the specific responsibilities of all parties, particularly in the areas of information security and business continuity planning. Financial institutions must also consider which of their critical financial services rely on TSP services, including key telecommunication and network service providers.

The institution should understand all relevant service provider business continuity requirements, incorporate those requirements within its own business continuity plan, and ensure the service provider tests its plan annually. Management should require the service provider to report all test plan results and to notify the institution after any business continuity plan modifications. The institution should integrate the provider's business continuity plan into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan.

Many financial institutions rely on outside data processing providers and any extended interruption or termination of service can disrupt normal operations. Termination of services should occur according to the terms of the service contract, but can result from unanticipated events.

If the provider complies with basic industry standards and maintains an effective business continuity plan, disruption of services should be minimal and the contract will remain intact. The business continuity plan should require the provider to maintain current data files and programs at an alternative site and arrange for processing at another location. At a minimum, these provisions should allow the provider to process the most important data applications. The institution's business continuity plan, which

should complement the provider's plan, is an essential recovery tool when disruption occurs with minimal advance notice.

Events that can cause interruption in the availability of an institution's technology include natural disasters, accidents, software errors, hardware failure, utility outages, and social, political, and economic instability. Even with an outsourcing arrangement, the institution should ensure appropriate backup provisions have been established for their critical data and related processing functions. Effective backup procedures will allow the institution to continue processing applications in the event the data communication system fails. Numerous options are available for management to consider, such as using batch rather than real-time processing methods, operating PCs in an offline mode, capturing data at the controller if transmission lines are lost, or altering communication links through redundant data communication lines, backup modems, or rerouted circuits from the local telephone carrier. Institutions that perform data capture or other functions in-house, should address alternative sites or other means in their backup plan to recover or continue these functions.

Regardless of the method used, an institution should have a comprehensive backup plan with procedures that detail how to obtain and use personnel and equipment. Institutions should test backup capabilities periodically to ensure protection is available and employees are familiar with the plan.

With respect to monitoring and maintaining business continuity plans, institutions should:

- Regularly review the business continuity plans of the service provider or vendor to ensure any services considered "mission critical" for the financial institution could be restored within an acceptable timeframe.
- Review the service provider's program for contingency plan testing. For critical services, annual or more frequent tests of the contingency plan are required.
- Assess service provider/vendor interdependencies for mission critical services and applications.

Outsourcing the Business Continuity Function

In addition to ensuring that outsourced financial and technology services include appropriate business continuity plans; financial institutions that outsource all or a portion of their business continuity capability should consider the following factors.

- **Staffing**-The provider should have sufficient and knowledgeable staff available to provide appropriate onsite technical support to ensure timely resumption of operations at the recovery site.
- **Processing Time Availability**-The provider should allocate sufficient processing time, resources, and security controls to accommodate the potential for multiple clients. The institution should ensure it could process normal volumes of work within appropriate time requirements.
- **Access Rights**-The provider should disclose any access limitations. The provider should guarantee the institution's right to use the site in case of an emergency.

Alternatively, the institution should understand any priority arrangements. For example, some sites operate on a first-come, first-serve basis until the site is at full capacity, but others have pre-arranged priorities based on contractual agreements.

- **Hardware and Software**-The recovery site should have compatible hardware and software. The institution should monitor the compatibility of the site to handle its specific computer hardware and software requirements. To facilitate the monitoring, the provider should be required by contract to notify the institution of any changes in the hardware, software, and equipment at the recovery site.
- **Security Controls**-The institution should ensure it can maintain adequate physical and logical security controls at the recovery site.
- **Testing**-The service provider contract should address access to the recovery site for periodic testing. At a minimum, the institution needs sufficient access to perform at least one full-scale test of the recovery site annually, including verification of telecommunications capabilities. Similarly, the institution should ensure the service provider also performs periodic tests of its own BCP and submits test results to customer financial institutions.
- **Confidentiality of Data**-The institution should ensure the provider can maintain the confidentiality of its business and customer data. The service provider should maintain controls sufficient to ensure the security and confidentiality of the information assets consistent with the institution's information security program. Confidentiality of data is particularly important when multiple clients operate from the same recovery site. Institution management should establish whether the service provider has addressed these issues in its contract, particularly the provisions concerning the Interagency Guidelines Establishing Standards for Safeguarding Customer Information. ^[5]
- **Telecommunications**-The institution should review telecommunications redundancy and capacity at the recovery site, including how communications from the institutions to the recovery site will be established. The service provider should take steps to ensure the recovery site will have adequate telecommunications services (both voice and data) for all of its clients.
- **Reciprocal Agreements**-Financial institutions contracting with another institution for a recovery site should consider the above issues of staffing, processing availability, access rights for recovery or testing, compatibility, security, capacity, etc. Both institutions should ensure they maintain sufficient capacity to meet recovery time objectives and minimum service levels in the event one institution needs to recover operations
- **Space**-The recovery site should have adequate space to accommodate the affected institution's recovery staff.
- **Printing Capacity / Capability**-The recovery site should maintain adequate printing capacity to meet the demand of the affected institution under acceptable levels of service.
- **Contacts**-Institution management should know the procedures for declaring a disaster including who has the authority to declare a disaster and initiate use of the recovery site. Also, the institution should maintain an updated list of contacts names and numbers for the recovery site provider and know the procedures for communicating with the provider.

Outsourced business continuity arrangements can be cost-effective for smaller institutions when compared to establishing and maintaining dedicated alternate recovery sites. Institutions should periodically conduct a thorough test of outsourced disaster recovery services (at least annually).

Information Security/Safeguarding

Information assets are valuable, and institutions should ensure these assets are adequately protected in outsourcing relationships. Financial institutions have a legal responsibility to ensure service providers take appropriate measures designed to meet the objectives of the information security guidelines, and comply with GLBA 501 (b). Those measures should result from the institution's security process and should be included or referenced in the contract between the institution and the service provider. Refer to the IT Handbook's "Information Security Booklet" for additional information on the information security process.

In choosing service providers, management should exercise appropriate due diligence to ensure the protection of both financial institution and customer assets. Before entering into outsourcing contracts, and throughout the life of the relationship, institutions should ensure the service provider's physical and data security standards meet or exceed standards required by the institution. Institutions should also implement adequate protections to ensure service providers and vendors are only given access to the information and systems that they need to perform their function. Management should restrict their access to financial institution systems, and appropriate access controls and monitoring should be in place between service provider's systems and the institution.

Multiple Service Provider Relationships

A multiple service provider relationship is an environment where two or more service providers collaborate to deliver an end-to-end solution to the financial institution.

An institution can select from two techniques to manage this relationship, but remains responsible for understanding and monitoring the control environment of all servicers that have access to the financial institution's systems, records, or resources. The first technique involves the use of a lead service provider to manage the institution's various technology providers. The second technique, which may present its own set of implementation challenges, involves the use of operational agreements between each of the service providers or stand-alone contracts. If the first technique is employed, management should ensure its primary service provider has a contractual obligation to notify the financial institution of any concerns (controls / performance) associated with any of its outsourced activities. Management should also ensure the service provider's control environment meets or exceeds the institution's expectations, including the control environment of organizations that the primary service provider utilizes.

Stand-alone contracts with each service provider require increased management of each provider. Contracting for a technology solution by using one lead provider may lessen the need for the institution to become directly involved if subcontractors fail to perform, but it does not diminish the responsibility for monitoring the internal and security controls of subcontractors through the primary service provider relationship. Because the institution has less control using the lead provider approach, management should require by contract that TSPs notify the institution of all subcontractor relationships.

Outsourcing to Foreign Service Providers

Some institutions develop outsourcing relationships with service providers located in foreign countries. These arrangements can provide cost, expertise, and other advantages to the institutions and should be subject to the same due diligence and assessment as domestic outsourcing relationships. In addition, foreign outsourcing relationships result in unique strategic, credit, liquidity, transactional, geographic, and compliance risks that institutions should identify, assess, prevent, and control. See Appendix C for additional detail.

Endnotes

[1]	See 12 USC 1867 (c)(1) and 12 USC 1464 (d)(7). The NCUA does not currently have independent regulatory authority over TSPs.
[2]	S. Rep. No. 2105, 87-2105 at 3 (1962). reprinted in 1962 U.S.C.C.A.N. 3878, 3880. Accord H.R. Rep. No. 105-417, at 4 (1998), reprinted in 1998 U.S.C.C.A.N. 22. 23.
[3]	Institutions may find advantages in contracting for services for three or more years because of the costs of en-tering into the contract, the costs of changing service providers, and favorable price breaks that may be offered by the vendor for longer terms. Contract flexibility is necessary under these circumstances because of the rapid changes occurring in an IT environment. Contract flexibility should allow for changes in service levels; increase or decrease in the scope of the process, service, or system due to changing institutional goals or objectives; and the retargeting of all relational elements on an annual basis. See Contract Inducement Concerns section in this booklet for further issues to be considered in entering into long-term contracts.
[4]	The "Guidelines Establishing Standards to Safeguard Customer Information" to implement section 501(b) of the Gramm-Leach- Bliley Act of 1999 (GLBA) promulgated by the FFIEC agencies requires institutions to, among other things, require service providers by contract to implement appropriate security controls to comply with the guidelines with respect to their handling of customer information.
[5]	See 66 Federal Register 8616 (Feb. 1, 2001); 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F. (Board); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS). See 66 Federal Register 8152 (Jan. 30, 2001); 12 CFR Part 748, app. A (NCUA).
[6]	The terms "foreign-based third-party service providers" or "foreign-based service provider" refer to any entity, including an affiliated organization or holding company, whose servicing operations are located in and subject to the laws of any country other than the United States, including service providers located outside the United States providing services to foreign branches of U.S. organizations. The term also includes the foreign opera-tions, whether by subcontract or otherwise, of a domestic service provider.
[7]	15 USC 6801. Gramm-Leach-Bliley Act, Section 501(b).
[8]	In this regard, organizations using foreign-based service providers should be aware of Section 319 of the USA Patriot Act, Pub. L. No. 107-56 (Oct. 26, 2001), which requires a financial institution to make information on anti-money laundering compliance by the institution or its customers available within 120 hours of a government request.

-
[9]	Organizations should identify and understand the application of any laws within a foreign jurisdiction that apply to information transferred from the United States to that foreign jurisdiction over the Internet or otherwise to information transferred from that jurisdiction to the United States, as well as to information collected within the foreign jurisdiction using automated or other equipment in that jurisdiction.
[10]	The Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against certain foreign countries, organizations sponsoring terrorism, and international narcotics traffickers based on U.S. foreign policy and national security goals. For more information, refer to the OFAC Web site at www.treas.gov/ofac .
[11]	Export controls on commercial encryption products are administered by the Bureau of Industry and Security, part of the Department of Commerce. Organizations may be exporters if they provide encryption software to a foreign-based service provider, but some exceptions are available that apply to foreign national employees, including contractors and consultants, of U.S. companies and their subsidiaries inside and outside the United States. Export administration regulations regarding encryption are contained in 15 CFR §§ 740.13, 740.17 & 742.15. See www.bis.doc.gov .
[12]	12 CFR part 364, Appendix B, III.D.2 - Banks and 12 CFR part 570, Appendix B, III (d)(2) - Thrifts.
[13]	12 CFR part 332 - Banks and 12 CFR part 573 - Thrifts.
[14]	The term "U.S. regulatory authorities" means the FFIEC member agencies issuing this booklet.
[15]	12 USC 1867(c)(1) - Banks and 12 USC 1464(d)(7)- Thrifts. In addition, organizations should notify their primary regulatory authority of a service relationship with a foreign-based service provider in accordance with regulations and guidance issued by that regulator.
[16]	In instances where the financial institution's foreign branches have outsourced local operations or services cross-border to third-party service providers domiciled in another foreign country, copies of such records can be maintained at the foreign branch office, but must also be available in the U.S.
-

Appendix A: Examination Procedures

EXAMINATION OBJECTIVE: Assess the effectiveness of the institution's risk management process as it relates to the outsourcing of information systems and technology services.

- Tier I objectives and procedures relate to the institution's implementation of a process for identifying and managing outsourcing risks.
- Tier II objectives and procedures provide additional validation and testing techniques as warranted by risk to verify the effectiveness of the institution's process on individual contracts.

Tier I and Tier II are intended to be a tool set examiners will use when selecting examination procedures for their particular examination. Examiners should use these procedures as necessary to support examination objectives.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Determine the appropriate scope for the examination.

1. Review past reports for weaknesses involving outsourcing. Consider:

- Regulatory reports of examination of the institution and service provider(s); and
- Internal and external audit reports of the institution and service provider(s) (if available).

2. Assess management's response to issues raised since the last examination. Consider:

- Resolution of root causes rather than just specific issues; and
- Existence of any outstanding issues.

3. Interview management and review institution information to identify:

- Current outsourcing relationships, including cloud computing relationships, and changes to those relationships since the last examination. Also identify any:
 - Material service provider subcontractors,
 - Affiliated service providers,
 - Foreign-based third party providers;
- Current transaction volume in each function outsourced;
- Any material problems experienced with the service provided;

- Service providers with significant financial or control related weaknesses; and
- When applicable, whether the primary regulator has been notified of the outsourcing relationship as required by the Bank Service Company Act or Home Owners' Loan Act.

Objective 2: Evaluate the quantity of risk present from the institution's outsourcing arrangements.

1. Assess the level of risk present in outsourcing arrangements. Consider risks pertaining to:

- Functions outsourced;
- Service providers, including, where appropriate, unique risks inherent in foreign-based service provider arrangements; and
- Technology used.

2. If the institution engages in cloud computing, determine whether:

- The cloud computing service is or will be hosted internally or outsourced to a third party provider (hosted externally).
- Resources are shared within a single organization or across various clients of the service provider. (Resources can be shared at the network, host, or application level).
- The institution has the ability to increase or decrease resources on demand without involving the service provider (on-demand self-service).
- Massive scalability in terms of bandwidth or storage is available to the institution.
- The institution can rapidly deploy or release resources.
- The financial institution pays only for those resources which are actually used (pay-as-you go pricing)

3. If the institution engages in cloud computing, identify the type(s) of service model that is or will be used:

- Software as a Service (SaaS) - application software is hosted in the cloud; commonly used for email applications such as Hotmail or Gmail, time reporting systems, customer relationship management (CRM) systems such as SalesForce, etc.;
- Platform as a Service (PaaS) - development platform such as Java, .Net, etc. for developing systems is hosted in the cloud;
- Infrastructure as a Service (IaaS) - infrastructure resources such as data processing, data storage, network systems, etc. are provided via the cloud; or
- Data as a Service (DaaS) - data is provided or accessed via the cloud.

4. If the institution engages in cloud computing, identify the type of deployment model to be used:

- Private Cloud - hosted for or by a single entity on a private network; can be hosted internally or outsourced but is most often operated internally; only those within the entity share the resources;
- Community Cloud - hosted for a limited number of entities with a common purpose; access is generally restricted; most often used in a regulated environment where entities have common requirements;
- Hybrid Cloud - data or applications are portable and permit private and public clouds to connect; or,
- Public Cloud - available to the general public; owned and operated by a third party service provider

Objective 3: Evaluate the quality of risk management 1. Evaluate the outsourcing process for appropriateness given the size and complexity of the institution. The following elements are particularly important:

- Institution's evaluation of service providers consistent with scope and criticality of outsourced services; and
- Requirements for ongoing monitoring.

2. Evaluate the requirements definition process.

- Ascertain that all stakeholders are involved; the requirements are developed to allow for subsequent use in request for proposals (RFPs), contracts, and monitoring; and actions are required to be documented; and
- Ascertain that the requirements definition is sufficiently complete to support the future control efforts of service provider selection, contract preparation, and monitoring.

3. Evaluate the service provider selection process.

- Determine that the RFP adequately encapsulates the institution's requirements and that elements included in the requirements definition are complete and sufficiently detailed to support subsequent RFP development, contract formulation, and monitoring;
- Determine that any differences between the RFP and the submission of the selected service provider are appropriately evaluated, and that the institution takes appropriate actions to mitigate risks arising from requirements not being met; and
- Determine whether due diligence requirements encompass all material aspects of the service provider relationship, such as the provider's financial condition, controls, key personnel, disaster recovery plans and tests, insurance, communications capabilities and use of subcontractors.

4. Evaluate the process for entering into a contract with a service provider. Consider whether:

- The contract contains adequate and measurable service level agreements;
- Allowed pricing methods do not adversely affect the institution's safety and soundness, including the reasonableness of future price changes;
- The rights and responsibilities of both parties are sufficiently detailed;
- Required contract clauses address significant issues, such as financial and control reporting, right to audit, ownership of data and programs, confidentiality, subcontractors, continuity of service, etc;
- Legal counsel reviewed the contract and legal issues were satisfactorily resolved; and
- Contract inducement concerns are adequately addressed.

5. If the institution engages in cloud processing, determine that inherent risks have been comprehensively evaluated, control mechanisms have been clearly identified, and that residual risks are at acceptable levels. Ensure that

- Action plans are developed and implemented in instances where residual risk requires further mitigation.
- Management updates the risk assessment as necessary.
- The types of data in the cloud have been identified (social security numbers, account numbers, IP addresses, etc.) and have established appropriate data classifications based on the financial institution's policies.
- The controls are commensurate with the sensitivity and criticality of the data.
- The effectiveness of the controls are tested and verified.
- Adequate controls exist over the hypervisor if a virtual machine environment supports the cloud services.
- All network traffic is encrypted in the cloud provider's internal network and during transition from the cloud to the institution's network.
- All data stored on the service providers systems are being encrypted with unique keys that only authenticated users from this institution can access.
- Unless the institution is using private cloud model, determine what controls the institution or service provider established to mitigate the risks of multitenancy.
- If a financial institution is using the Software as a Service (SaaS) model, determine whether regular backup copies of the data are being made in a format that can be read by the financial institution. (Backup copies made by the service provider may not be readable.)
- Ensure that the financial institution's business continuity plan addresses contingencies for the cloud computing service. Determine whether the financial institution has an exit strategy and de-conversion plan or strategy for the cloud services.

- Determine whether the cloud service provider has an internal IT audit staff with adequate knowledge and experience or an adequate contractual arrangement with a qualified third-party audit firm.

6. Evaluate the institution's process for monitoring the risk presented by the service provider relationship. Ascertain that monitoring addresses:

- Key service level agreements and contract provisions;
- Financial condition of the service provider;
- General control environment of the service provider through the receipt and review of appropriate audit and regulatory reports;
- Service provider's disaster recovery program and testing;
- Information security;
- Insurance coverage;
- Subcontractor relationships including any changes or control concerns;
- Foreign third party relationships; and
- Potential changes due to the external environment (i.e., competition and industry trends).

7. Determine whether the following policies and processes have been revised in light of the need for increased controls brought about by the implementation of cloud computing:

- The Information Security Risk Assessment;
- The Technology Outsourcing (Vendor Management) Policy;
- 8. Review the policies regarding periodic ranking of service providers by risk for decisions regarding the intensity of monitoring (i.e., risk assessment). Decision process should:
- The Information Security Policy;
- The Security Incident or Customer Notification Policy;
- The Business Continuity Plan

8. Review the policies regarding periodic ranking of service providers by risk for decisions regarding the intensity of monitoring (i.e., risk assessment). Decision process should:

- Include objective criteria;
- Support consistent application;
- Consider the degree of service provider support for the institution's strategic and critical business needs, and
- Specify subsequent actions when rankings change.

9. Evaluate the financial institution's use of user groups and other mechanisms to monitor and influence the service provider.

Objective 4: Discuss corrective action and communicate findings

1. Determine the need to complete Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.
2. Review preliminary conclusions with the EIC regarding:
 - Violations of law, rulings, regulations;
 - Significant issues warranting inclusion in the Report as matters requiring attention or recommendations; and
 - Potential impact of your conclusions on the institution's risk profile and composite or component IT ratings.
3. Discuss findings with management and obtain proposed corrective action for significant deficiencies.
4. Document conclusions in a memo to the EIC that provides report ready comments for the Report of Examination and guidance to future examiners.
5. Organize work papers to ensure clear support for significant findings by examination objective.

TIER II OBJECTIVES AND PROCEDURES

A. IT REQUIREMENTS DEFINITION

1. Review documentation supporting the requirements definition process to ascertain that it appropriately addresses:
 - Scope and nature;
 - Standards for controls;
 - Minimum acceptable service provider characteristics;
 - Monitoring and reporting;
 - Transition requirements;
 - Contract duration, termination, and assignment' and
 - Contractual protections against liability.

B. DUE DILIGENCE

1. Assess the extent to which the institution reviews the financial stability of the service provider:

- Analyzes the service provider's audited financial statements and annual reports;
- Assesses the provider's length of operation and market share;
- Considers the size of the institution's contract in relation to the size of the company;
- Reviews the service provider's level of technological expenditures to ensure on-going support; and
- Assesses the impact of economic, political, or environmental risk on the service provider's financial stability.

2. Evaluate whether the institution's due diligence considers the following:

- References from current users or user groups about a particular vendor's performance;
- The service provider's experience and ability in the industry;
- The service provider's experience and ability in dealing with situations similar to the institution's environment and operations;
- The quality and effectiveness of any cost/benefit analyses. Determine whether the analysis considered the incremental costs of the additional monitoring, operations responsibilities, and protections that may be required of the financial institution.
- The cost for additional system and data conversions or interfaces presented by the various vendors;
- Shortcomings in the service provider's expertise that the institution would need to supplement in order to fully mitigate risks;
- The service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities;
- The service provider's ability to respond to service disruptions;
- Key service provider personnel that would be assigned to support the institution;
- The service provider's ability to comply with appropriate federal and state laws. In particular, ensure management has assessed the providers' ability to comply with federal laws (including GLBA and the USA PATRIOT Act); and
- Country, state, or locale risk.

C. SERVICE CONTRACT

1. Verify that legal counsel reviewed the contract prior to closing.

- Ensure that the legal counsel is qualified to review the contract particularly if it is based on the laws of a foreign country or other state; and
- Ensure that the legal review includes an assessment of the enforceability of local contract provisions and laws in foreign or out-of-state jurisdictions.

2. Verify that the contract appropriately addresses:

- Scope of services;
- Performance standards;
- Pricing;
- Controls;
- Financial and control reporting;
- Right to audit;
- Ownership of data and programs;
- Confidentiality and security;
- Regulatory compliance;
- Indemnification;
- Limitation of liability;
- Dispute resolution;
- Contract duration;
- Restrictions on, or prior approval for, subcontractors;
- Termination and assignment, including timely return of data in a machine-readable format;
- Insurance coverage;
- Prevailing jurisdiction (where applicable);
- Choice of Law (foreign outsourcing arrangements);
- Regulatory access to data and information necessary for supervision; and
- Business Continuity Planning.

3. Review service level agreements to ensure they are adequate and measurable. Consider whether:

- Significant elements of the service are identified and based on the institution's requirements;
- Objective measurements for each significant element are defined;
- Reporting of measurements is required;
- Measurements specify what constitutes inadequate performance; and
- Inadequate performance is met with appropriate sanctions, such as reduction in contract fees or contract termination.

4. Review the institution's process for verifying billing accuracy and monitoring any contract savings through bundling.

D. MONITORING SERVICE PROVIDER RELATIONSHIP(S)

1. Evaluate the institution's periodic monitoring of the service provider relationship(s), including:

- Timeliness of review, given the risk from the relationship;
- Changes in the risk due to the function outsourced;
- Changing circumstances at the service provider, including financial and control environment changes;
- Conformance with the contract, including the service level agreement; and
- Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship.

2. Review risk rankings of service providers to ascertain:

- Objectivity;
- Consistency; and
- Compliance with policy.

3. Review actions taken by management when rankings change, to ensure policy conformance when rankings reflect increased risk.

4. Review any material subcontractor relationships identified by the service provider or in the outsourcing contracts. Ensure:

- Management has reviewed the control environment of all relevant subcontractors for compliance with the institution's requirements definitions and security guidelines; and
- The institution monitors and documents relevant service provider subcontracting relationships including any changes in the relationships or control concerns.

Appendix B: Laws, Regulations, and Guidance

Laws

- 12 USC 1464 (d) (7): Home Owners' Loan Act (Thriffs) (N/A)
- 12 USC 1867 (c) (11): Bank Service Company Act (Banks) (N/A)
- 15 USC 6801: Gramm-Leach-Bliley Act (N/A)
- Pub. L. No. 107-56: USA PATRIOT Act (N/A)

Federal Reserve Board

- SR 00-4 (SUP): Outsourcing of Information and Transaction Processing (February 2000)
- SR 00-17 (SPE): Guidance on the Risk Management of Outsourced Technology Services (November 30, 2000)

Federal Deposit Insurance Corporation

- FIL-49-99: Bank Service Company Act (June 3, 1999)
- FIL-50-2001: Bank Technology Bulletin: Technology Outsourcing Information Documents (June 4, 2001)

National Credit Union Administration

- NCUA Letter to Credit Unions No. 02-CU-17: E-Commerce Guide for Credit Unions (December 2002)
- NCUA Letter to Credit Unions No. 01-CU-20: Due Diligence Over Third Party Service Providers (November 2001)

Office of the Comptroller of the Currency

- OCC Bulletin 2002-16: Bank Use of Foreign-Based Third-Party Service Providers (May 15, 2002)
- OCC Bulletin 2001-47: Third-Party Relationships, Risk Management Principles (November 1, 2001)

Office of Thrift Supervision

- 12 CFR Part 570, Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
- CEO Letter 113: Internal Controls (July 14, 1999)
- Thrift Activities Handbook: Section 340: Internal Control (December 2003)
- Thrift Activities Handbook: Section 341: Technology Risk Controls (October 1997)

Appendix C: Foreign-Based Third-Party Service Providers

The material provided in this appendix focuses on foreign-based third-party service providers and should be used, in addition to all other material in this booklet, when examining such relationships. This appendix discusses the primary risks that may arise from service relationships between financial institutions and foreign-based third-parties [6], the steps institutions should consider when managing those risks, and the implications of the relationships within the context of the examination process.

BACKGROUND

Organizations often use domestic third-party service providers as an economic alternative to internal technology and data processing functions. Increasingly, these organizations are considering arrangements with foreign-based third parties or domestic firms that subcontract portions of their operations to foreign-based entities.

The use of foreign-based service providers is a common business practice that can be a less costly alternative to self-processing or to using domestic service providers. However, this practice raises country, compliance, contractual, operational (e.g., transactional), and strategic issues in addition to those presented by use of a domestic service provider. In managing these issues, management should conduct appropriate risk assessments and due diligence procedures and closely evaluate all contracts. Additionally, management should establish ongoing monitoring and oversight procedures.

RISK MANAGEMENT

A financial institution's senior managers are responsible for understanding the risks associated with foreign-based relationships and for ensuring that effective risk management practices are in place. Management should determine if a foreign-based technology relationship is consistent with the organization's overall business and technology strategies and if it can mitigate identified risks adequately. Before management executes a contract with foreign-based entities, it should consider issues such as choice-of-law and jurisdictional considerations. Additionally, organizations should establish appropriate due diligence and risk management policies that include oversight and monitoring procedures. These policies and procedures should consider that all of the risks associated with domestic third party providers are present in foreign-based arrangements in addition to the unique issues such as country and compliance risks arising from the fact that the third parties may not fall under the jurisdiction of domestic laws and regulations.

COUNTRY RISK

Country risk is an exposure to economic, social, and political conditions in a foreign country that could adversely affect a vendor's ability to meet its service level requirements. In certain situations, country risks could result in the loss of an organization's data, research, or development efforts. Managing country risk requires organizations to gather and assess information regarding foreign political, social, and economic conditions and events, and to address the exposures introduced by the relationship with a foreign-based provider. Risk management procedures should include

the establishment of contingency, service continuity, and exit strategies in the event of unexpected disruptions in service.

COMPLIANCE RISK

Compliance risk involves the impact foreign-based arrangements could have on an organization's compliance with applicable U.S. and foreign laws and regulations. An organization's use of a foreign-based third party service provider should not inhibit the organization's compliance with applicable U.S. laws including consumer protection, privacy (Section 501(b) of GLBA) ^[7], and information security laws as well as Bank Secrecy Act requirements ^[8] concerning the reporting and documentation of financial transactions. Additionally, organizations should consider the impact and operational requirements of foreign data privacy laws or regulatory requirements ^[9]. Organizations engaging foreign-based entities should also consider the sanctions and embargo provisions ^[10] of the U.S. Treasury Office of Foreign Assets Control (OFAC) as well as the requirements regarding exportation of encryption-related technologies discussed in the following paragraph.

Export Controls

The United States has export control laws that restrict the export of software and other items (U.S. Export Administration Regulations). ^[11] These laws apply to all aspects of encryption usage, including but not limited to, software, hardware, and network applications. Organizations should ensure they and their service provider(s) comply with these laws. Contracts should include a representation and warranty that service providers will comply with U.S. export control laws.

DUE DILIGENCE

Management of an organization considering a foreign-based outsourcing arrangement should perform appropriate due diligence similar to domestic outsourcing arrangements before selecting or contracting with a service provider. The process should include an evaluation of a firm's financial stability and commitment to service, and the potential impact of the foreign jurisdiction's regulations, laws, accounting standards, and business practices. Additionally, management should consider the degree to which geographic distance, language, or social, economic, or political changes may affect the foreign-based service provider's ability to meet the organization's servicing needs. Management should consider the cost and logistical implications of managing a cross-border relationship, including the ongoing costs of managing and monitoring cross-border and foreign-based provider relationships.

CONTRACTS

Contracts between an organization and a foreign-based entity should address the risks identified during risk assessments and due diligence processes. Specific topics that should be considered regarding such contracts are discussed in the following paragraphs.

Security, Confidentiality and Ownership of Data

Management should require contract provisions to protect its customers' privacy and the confidentiality of organizational records in conformance with U.S. laws and regulations. Federal regulations require that service provider contracts include provisions requiring the service provider to implement procedures and security measures that meet the objectives of customer information security guidelines.^[12] Additionally, contracts should include provisions prohibiting the disclosure of any customer information to nonaffiliated third parties, other than as permitted under U.S. privacy laws.^[13]

Any agreement with a foreign-based service provider should also include a provision that all information transferred to the foreign-based entity remains the property of the organization, regardless of how it is processed, stored, copied, or reproduced.

Regulatory Authority

Arrangements with foreign-based service providers should contain a provision acknowledging the authority of U.S. regulatory authorities^[14] (pursuant to the Bank Service Company Act or the Home Owner's Loan Act) to examine the services performed by the provider.^[15] Financial institutions must not share U.S. regulatory examination reports or information contained therein with either foreign regulators or foreign-based service providers without the express written approval of the appropriate U.S. regulatory authority.

Choice Of Law

Before entering into an agreement or contract with a foreign-based vendor or developer, an organization should carefully consider which country's law it wishes to control the relationship. Based on that review, organizations should include choice of law and jurisdictional covenants that provide for the resolution of disputes between the parties under the laws of a specific jurisdiction.

These provisions are necessary to maintain continuity of service, access to data, and protection of customer information. For these reasons, it can be particularly important when dealing with foreign service providers to specify exactly which country's laws will control the contractual relationship between the parties. Additionally, contract provisions may be subject to foreign-court interpretations of local laws. The laws of the foreign country may not recognize choice of law provisions and may differ from U.S. law regarding what they require of organizations or how they protect bank customers. Thus, an organization's due diligence should include analysis of a country's local laws by legal counsel competent in assessing the enforceability of all aspects of a contract.

MONITORING AND OVERSIGHT

Monitoring foreign entities requires the same steps as monitoring domestic servicers and vendors in addition to the recommendations presented within this appendix. When organizations establish a servicing arrangement with a foreign-based service provider, management should monitor both the entity and the conditions within the foreign country.

The organization should determine that the foreign-based service provider maintains adequate physical and data security controls, transaction procedures, business resumption and IT contingency arrangements (including periodic testing), insurance coverage, and compliance with applicable laws and regulations. Further, where indicated by the organization's security risk assessment, the organization must monitor its foreign-based service providers to confirm that they have satisfied security obligations imposed in the contract to comply with Section 501(b) of GLBA.

Organizations also should monitor economic and governmental conditions within the foreign country to determine whether changes are likely to affect the ability of the service provider to perform under the arrangement.

REGULATORY AGENCY ACCESS TO INFORMATION

U.S. regulatory authorities must have the ability to examine the services performed by an organization's third-party service provider regardless of whether it is foreign or domestically based. Organizations must maintain, in the files of a U.S. office, appropriate English language documentation to support all arrangements with service providers. Appropriate documentation typically includes a copy of the contract establishing the arrangement, supporting legal opinions, due diligence reports, audits, financial statements, performance reports, and other critical information. ^[16] In addition, the organization should have an appropriate contingency plan to ensure continued access to critical information, to maintain service continuity, and the resumption of business functions in the event of unexpected disruptions or restrictions in service resulting from transaction, financial, or country risk developments.

EXAMINATION CONSIDERATIONS

U.S. regulatory authorities may examine the services performed for an organization under an outsourcing arrangement with a foreign-based service provider. Likewise, in the case of a foreign-regulated entity, U.S. regulatory authorities may be able to obtain information through the appropriate supervisory agency in the service provider's home country.

With respect to the outsourcing organization in such arrangements, U.S. regulatory authorities will focus reviews on the adequacy of an organization's due diligence efforts, its risk assessments, and the steps taken to manage those risks including the effect of the arrangement upon the organization's compliance with applicable laws and its access to critical information. Regulatory reviews will assess the organization's contract provisions and its ongoing monitoring or oversight program, including any internal and external audits arranged by the foreign-based service provider or the organization.

An organization's use of a foreign-based third-party service provider (and the location of critical data and processes outside of U.S. territory) must not compromise the ability of U.S. regulatory authorities to effectively examine the organization. Thus, organizations should not establish servicing arrangements with entities where local laws or regulations would interfere with U.S. regulatory agencies' full and complete access to data or other relevant information. Any analysis of foreign laws obtained from counsel should include a discussion regarding regulatory access to information for supervisory purposes.

Appendix D: Managed Security Service Providers

Background and Purpose

A growing number of financial institutions (FIs) are partially or completely outsourcing the security management function to third parties, typically known as Managed Security Service Providers (MSSPs). FIs engage MSSPs due to increasingly sophisticated threats, cost pressures, and absence of internal expertise. The services that MSSPs provide present additional risks FIs are required to manage.

The purpose of this appendix is to identify the risks associated with the MSSP engagement and offer guidance to assist FIs in mitigating these risks. While the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) on Information Security Booklet provides related guidance, FIs should pay particular attention to risk management issues that are heightened when serviced by MSSPs. The loss of control that comes with the outsourced security function introduces an element of risk that FIs need to understand and appropriately manage. The following subsection, MSSP Engagement Criteria covers numerous engagement criteria and related contract considerations institutions should consider when engaging an MSSP.

In addition to the normal vendor management responsibilities, a successful engagement with an MSSP should include:

- A contract with mutually agreed upon Service Level Agreements (SLAs);
Strategies for ensuring transparency and accountability that include:
 - Regular communication between the FI and the MSSP
on matters including change control, problem
resolution, threat assessments, and MIS reporting,
 - Descriptions of processes for physical and logical controls
over FI data; and,
 - Periodic review of the MSSP's processes, infrastructure, and control
environment through offsite reviews of documentation and onsite visitations.

Types of Managed Security Services

Following are some of the many types of security-related services offered by MSSPs:

- Network Boundary Protection

Using technology such as firewalls and virtual private networks (VPNs), the MSSP protects the FI's network perimeter. The MSSP should provide device monitoring of connections to external third parties such as Internet Service Providers.

- Management of Intrusion Detection and Prevention for Networks and Hosts

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are automated services that can detect patterns in network traffic and may take action according to a rule set or pattern definition database.

- Event Log Management and Alerting

Event log management and alerting is conducted to monitor event logs generated by network devices or computer systems to centralize, filter, and provide management reports on material activity. Alerts can be set for highly sensitive events or activities.

- Anti-virus and Web Content Filtering Services

Managed antivirus protection provides organizations with malware protection that helps safeguard FIs from new threats. The malware definitions are updated frequently to help recognize the new threats.

- Patch Management and Security Software Management

MSSPs can identify and manage network security related software systems and components requiring regular security updates; conduct compatibility testing before deployment; deploy the updates uniformly; and provide reporting on the status and effectiveness of the security software as implemented.

- Security Incident Response and Management

MSSPs can assist an organization in building an incident response team or providing a turnkey incident response in the event of a breach.

- Data Leak Prevention

MSSPs can help identify all methods of data ingress and egress, and establish systems that monitor and enforce appropriate controls.

- Secure Messaging

MSSPs can provide services to ensure the security of messages into and out of the FI.

- Information Security Consulting Services

Security consulting by MSSPs may include risk assessment, vulnerability assessment testing, penetration testing, compliance tools, education and training, and attestation services.

Description of Managed Security Services Arrangements

Managed security services arrangements can include the following four deployment models:

- Full Outsourcing: Under this model the MSSP performs the following functions autonomously.
 - Manage all network connections at customer premises;
 - Manage network platforms;
 - Update rules and thresholds over networking devices;
 - Analyze data and necessary escalation responses; and
 - Provide client reports or alerts on outcomes of the managed service.
- Co-managed: Under this model the FI and MSSP use the same infrastructure and have access rights and responsibilities on platforms
 - Typically involves client-owned network equipment on their premises;
 - Includes common security event monitoring tools and data loss prevention solutions; and
 - IDS/IPS events are reported to the MSSP and the FI consults with the MSSP providing primary services during off hours.
- Split Processing: Under this model, the MSSP performs some functions and the FI performs others.
 - Most commonly used with firewall and network devices where the MSSP monitors log data, health and capacity with the FI pushing system updates, rules changes, or configurations;
 - Vulnerability assessment and analysis where the MSSP and FI each test applications and platforms; and
 - Sometimes used when multiple MSSPs are employed.
- Consulting: Consulting services provided by MSSPs can include assisting with risk assessments, initial system configuration, policy formulation, compliance (PCI, GLBA, and SOX), forensics, penetration testing, application security testing, application code review, social engineering, physical security, and management reporting.

Governance

Effective governance is fundamental for understanding and managing the risks involved when outsourcing to MSSPs. Critical areas include availability, integrity, and confidentiality of FI data. The costs to procure, operate, and manage service delivery, including review for compliance with the SLAs, should be part of the overall contract.

Risk Assessment

A risk assessment must be performed as part of, or in conjunction with, the due diligence review when an FI is considering outsourcing security services. Concerns about vendors become especially important as security practices that were traditionally conducted in-house are outsourced to an MSSP. The MSSP risk assessment should guide the FI as it develops, implements, tests, and maintains the information systems security program.

Financial Institution Requirements

Gathering necessary information internally and from the potential MSSP is necessary to identify potential threats, vulnerabilities, and controls. Documentation of the risk assessment is especially important to help ensure coordination, consistency, and standardization between the FI and the MSSP. The identification of information systems and the ranking of sensitive data and applications at the MSSP should be part of the risk assessment process. Coordination is also necessary to help ensure that vulnerabilities are identified and processes are validated through testing.

Risk Considerations for Managed Security Services

The reliance on MSSPs may significantly increase an FI's risk profile. Increased risk can arise from poor planning, lack of oversight and control, and/or poor MSSP performance or service. To control these risks, the FI should exercise appropriate due diligence prior to entering an MSSP relationship and maintain effective governance during the relationship.¹

Below are risk elements that should be considered in an FI's MSSP risk assessment.² The risks identified are relevant regardless of the type of MSSP arrangement.

Risk Elements Pertaining to Managed Security Services

- **Business Process**

According to the FI's risk profile, the following risks should be considered:

- Liability under business partnership agreements;
- False sense of security by FI management;
- Diverse offshore legal, geo-political, and cultural risk;
- Impact on competitive advantage when valuable intellectual property or proprietary information is stolen;

- Damage should the MSSP fail to provide the contracted service;
- Heightened legal and regulatory issues;
- Dependence on an outside organization for critical services;
- Loss of the FI experience, knowledge, and skill development; and
- Vendor financial condition decline.

Information Security Infrastructure

To optimize service availability while mitigating risks, the following should be considered:

- Complexity of network infrastructure and deployment of agents;
- Information security breaches and data loss;
- Loss to the FI for failing to comply with applicable regulations and laws;
- Downtime due to lack of resilient MSSP infrastructure; and
- Loss of the FI's key control requirements due to MSSP's "one size fits all" products.

- **Access Management and Control**

Ensure FI and MSSP user access is monitored, controlled, and assessed for inappropriate or inadequate:

- MSSP access of FI data;
- User access controls;
- Segregation of duties;
- Control and oversight of MSSP activity by the FI; and
- Attestations of MSSP access to FI systems and data.

- **Protection Against Malware**

To protect the computing environment of malicious software the MSSP should have the following:

- Current antivirus/malware protection;
- Strong patch and/or configuration management policies and procedures;
- Timely identification of compromised devices; and
- Appropriate endpoint protection tools.

- Data and Media Handling

To foster adequate data and media handling protection, consider if the MSSP has:

- Proper application configuration;
- Secure data storage and/or processing by MSSPs;
- Adequate access and integrity controls;
- Appropriate encryption;
- Adequate key management for encrypted data; and
- Sufficient data retention.

- Application Development and Systems Integration

An FI should confirm that application development and change management are performed securely by an MSSP. The following should be considered:

- Configuration specifications;
- Change management processes at the MSSP and/or at the FI;
- Logging and monitoring; and
- Recertification of software and permissions.

- Business Continuity and Disaster Recovery

An FI should confirm that MSSPs can provide resilient services in the event of an outage or disruption. Risks that FIs should identify and address include:

- Incompatible continuity plans and unrealistic disaster recovery planning;
- Insufficient distance between datacenter and backup datacenter (or recovery cite) for disaster recovery;
- Inadequate disaster recovery testing and postmortem report (Disaster recovery is not in line with disaster recovery needs.);
- Poor communication between the FI and MSSP during a disaster; and
- Inadequate capacity of the MSSP to service all clients during an outage.

- Incident Response Management

An FI should identify, monitor, and manage incidents in coordination with the MSSP. Risks that FIs should identify and address include:

- Undefined roles and responsibilities between the FI and the MSSP;
- Untimely reporting of incidents and/or data breaches;
- Failure to take appropriate steps to contain and control the incident;
- Failure to notify the FI's customers or regulators on FI's behalf per contract agreement;
- Failure to perform joint incident response table-top testing with MSSPs;
- Overdependence on the MSSP for incident response; and
- Legal issues arising from a security incident involving both parties.

- Awareness and Training

An FI should determine that all parties are aware of and trained in processes and MIS reports. Potential risks to be addressed include:

- Insufficient training or expertise at either the MSSP or FI; and
- Inadequate MSSP personnel screening practices.

Request for Information and Request for Proposal

Request for Information (RFI) and Request for Proposal (RFP) are part of a deliberate and intentional process associated with engaging an MSSP. This type of evaluation should be completed in accordance with the FI's strategic plan and tactical approach to security. For example, the strategic plan should determine what security functions to maintain in-house, whether to contract a sole provider, or split services between providers. The RFI, the initial formal step in selection, must define FI objectives for the service needed. These objectives primarily are to be based on the FI's configuration (OS, security, network, and servers) and security policies. The FI should also consider the MSSP's staffing, certifications, training, transition process, and incident response methodology.

It is essential for the FI to coordinate with the MSSP regarding configuration and staff resources. This will be important not only to initial selection through the RFI/RFP and contracting process, but as the relationship evolves. It is important that the MSSP be a cultural fit with the FI. 3 MSSP specific contract language will require modification to RFIs and RFPs based on the FI and vendor configuration. See subsection, MSSP Engagement Criteria for RFI/RFP examples specific to MSSPs.

Initial Due Diligence

An FI considering an MSSP engagement must perform adequate due diligence to validate that the vendor is capable of managing security services that are aligned with their risk profile. Management should consider performing an onsite visitation to determine if the servicer has the appropriate experience and control environment to meet the FI's needs, how long the MSSP has been in business, the MSSP's staffing, the MSSP's incident response methodology, etc.

When performing an onsite visitation, the FI should determine if the MSSP can ensure the security of their data. Pertinent entity and operating information should be obtained to facilitate the vendor selection process. Discussions with management should focus on the risk elements noted in the risk assessment section with emphasis on determining that the MSSP has the necessary expertise and experience to service the FI and will provide sufficient metrics for the FI to assess compliance with the contract.

The time the MSSP has been operating and if there are any expected changes (e.g., merger, acquisitions, expansion/growth, etc.), that could impact contracted services should be determined. The number of clients the MSSP services and number of FI clients also should be identified. If the MSSP does not have FI clients, it may indicate the vendor is seeking to enter into an unfamiliar business area. Before accepting this risk, the MSSP's familiarity with pertinent regulatory requirements such as GLBA, SOX, and FFIEC guidance must be validated.

When evaluating the MSSP's expertise, the following should be considered:

- Current and unbiased customer testimonials and/or references;
- Use of current monitoring and risk management technologies;
- The MSSPs ability to:
 - Generate timely MIS reporting and incident notification;
 - Maintain confidentiality, integrity, and availability of FI data; and
- Manage prospective services for the defined contract term.

If the MSSP does not perform all services in-house, FIs should determine which services are to be outsourced, the quality of vendor management exercised by the MSSP, and whether the service provider(s) is/are offshore.

To fulfill its duties, an MSSP may be required to install software and/or hardware in an FI's data center. What data will be collected, reviewed, stored, and secured by the MSSP should be defined with established SLAs based on business requirements. The dialog between the MSSP and the FI should focus on identifying services that preserve security.

The initial due diligence process is a key method to determine if an MSSP can provide the necessary services to an FI. Each of the above recommendations should be

considered in deciding if the MSSP is viable and has the ability to fulfill the terms of the engagement.

Contracts

In any MSSP arrangement, the contractual expectations and obligations of each party should be clearly defined, understood, monitored, and enforced. FI managers who have a strong understanding of MSSP risks and mitigating controls should be involved in contract development. Legal representatives with the expertise to assess the enforceability and legitimacy of MSSP contract terms should review contract provisions and be included in contract negotiations. The alignment of contract provisions with FI security policies and procedures creates a strong foundation for the development of comprehensive MSSP agreements.

Although most contract requirements for MSSPs are similar to those of other outsourcing arrangements, FIs should consider the following provisions when developing a formal contract with an MSSP.

Scope of Service

Contract discussion should include:

- Specific services provided, timelines for implementation, and explicit responsibilities of the MSSP and the FI;
- The right to modify existing services performed under the contract;
- The type and frequency of reports available;
- Activities the MSSP is allowed to conduct when operating within the FI network;
- Handling of confidential data;
- Ownership of data generated by proprietary security or third-party monitoring tools owned by the MSSP; and
- Access rights granted to the MSSP as it relates to FI network systems.

Service Level Agreements

Well defined SLAs provide the framework for establishing the expectations and metrics for the effective delivery of service such as levels of availability, performance, or support. When working with MSSPs, attention should be given to the engagement criteria in Appendix A.

Contract Term and Renewal

The role of the MSSP relationship and how the length of the contract integrates with the FI's overall business strategy and objectives should be defined. Long-term contracts may limit flexibility and consideration should be given to whether to accept automatic contract renewal provisions.

Termination

FIs should consider including termination rights for a variety of conditions including material breach, critical performance failure, and material non-performance. Grounds for termination should be clearly defined and agreed on by the FI and service provider. If the contract is terminated for cause, the MSSP should cover damages. The FI's exit strategy should consider post-termination rights including:

- Transfer of data in the FI's preferred format;
- Transfer of FI data or assets from the MSSP and all subcontractors;
- Assistance from the service provider to migrate services in-house or to another provider;
- Right to purchase non-proprietary tools used by the MSSP to provide the services; and
- Timely response to the FI's post-termination requests.

Managing the Relationship

While the initial due diligence is critical to managing the MSSP relationship, ongoing monitoring and oversight is equally important. Risks of the MSSP relationships are generally similar to risks of other outsourcing arrangements that need to be addressed within the FI's vendor management program, but the MSSP relationship has some attributes that may call for a heightened level of (or more targeted) education and training.

Education and Awareness

Effective MSSP oversight requires an FI to maintain adequate in-house technical expertise. This enables the FI to monitor and maintain acceptable risk exposure and confirm the MSSP is fulfilling contractual obligations. Education and awareness for FI employees is necessary to help ensure:

- The MSSP is effectively managing the relevant information security risk;
- Personnel understand the processes, procedures, and protocols of the MSSP, including the use of subcontractors; and
- FI management understands:
 - What data the MSSP is collecting and who has access to the data;
 - Information in audit reports and security testing of the MSSP; and
 - How to measure a successful relationship.

Given the high risk and trust of the relationship, the FI should verify that the MSSP is appropriately managing the contracted security services on its behalf. The following should be addressed in the FIs education and awareness program:

- Training, education, and awareness provided by the MSSP to FI employees;
- Identifying and understanding accountable and responsible parties at the FI and MSSP;
- Maintaining the expertise needed to understand metrics and reporting provided by the MSSP; and
- Training frequency for FI employees.

Contract Performance

FI management should have a monitoring process to attest to the MSSP meeting its contractual obligations. This typically entails reviewing items such as SLAs, Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), security event notification, incident response, and any other metrics relative to performance. These items should be included in MSSP reports, and FIs should perform supplemental monitoring as necessary to evaluate contractual performance.

Ongoing Oversight of MSSP Relationship

The critical services provided by MSSPs require a high level of FI oversight throughout the lifecycle of the contracting relationship. Processes should include maintenance of controls established as part of the initial due diligence, including:

- Reviewing:
 - MSSP provided MIS reports,
 - MSSP audit reports, including SSAE 16 and other independent assessment reports, and
 - Penetration testing and vulnerability assessment test results;
- Performing periodic onsite visitations of the MSSP;
- Monitoring the MSSP's internal risk assessment process; and
- Discussing any concerns related to the above items with MSSP management.

Contingency & Event Planning

Business Continuity Planning

To avoid a gap in service in the event of an MSSP outage, the FI should:

- Review the MSSP's business continuity plans for the ability to provide continuous services to the FI;
- Confirm that MSSPs have tested their business continuity plans at least annually and have forwarded a summary to the FI; and
- Include critical MSSPs in the FI's tabletop exercise or other business continuity testing.

Incident Response

To assess that the FI is fully prepared to respond to incidents, the FI should:

- Develop and maintain an incident response plan which includes a remediation process clearly defining roles and responsibilities between the MSSP and the FI;
- Establish and review processes and procedures to handle communications to and from the MSSP;
- Establish and define event types and response procedures; and
- Include the MSSP in testing of the incident response plan.

Alternative Providers

To prevent gaps in service associated with MSSP failure, the FI should:

- Maintain awareness of alternate providers;
- Develop policies and procedures to outline FI data ownership;
- Have a clear understanding of service provider roles and responsibilities;
- Assess the MSSP for dependencies with critical services; and
- Consider using multiple vendors to provide various MSSP services.

Demarcation of Responsibility

Along with general monitoring and oversight of the MSSP, FIs should have involvement in the operational and policy activities associated with the MSSP. Examples include:

Policy and Procedures

Outsourcing certain security activities does not diminish the need for adequate security policies at the FI. They should coordinate their information security program with the policies, standards, guidelines, and procedures of the MSSP.

Incident Response

The incident response function needs to be coordinated and clearly defined between the FI and MSSP. Notification and escalation requirements regarding incident response should be clearly documented and aligned between the FI and MSSP. The definition of a reportable event should be clear and unambiguous.

Access Controls

Assess controls/methods and audit trails related to the FI's systems, devices, and data being managed by the MSSP.

Physical Security

Typically the MSSP will place devices within the FI (e.g., firewall, IDS, etc.) which the MSSP may own and/or control. FIs should consider appropriate physical security of such devices regardless of ownership and/or control.

Change Control

There should be a clear process to communicate changes implemented by either the FI or MSSP. Changes can have a material impact on the security environment, and both parties should undergo an adequate change control review. Advanced notification of any changes should be provided whenever possible.

Data Collection/Logging

The FI should maintain awareness of data the MSSP is collecting, how it is stored, and how it is used. The FI should maintain its data or logs separate from other MSSP clients. The MSSP's data collection and security event classification processes should be defined and understood to help in corroborating the integrity of the FI's data and in establishing a more effective log review process.

Metrics and Reporting

The MSSP should provide regular reporting on agreed on performance metrics to the client FI. It is important that qualified FI personnel review these reports to attest that the security controls of MSSPs are operating as expected. Metrics and reporting should include security:

- Events potentially affecting the FI;
- Statistics specific to the FI;
- Intelligence, and;

- Operational statistics and conditions specific to the FI.

Emerging Risks

Cloud computing is an emerging trend in which some of the IT industry's biggest players are investing significant resources. Cloud computing in general is a migration from owned resources to shared resources in which client users receive information technology services on demand from third-party service providers via the Internet "cloud." In cloud environments, a client or customer will relocate their resources such as data, applications, and services to computing facilities outside the corporate firewall, which the end user then accesses via the Internet.

Cloud-based MSSP services may be implemented as part of Internet access services. Examples of "in-the-cloud" services include carrier-based denial of service protection, virtual firewall services, and carrier-provided URL blocking.

When an MSSP offers services that use a cloud computing architecture, the same risks that are specific to non-cloud-based security services apply. However, there are a few additional risk considerations that should be assessed when moving to a cloud computing environment. Areas for FIs to consider when an MSSP uses cloud computing in their managed security services environment include:

- Protecting data in transit to avoid data leakage;
- Securing data at rest so that one data breach within the cloud does not breach the other customer data within the cloud;
- Maintaining compliance with applicable regulatory requirements;
- Complying with foreign government privacy laws when outsourcing is performed offshore;
- Segregating customer data appropriately to comply with audit and legal requirements; and
- Avoiding sharing of authentication credentials to prevent the impersonation of users.

Conclusion

Financial institutions' challenges in dealing with high profile network security breaches, changing technology, malware, system maintenance costs, complexity, and uncertainty surrounding network security have resulted in an increased use of MSSPs. While FIs can leverage the expertise of the MSSP, managing this relationship can be an additional challenge, particularly when MSSPs have access to confidential or sensitive information that requires increased protection. In addition, FIs can have high levels of risk exposure in the event that an MSSP cannot comply with service level agreements.

As with all outsourcing arrangements FI management can outsource the daily responsibilities and expertise; however, they cannot outsource accountability.

MSSP Engagement Criteria

MSSP: ENGAGEMENT CRITERIA

SLA - Service level agreement

RFI - Request for information

RFP - Request for proposal

* Contract Provisions for consideration

Criteria	Description	Phase	Information/Expectations
Service Availability	Due to the nature of managed security services, it is critical that the service be operational 24x7 to the fullest extent practicable. While an outage to a core banking system (e.g., teller, loan processing, etc.) may be manageable, a momentary failure of a FI's managed security environment could have disastrous consequences.	SLA* RFP/RFP/SLA SLA* SLA RFP/SLA*	Specify recovery time when a service outage occurs MTTR (Mean Time to Recovery) Identify expectations of percentage of system uptime Notification of any planned outages Defined system performance reports Schedule for applicable credits and compensation
Incident Response and Notification	Timely notification and classification of incidents is critical for most MSSP engagements. The severity of the incident and its potential impact must be identified and communicated to appropriate staff. Plans should be comprehensive and customized to the FI in order to minimize the impact of the breach.	SLA RFP/SLA RFP/SLA RFP/SLA* RFP/SLA* RFP/SLA	Key staff and backups identified with 24x7 availability Defined severity levels with appropriate escalation requirements Maximum timeframe for communicating new problems and action items Review MSSP incident response plan which should specify how incidents will be handled and by whom. Table top testing is vital to ensure MSSP and FI understand their roles in an actual event Consider MSSP forensic analysis procedures
State/Federal Compliance	Existing state and federal law and regulations	RFP*	Ensure MSSP complies with applicable notification requirements for data security/privacy

Criteria	Description	Phase	Information/Expectations
Staffing	MSSPs provide specialized services performed by IT professionals that must have the expertise necessary to identify and respond to current IT security issues.	RFP/SLA	Identification of staff professional certifications (e.g., CISSP, CISM, etc.)
		RFP/SLA	Procedures for background checks and hiring criteria
		RFI/RFP	Describe process for monitoring Security Operations Center (SOC) personnel
		RFI/RFP	Describe procedures for initial and ongoing staff training.
		RFI/RFP	Provide profile of staffing resources (e.g., experience, number of employees, etc.)
Third-Parties and Subcontractors	FIs must protect customer information, sensitive corporate data, and maintain high availability of services regardless of outsourced relationships. This obligation extends to any third parties utilized to deliver their services.	RFI/RFP*	Identify 3rd parties that may be used and describe roles and oversight.
		RFP*	Notification/approval of significant subcontractors

Handling Sensitive Data	In many engagements, MSSPs may have access to non-public customer data and sensitive information about the FI and its operating environment. Depending on the relationship, the FI may no longer have direct control over the data.	SLA* SLA RFI/RFP/SLA RFP/SLA*	Procedures for restricting use of any sensitive data whether in-transit or at rest Procedures for disclosing the loss or unauthorized access to sensitive data Primary location of data processing and storage (US based) Secure storage, retention, and destruction of data should be clearly defined
Service Scalability	The ability to provide scalable services on a near real-time basis is often one of the key factors considered by FIs in choosing an MSSP.	SLA SLA	Regular reporting of capacity-related statistics such as bandwidth utilization, storage used, and percent of system capacity used. Consideration of anticipated rates of capacity growth, storage needs, and seasonal or promotional spikes

Criteria	Description	Phase	Information/Expectations
Disaster Recovery	In the event the MSSP is subject to a disruptive event, it is critical that services to the FIs remain uninterrupted to the fullest extent practicable.	RFP/SLA*	Access to MSSPs' business continuity plan and testing results
		RFP/SLA*	Standards for Mean Time to Recovery (MTTR)
Customer Support	The breadth of issues that may arise in an MSSP engagement may require 24x7 live customer support.	RFP/SLA	Customer support Guaranteed Response Time (GTR)
Hardware Replacement*	Some MSSP services involve installation of a proprietary hardware device at the FI.	SLA*	Minimum time for delivery of replacement device
		SLA	Backup device
		RFP/SLA	Established procedures for onsite support
Training/Education	FIs may not have the staff expertise to understand the information provided by MSSP specialized management and reporting tools.	RFP/SLA	Classroom/onsite training
		RFP/SLA	Web-based tutorials
		RFP/SLA	Consulting services

Technology	MSSPs utilize specialized technology and information resources that are critical to the service offerings.	RFI/RFP SLA RFP RFI/RFP/SLA	Describe methodology used for collecting, reporting, and analyzing threats, vulnerabilities, or possible attacks. Proprietary technology required Changes required to existing network architecture, configuration or systems SDLC procedures for services delivered
Due Diligence (e.g., onsite visits, audits, financial reviews)	MSSPs have evolved rapidly over the past 10 years from the entrepreneurial "garage business" to formal offerings and facilities. Onsite visits and audit reviews throughout the lifecycle can provide a valuable window to ensure services are offered in a safe and secure manner.	RFI/RFP/SLA RFP/SLA RFP*	What recognized audit reports are available for review (e.g., SAS70, SSAE16, etc.) Provision for pre-engagement and periodic site visits. Access to annual financial statements

MSSP Examination Procedures

EXAMINATION PROCEDURES

NOTE: This appendix includes all of the steps in Appendix A, plus unique ones for MSSP's.

EXAMINATION OBJECTIVE: Assess the effectiveness of the institution's risk management process as it relates to the outsourcing of information systems and technology and security services, and the heightened risks specific to the outsourcing of security services to a Managed Security Services Provider (MSSP).

Tier I and Tier II Objectives and Examination Procedures are intended to be a tool set examiners will use when selecting examination procedures for their particular examinations. Examiners should use these procedures as necessary to support examination objectives.

Tier I Objectives and Procedures relate to the institution's implementation of a process for identifying and managing risks related to outsourcing functions to an MSSP.

Tier II Objectives and Procedures provide additional validation and testing techniques, as warranted by risk, to verify the effectiveness of the institution's process on individual MSSP contracts.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Determine the appropriate scope for the examination.

1. Review past reports for weaknesses involving outsourcing. Consider:

- Regulatory reports of examination of the institution and service provider(s); and
- Internal and external audit reports of the institution and service provider(s).

2. Assess management's response to issues raised since the last examination.

Consider:

- Resolution of root causes rather than just specific issues; and
- Existence of any outstanding issues.

3. Interview management and review institution information to identify:

- Current outsourcing relationships and changes to those relationships since the last examination. Also identify: Material service provider subcontractors,

Also identify:

- Material service provider subcontractors,
- Affiliated service providers,
- Foreign-based third party providers;
- Current transaction volume for each function outsourced;
- Material problems experienced with the service provided;
- Service providers with significant financial or control-related weaknesses;
and
- When applicable, whether the primary regulator has been notified of the outsourcing relationship as required by the Bank Service Company Act or Home Owners' Loan Act.

Objective 2: Evaluate the quantity of risk present from the institution's outsourcing arrangements.

1. Assess the level of risk present in outsourcing arrangements. Consider risks pertaining to or associated with:

- Functions outsourced;
- Service providers, including where appropriate, unique risks inherent in foreign-based service provider arrangements;
- Technologies used;
- Staff qualifications;
- The MSSP's risk assessment program and whether it includes business process, information security infrastructure, related risk assessments, etc.; and
- The frequency of MSSP risk assessments

Objective 3: Evaluate the quality of risk management.

1. Evaluate the outsourcing process for appropriateness, given the size and complexity of the institution. The following elements are particularly important;

- Institution's evaluation of service providers consistent with scope;
- Requirements for ongoing monitoring; and
- Determination of whether the Request for Information (RFI) document outlines the security functions the financial institution (FI) intends to incorporate into the contract with an MSSP.

2. Evaluate the requirements definition process.

- Ascertain that all stakeholders are involved; the requirements are developed to allow for subsequent use in Request For Proposals (RFPs), contracts, and monitoring; and actions are required to be documented; and
- Ascertain that the requirements definition is sufficiently complete to support the future control efforts of service provider selection, contract preparation, and monitoring.

3. Evaluate the service provider selection process to determine if:

- An RFI/RFP was completed;
- The FI included RFI/RFP elements appropriate to level of risk;
- The RFP adequately encapsulates the institution's requirements and that elements included in the requirements definition are complete and sufficiently detailed to support subsequent RFP development, contract formulation, and monitoring;
- Any differences between the RFP and the submission of the selected service provider are appropriately evaluated, and that the institution takes appropriate actions to mitigate risks arising from requirements not being met; and
- Due diligence requirements encompass all material aspects of the service provider relationship, such as the provider's financial condition, controls, key personnel, disaster recovery plans and tests, insurance, communications capabilities and use of subcontractors.

4. Evaluate the process for entering into a contract with a service provider.

Consider whether:

- The contract contains adequate and measurable service level agreements;
- Allowed pricing methods adversely affect the institution's safety and soundness, including the reasonableness of future price changes;
- The rights and responsibilities of both parties are sufficiently detailed;
- Required contract clauses address significant issues, such as financial and control reporting, right to audit, ownership of data and programs, confidentiality, subcontractors, continuity of service, etc.;
- Legal counsel reviewed the contract and legal issues were satisfactorily resolved;
- Contract inducement concerns are adequately addressed; and
- Contracts contain the following relative to MSSP engagements:
 - Appropriate MIS reporting commensurate with risk;
 - Agreed upon privileged access rights;
 - Termination rights and appropriate renewal language;

- Timelines for service implementation and explicit responsibilities of the MSSP and the FI;
- The right to modify existing services performed under the contract;
- A security provision in accordance with the FI's security program; and
- Ownership of data generated by proprietary security or third- party monitoring tools owned by the MSSP;
- Determine if the FI has a process to monitor that the MSSP is fulfilling their obligations outlined within the contract (e.g. Service Level Agreements (SLAs), Knowledge Performance Indicators (KPIs)/Knowledge Risk Indicators (KRIs)).

5. Evaluate the overall governance of the MSSP program.

- Appraise senior management support of the use of MSSPs;
- Review reports related to MSSP compliance with FI information security program;
- Assess changes to the information security program arising from the use of MSSPs; and
- Evaluate MIS reports provided to FI from MSSPs.

6. Evaluate the institution's process for monitoring the risk presented by the service provider relationship. Ascertain that monitoring addresses:

- Key service level agreements and contract provisions;
- Financial condition of the service provider;
- General control environment of the service provider through the receipt and review of appropriate audit and regulatory reports;
- Service provider's disaster recovery program and testing;
- Information security;
- Insurance coverage;
- Subcontractor relationships including any changes or control concerns;
- Foreign third party relationships; and
- Potential changes due to the external environment (i.e., competition and industry trends).

7. Review policies regarding periodic ranking of service providers by risk.

The decision process should:

- Include objective criteria;
- Support consistent application;
- Consider the degree of service provider support for the institution's strategic and critical business needs; and
- Specify subsequent actions when rankings change.

8. Evaluate the financial institution's use of user groups and other mechanisms to monitor and influence the service provider.

Objective 4: Discuss corrective action and communicate findings.

1. Determine the need to complete Tier II Procedures for additional validation to support conclusions related to any of the Tier I Objectives.

2. Review preliminary conclusions with the EIC regarding:

- Violations of law, rulings, regulations;
- Significant issues warranting inclusion in the Report as matters requiring attention or recommendations; and
- Potential impact of your conclusions on the institution's risk profile and composite or component IT ratings.

3. Discuss findings with management, and obtain proposed corrective action for significant deficiencies.

4. Document conclusions in a memo to the EIC that provides report ready comments for the Report of Examination and guidance to future examiners.

5. Organize work papers to ensure clear support for significant findings by examination objective.

TIER II OBJECTIVES AND PROCEDURES

A. IT REQUIREMENTS DEFINITION

1. Review documentation supporting the requirements definition process

to ascertain that it appropriately addresses:

- Scope and nature;
- Standards for controls;
- Minimum acceptable service provider characteristics;
- Monitoring and reporting;
- Transition requirements;
- Contract duration, termination, and assignment; and
- Contractual protections against liability.

B. DUE DILIGENCE

1. Assess the extent to which the institution reviews the financial stability

of the service provider:

- Analyzes the service provider's audited financial statements and annual reports;
- Assesses the provider's length of operation and market share;
- Considers the size of the institution's contract in relation to the size of the company;
- Reviews the service provider's level of technological expenditures to ensure on-going support; and
- Assesses the impact of economic, political, or environmental risk on the service provider's financial stability.

2. Evaluate whether the institution's due diligence considers the following:

- References from current users or user groups about a particular vendor's performance;

- The service provider's:
 - Experience and ability in the industry;
 - Experience and ability in handling situations similar to the Institution's environment and operations;
 - Shortcomings in the service provider's expertise that the institution may need to supplement in order to fully mitigate risks;
 - Proposed use of third parties, subcontractors, or partners to support the outsourced activities;
 - A ability to respond to service disruptions;
 - Assigning of Key personnel that would support the institution;
 - Ability to comply with appropriate federal and state laws.
 - In particular, ensure management has assessed the providers' ability to comply with federal laws (including GLBA and the USA PATRIOT Act);
- The cost for additional system and data conversions or interfaces presented by the various vendors; and
- Country, state, or locale risk.

3. Evaluate how the FI determines whether the MSSP meets its risk profile.

Consider whether the FI:

- Performed an onsite visitation of the MSSP; Considered business changes at the MSSP;
- Assessed the extent of MSSP use of subcontractors and if any will be performed by an offshore entity; and
- Evaluated controls over sensitive data where offshore subcontracting is performed.

C. SERVICE CONTRACT

1. Verify that legal counsel reviewed the contract prior to signing. Ensure that:

- Legal counsel is qualified to review the contract particularly if it is based on the laws of a foreign country or other state; and

- Legal review includes an assessment of the enforceability of local contract provisions and laws in foreign or out-of-state jurisdictions.

2. Verify that the contract appropriately addresses:

- Scope of services;
- Performance standards;
- Pricing;
- Controls;
- Financial and control reporting;
- FI's right to audit;
- Ownership of data and programs;
- Confidentiality and security;
- Regulatory compliance;
- Indemnification;
- Limitation of liability;
- Dispute resolution;
- Contract duration;
- Restrictions on, or prior approval for, subcontractors;
- Termination and assignment, including timely return of data in a machine-readable format;
- Insurance coverage;
- Prevailing jurisdiction (where applicable);
- Choice of law (foreign outsourcing arrangements);
- Regulatory access to data and information necessary for supervision; and
- Business Continuity Planning.

3. Review service level agreements to ensure they are adequate and

measurable. Consider whether:

- Significant elements of the service are identified and based on the institution's requirements;
- Objective measurements for each significant element are defined;
- Reporting of measurements is required;
- Measurements specify what constitutes inadequate performance; and
- Inadequate performance is met with appropriate sanctions, such as reduction in contract fees or contract termination.

4. Review the institution's process for verifying billing accuracy and monitoring any contract savings through bundling.

D. MONITORING SERVICE PROVIDER RELATIONSHIP(S)

1. Evaluate the institution's periodic monitoring of the service provider relationship(s), including:

- Timeliness of review, given the risk from the relationship;
- Changes in the risk due to the function outsourced;
- Changing circumstances at the service provider, including financial and control environment changes;
- Conformance with the contract, including the service level agreement; and
- Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship.

2. Determine if adequate in house expertise exists to manage an MSSP relationship by evaluating:

- FI management's understanding of the MSSP's process, procedures, and protocols;
- Whether the FI has a thorough understanding of the data the MSSP is collecting and whom has access to the data; and
- The training, education, and awareness provided by the MSSP to the FI.

3. Relative to contingency and event planning between the FI and an MSSP. Evaluate:

- The most recent business continuity test with the MSSP; review the results, lessons learned and issues to be addressed;
- How the FI monitors the MSSP's BCP plan and testing results;
- The process to develop and maintain incident response processes that include the MSSP;
- How the MSSP roles and responsibilities have been established; and
- Provisions in the FI's contingency plan for continuance of processing activities, either in-house or with another vendor, in the event that the vendor is no longer able to provide the contracted services or the arrangement is otherwise terminated unexpectedly.

4. Relative to ongoing monitoring of an MSSP relationship, the

following should be considered:

- Event notification procedures, response time expected, and actions the MSSP will take to protect the FI;
- Clearly defined support to be provided during and after "events," (e.g., incident response, forensics, etc.);
- How the MSSP provides continuous monitoring of the FI;
- The quality of the management information reports the MSSP provides to the FI; and
 - Determine if reports include status of security, incidents, business continuity plans, and financial condition.
- How management at the FI is periodically updated regarding MSSP activities. Assess the scope of reporting including risk assessments, information security, significant incidents, business continuity, and financial condition.

5. Review risk rankings of service providers to ascertain:

- Objectivity;
- Consistency; and
- Compliance with policy.

6. Review actions taken by management when risk rankings change, to ensure policy conformance when rankings reflect increased risk.

7. Review any material subcontractor relationships identified by the service provider or in the outsourcing contracts. Ensure:

- Management has reviewed the control environment of all relevant subcontractors for compliance with the institution's requirements definitions and security guidelines; and
- The institution monitors and documents relevant service provider subcontracting relationships including any changes in the relationships or control concerns.

8. Determine if there is adequate coordination between the FI's security policies and the policies/practices of the MSSP.

Consider whether:

- There is clear understanding of responsibility and accountability during a security event (i.e., incident response);
- The FI has considered access controls surrounding the systems, devices and data that the MSSP can access;
- Effective change control processes and communication exist between the FI and MSSP;
- The quality of the log collection of the MSSP and related Security Information and Event Management tools;
- The quality of the physical security around devices that are owned and/or maintained by the MSSP on the FI's premises;
- The FI's data is maintained in separate client logs at the MSSP; and
- Monitoring for security events/incidents is being conducted by the MSSP on a real-time system (e.g., security console)



Federal Financial Institutions Examination Council

FFIEC

Retail Payment Systems

April 2016

RPS

IT EXAMINATION

HANDBOOK

Table of Contents

Introduction	1
Retail Payment Systems Overview	2
Payment Instruments, Clearing, and Settlement	4
Check-Based Payments	6
Remotely Created Checks	8
Electronically Created Payment Orders	10
Remote Deposit Capture	10
Check Clearing Houses	11
The Automated Clearing House (ACH)	13
The ACH Network	13
NACHA Rule and Product Changes	16
Card-Based Electronic Payments	17
General Purpose Credit Cards	18
Co-Branded/Affinity Credit Cards	19
Debit and ATM Cards	21
EFT/POS Networks	22
Prepaid (Stored Value) Cards	24
Payroll Cards	25
General Spending Reloadable Cards	27
Online Person-to-person (P2P), Account-to-Account (A2A) Payments and Electronic Cash	30
Emerging Retail Payment Technologies	32
Contactless Payment Cards, Proximity Payments and Other Devices	33
Biometrics for Payment Initiation and Authentication	33
Emerging Network Technologies	33
Retail Payment Systems Risk Management	35
Payment System Risk (PSR) Policy	36
Strategic Risk	37

Credit Risk	38
Liquidity Risk	40
Legal (Compliance) Risk	40
Operational Risk	42
Audit	44
Information Security	45
Business Continuity Planning	47
Vendor and Third-Party Management	48
Retail Payment Instrument Specific Risk Management Controls	49
Checks	49
ACH	50
Third-Party ACH Processing	52
Credit Cards	53
Debit/ATM Cards	54
Card/PIN Issuance	54
Merchant Acquiring	55
EFT/POS and Credit Card Networks	60
Appendix A: Examination Procedures	A-1
Appendix B: Glossary	B-1
Appendix C: Schematic of Retail Payments Access Channels & Payments Method	C-1
Appendix D: Laws, Regulations, and Guidance	D-1
Appendix E: Mobile Financial Services	E-1

Introduction

The FFIEC IT Examination Handbook (IT Handbook), "Retail Payment Systems Booklet" (booklet), provides guidance to examiners, financial institutions, and technology service providers (TSPs) ^[1] on identifying and controlling risks associated with retail payment systems and related banking activities. ^[2]

Financial institutions accept, collect, and process a variety of payment instruments and participate in clearing and settlement systems. In some cases, financial institutions perform all of these tasks. However, independent third parties are increasingly involved in this process, introducing new risks that affect the security of financial institutions. Financial institutions, acting either in consortiums or independently, remain the core providers to businesses and consumers for most retail payment instruments and services. Federal government-affiliated providers and operators, such as the Federal Reserve Banks (Reserve Banks), also compete with numerous financial institutions and private sector firms in providing various services in support of retail payments.

Recently, a number of new payment instruments have emerged that are largely or wholly electronic. Electronic payment systems offer efficiency gains by allowing for rapid and convenient transmission of payment information among system participants. However, the emergence of a new payment mechanism can also enable the rapid propagation of fraud, money laundering, and operational disruption if data is compromised. Another trend associated with emerging payments is the increased participation of nonbank third parties in retail payment systems and a lengthened transaction chain, which may increase risk in payment processes. Management of retail payments risk is increasingly difficult and requires diligent oversight of third-party service providers.

Much of the guidance in this booklet, involving traditional retail payment systems, has not been revised significantly because of the maturity of these systems in the product life cycle. Mature payment systems are better understood, whereas emerging payment systems require a closer look to better understand the risks and associated controls. New guidance is offered for remotely created checks (RCCs), electronically created payment orders, automated clearing house (ACH) transactions, The Check Clearing for the 21st Century Act (Check 21), ^[3] and Merchant Card Processing due to recent developments in these areas. Also, this booklet includes a new section that covers some emerging technologies in retail payment systems. Additional emphasis is placed on the need for improved operational, credit, legal, and compliance risk processes for retail payment products, especially for the deployment of remote and Internet-based check and ACH capture systems.

Examination guidance for Retail Payment Systems is provided in three sections, followed by examination procedures, a glossary, and references:

- Retail Payment Systems Overview-The first section of the booklet presents an overview of retail payment systems, grouping retail payment instruments in various categories, including: checks, card-based electronic payments, and other electronic payments, such as person-to-person (P2P), electronic benefits transfer (EBT), and ACH.
- Payment Instruments, Clearing, and Settlement-The second section of the booklet

describes the retail payment system instruments typically offered by financial institutions and the roles of various payment system participants, including third parties. Diagrams showing the typical payment flows and clearing and settlement arrangements for each of the retail payment instruments described are also included.^[4]

- **Retail Payment Systems Risk Management**-The third section describes the risks associated with various retail payment systems and instruments, using the regulatory risk categories: strategic, credit, liquidity, settlement, legal/compliance, and operational/transaction risk. This section also presents the risk management practices financial institutions should implement in order to mitigate the risks described, and it concludes with specific controls appropriate to a number of retail payment instruments. Management action summaries for selected risks and functions are also included in this section, providing a snapshot of the risks and risk management practices described in the text.

This booklet includes a number of references to other IT Handbook booklets, including "Information Security," "Business Continuity Planning," "Audit," "Outsourcing Technology Services," "Electronic Banking," and "Wholesale Payment Systems." Also, there are references to FFIEC guidance for Bank Secrecy Act examinations that are relevant to retail payment systems and for Check 21. In addition to describing the IT risks and controls, the booklet also discusses certain credit and liquidity risks that may also be present when providing retail payment services. A full review of a particular financial institution's retail payment system environment will require an interdisciplinary team of examiners with experience in operational, credit, liquidity, and compliance risks.

Examiners should use the examination procedures for evaluating the risks and risk management practices at financial institutions offering retail payment system products and services. These procedures address services and products of varied complexity; therefore, examiners should adjust the procedures, as appropriate, for the scope of the examination and the risk profile of the institution. The procedures may be used independently or in combination with procedures from other IT Handbook booklets and agency-specific handbooks and guidance documents.

Retail Payment Systems Overview

Retail payments usually involve transactions between two consumers, between consumers and businesses, or between two businesses. Wholesale payments are typically made between businesses. Although there is no definitive division between retail and wholesale payments, retail payment systems generally have higher transaction volumes and lower average dollar values than wholesale payment systems. This section provides background information on payments typically classified as retail payments. The following are examples of typical retail payments. These retail payments may involve the use of various retail payment instruments or access devices (e.g., checks, ACH, card, phones, etc.).

Purchase of Goods and Services-Purchase of goods and services can occur at the point-of-sale (POS) (e.g., in person at a merchant location, through the Internet, or by telephone). These payments include attended POS payment transactions for goods or services, such as with traditional retailers, and unattended payment transactions, as with

vending machines. Increasingly, traditional retailers such as grocers and home improvement stores are using unattended payment systems at the POS as well. As technology advances, the consumer can purchase goods and services remotely without physical presence at the POS, such as via the Internet or a telephone/mobile phone. Payment instruments for retail purchases of goods and services have expanded beyond traditional vehicles (i.e., cash, checks, and credit and debit cards) to prepaid cards, contactless debit and credit cards, and other contactless devices such as key fobs, mobile phones. In addition, merchants may convert checks to electronic form at the POS, and use the ACH system for clearing and settlement.

Bill Payment-Consumers may elect to pay (or provide payment instructions for) recurring or nonrecurring bills and invoices via electronic bill payment. A particular biller's periodic recurring invoices can be electronically paid individually or set up to be paid automatically to a payment schedule. In recent years, there has been a growing trend toward payment of recurring and nonrecurring bills using Internet-based bill payment services.

P2P Payments-The vast majority of consumer-to-consumer payments are conducted with checks and cash, with some transactions using electronic P2P payment systems. The expansion of systems that permit customers to conduct P2P payments is anticipated through account-to-account (A2A) transfers, which use either the ACH or Automated Teller Machine (ATM) networks for movement of funds.

A2A Payments-With A2A payments, the consumer moves funds from his or her account at a financial institution to the account of another individual or business at the same or a different financial institution. The emerging use of the ATM networks for movement of funds may allow same day availability of funds at a cost far less than traditional wire transfer systems.

Cash Withdrawals and Advances-Consumers use retail payment instruments to obtain cash from merchants or ATMs. For example, consumers can use a credit card to obtain a cash advance through an ATM or an ATM or debit card to withdraw cash from an existing account. Consumers can also use personal identification number (PIN)-based debit cards to withdraw cash at an ATM or receive cash back at some POS locations.

Retail payment systems continue to evolve with advances in technology. These advances enable financial institutions to develop new products and services, lower the barriers to business entry for smaller institutions, and exploit economies of scale.

Recent changes in payments technology have influenced three important trends in retail payments. First, as firms seek economies of scale, the banking industry has witnessed the rapid consolidation of retail payment service providers, credit issuers, merchant acquirers, processing companies, and check processors. As a result, some small and mid-sized financial institutions have exited the business and outsourced certain functions of the retail payments process to larger financial and non-financial institutions. Nonbanks, in particular, are assuming more roles in retail payment systems such as the clearing and settlement payment functions and the issuance and processing of electronic payment cards and other devices.

The second trend is the shift from paper to electronic payments as technology has converged with the change in consumers' and merchants' preferences for convenient and low cost payment alternatives. The most significant growth is seen in debit and prepaid cards (stored value cards), followed by the increased use of Internet services like online banking and bill pay. The volume of checks and cash payments continues to decrease, with cash usage declining at a much slower rate. The emergence of new

electronic payment vehicles in the U.S. is anticipated as they are adopted in the global market.

Use of automated bill pay is a third important trend. Although consumers traditionally used checks for a large portion of bill payments in the U.S., direct bill payment through the ACH system are increasingly popular. More recently, retail firms have used check-to-ACH conversion processes to allow electronic settlement, thereby reducing the number of checks that flow through the payment system.

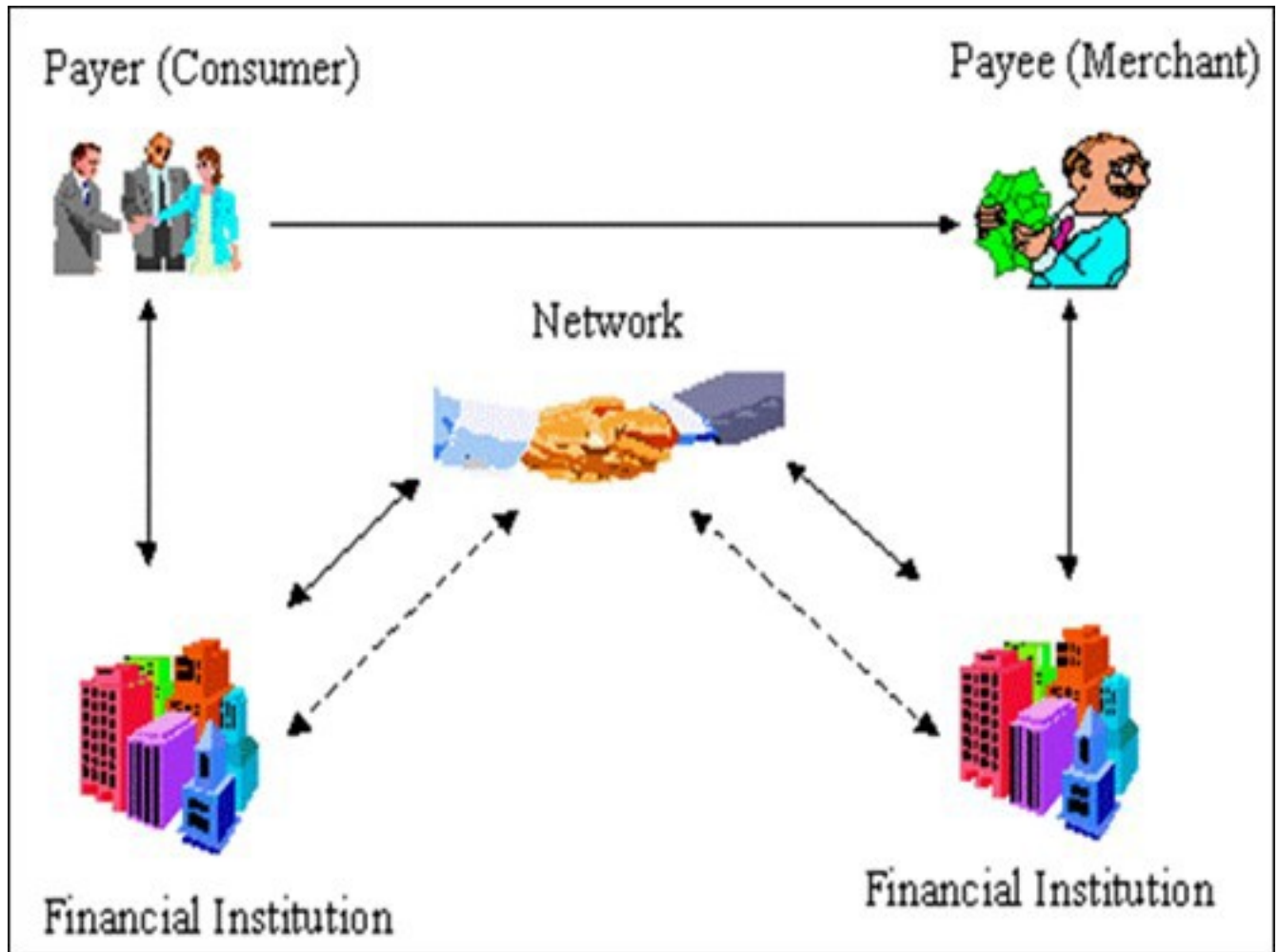
International retail payments are relatively new in the ACH industry and are largely driven by businesses and consumers seeking cost reductions for funds transfers across borders. Several financial institutions maintain their own proprietary systems, and more recently the Reserve Banks began offering FedACH International Services. FedACH International provides a means of transmitting funds between the U.S. and other countries using NACHA - The Electronic Payments Association (NACHA) rules. ^[5]

Beginning September 18, 2009, a new Standard Entry Class (SEC) code became effective that is expected to facilitate compliance due diligence with the use of the ACH system for international payments. The International ACH Transaction SEC code (IAT) will enable financial institutions to identify international ACH payments and perform the due diligence required by the U.S. Office of Foreign Assets Control.

Consumer and merchant acceptance of all the technological changes has been vital to the success of emerging retail payment systems and products. Consumers have shown willingness to accept new retail payment technologies more quickly because of the convenience afforded by these new services.

Payment Instruments, Clearing, and Settlement

This section provides an overview of the various payment instruments and clearing and settlement processes used for different retail payment systems. Although the diagrams reflect the general flow of transactions and participants, in many cases, other third parties may facilitate one or more processing functions.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 1: Four-Corner Payments Model

Figure 1 displays the clearing and settlement process for retail payments using a standard four-corner payments model. While the flow of information and funds is different for each payment instrument, there is a common set of participants for retail payments. The initiator of the payment, typically a consumer, is located in the upper left-hand corner of the diagram. The recipient of the payment, typically a merchant, is in the upper right-hand corner of the diagram. The lower two corners of the model represent the relationship of the consumer and merchant with their financial institutions. The payments networks or clearing house organizations that route the transactions between financial institutions are in the middle of the chart. In subsequent model figures, solid lines represent the flow of information, and dashed lines represent the flow of funds. This generic figure can be applied to all retail payments.

More financial institutions are engaging third-party service providers to act on their behalf rather than keeping all payment functions in-house. In some instances, such as in check

clearing, a financial institution may exchange check items directly with another financial institution without using an intermediary.

There are a variety of retail payment clearing and settlement systems. These include; check clearing systems, ACH networks, ATM networks, and bankcard networks. Check clearing systems can be paper-based or electronic. Check 21 is facilitating the expanded use of electronic imaging technologies in check processing, enabling the banking industry to improve the efficiency and cost-effectiveness of check processing operations.

ACH payments also have grown significantly as consumers are using more direct bill payments through the ACH. More recently, retail firms have employed check-to-ACH conversion processes to obtain the efficiencies of electronic processing, reducing the number of checks that flow through the payment system.

Internet-based bill payment systems are transaction origination platforms that allow customers to initiate bill payments through existing payment systems. Depending on the bill payment software implemented, the payment transaction may be processed through ATM, ACH, or check systems. ^[6] The following sections describe these systems in more detail.

Debit and credit cards, particularly signature and PIN debit, have driven much of the growth in electronic payments. The recent introduction of contactless payment cards is expected to contribute to the increase of merchant acceptance and financial institution issuance of cards and investment in contactless payment infrastructure.

Retail payments often move through multiple channels, which results in data being processed and stored on multiple systems that are typically outside of the direct control of the customer's financial institution. There are two primary challenges for financial institutions in managing these complex payment systems. First, the lack of interoperability ^[7] that often characterizes these systems and the associated lack of optimal data protocols may result in data integrity issues. Second, the complexity of systems increases the difficulty of the management of data security and system availability.

Check-Based Payments

Checks are the traditional method that consumers can use to access their accounts. A check contains the names of the payer and the payee, the payer's account number, amount of the check, and the name and routing number of the paying financial institution. The magnetic ink character recognition (MICR) line at the bottom of the check enables high-speed reader/sorter equipment to process checks. Before financial institutions process checks, they encode the amount of the check in magnetic ink at the bottom of the check. Check formats are governed by standards developed by the Accredited Standards Committee (ASC) on Financial Services, X9B Committee, which works under procedures sanctioned by the American National Standards Institute (ANSI). ^[8]

Check processing has undergone a transformation during the past five years; a trend that is expected to continue for the next several years. Until recently, consumers in the United States used checks more often than any other retail payment instrument other than cash. However, in an increasing number of payment situations, checks are no longer the most convenient payment instruments for consumers, or the most cost-

effective payment method for financial institutions and merchants. Checks comprise a decreasing percentage of the total noncash payment volume in the United States. Many consumers use checks merely for person-to-person transactions that are not conducive to electronic payments, and have shifted to electronic payments for POS transactions and bill payment. In addition, a significant volume of checks are converted to ACH debits at POS and at lock-box operations.

Legal developments have affected the processing of checks as well. Check 21, which became effective on October 28, 2004, has succeeded in reducing check processing times as well as the float period previously associated with physical processing. By authorizing the use of a new negotiable instrument called a substitute check, Check 21 facilitates the broader use of electronic check processing.

A properly-prepared substitute check is the legal equivalent of the original check and includes all the information contained on the original check. The law does not require financial institutions to accept checks in electronic form, nor does it require financial institutions to use the new authority granted by the act to create substitute checks. The law permits financial institutions to truncate ^[9] original checks, process the check information electronically, and deliver substitute checks to financial institutions that wish to receive paper checks in lieu of electronic alternatives.

For many financial institutions, implementing a Check 21 strategy involves a significant investment in new hardware and software as well as the reengineering of check processing routines. Consequently, financial institutions should deploy Check 21 with appropriate risk management, including strategic planning, project management, and vendor management. Check 21 requires the bank ^[10] that creates a substitute check, the reconverting bank, to warrant that there will not be duplicate presentments of the check (or copy or representation thereof) and that the substitute check is an accurate representation of the original check as of the time the original check was truncated. Such substitute checks must meet specific requirements to be treated as a legal equivalent, and the bank that creates a substitute check must indemnify other parties for losses that result from their receipt of a substitute check instead of the original check.

Financial institutions implementing a Check 21 strategy must consider new processes for imaging checks, transferring files of imaged checks, and archiving and retrieving imaged checks. For example, a number of financial institutions are implementing remote check capture systems in their branches and processing centers as a means of significantly reducing check transit costs. Some financial institutions are providing selected customers with remote check capture devices. Examiners are encouraged to review the FFIEC's guidance for Risk Management of Remote Deposit Capture. ^[11]

Another important catalyst for the changes taking place in payment systems is electronic check conversion, a process in which information from a check is used to create an ACH debit. The conversion may occur at a retailer's POS, or at lock-box processing centers to which a consumer mails checks. Electronic check conversion is similar to, but separate from, the check substitution process authorized by Check 21. Instead of using the image of a paper check, as in the Check 21 process, the recipient uses the account and financial institution information contained on the consumer's check to create a new electronic payment through either the ACH or debit card networks. ^[12]

ACH electronic fund transfers between financial institutions are not considered check transactions; thus, they are not subject to laws governing check processing. Rather, they are governed by the rules of the ACH that processes the electronic fund transfer. ACH transactions to or from consumer accounts also are subject to the provisions of the Federal Reserve Board's Regulation E, Electronic Fund Transfers.

Evolution of Electronic Check Collection

Two general models of electronic check collection are emerging as a result of the passage of Check 21. Each model has its advantages and disadvantages. In one model, check images including the MICR payment information are transmitted to the paying financial institution. These institutions do not have to rely on multiple image archive providers (with whom they may have no direct contractual relationship) to obtain check images for customer online banking services and back-room operations.

In a second model, only the MICR information is transmitted to the paying financial institution while the check images are stored in remote archives that can be accessed on demand. The MICR information on a check could be transmitted through a dedicated network or possibly the ACH network. A small number of centralized check-image archives could be more cost-effective and might not increase risk appreciably or degrade customer service.

As electronic check collection methods evolve, efficiencies may develop to make one method superior to the other. Notwithstanding, electronic check collection methods will continue to pose certain risks. Frequently-used services that utilize both image and ACH technologies are remotely created checks (RCCs), electronically created payment orders, and remote deposit capture (RDC). Each of these is discussed in the sections that follow.

Remotely Created Checks

A closely related transaction to electronic check conversion, in that there is an authorization to debit an account, is the RCC.^[13] An RCC does not bear the signature of a person on whose account the check is drawn. In place of the signature, the RCC bears the account holder's printed or typed name or a statement that the account holder authorized the check.^[14] The account holder can authorize the creation of an RCC by telephone by providing the appropriate information, including the MICR data. Common examples of RCCs are those created by a credit card company, utility company, or telemarketer. RCCs may be processed through the check clearing networks or converted and processed as an ACH debit.

The risk of fraud associated with RCCs is similar to the risk associated with other kinds of debits that post to bank accounts. A fraudster might obtain an account holder's account number by copying that information from one of the account holder's authorized checks, or by tricking the account holder into providing the information over the telephone or the Internet. Once a fraudster obtains the account information, he or she has the data necessary to originate unauthorized RCC transactions through the check collection system or the ACH network. As with all payment systems and mechanisms, a financial institution must also assume responsibility for an effective system of internal controls and ongoing account monitoring related to RCCs.

For RCCs, the check and ACH rules differ as to how an accountholder receives a re-credit for an unauthorized transaction and how the loss is allocated among the participating financial institutions. ACH debits to consumer accounts are governed by applicable ACH rules and by the Electronic Fund Transfer Act and Regulation E. Unauthorized checks posted to consumer accounts are governed by check law, which includes the Uniform Commercial Code (UCC), as enacted in the applicable state, as well as the Expedited Funds Availability Act, as implemented by the Federal Reserve

Board's Regulation CC. In instances when checks are converted to ACH entries, applicable ACH rules apply.

If an unauthorized ACH debit is posted to a consumer's account, Regulation E gives the consumer 60 days after an institution transmits to the consumer a periodic account statement to report that the ACH debit was unauthorized. Regulation E imposes obligations on the consumer's financial institution with respect to error resolution procedures and refunds of unauthorized payments. When a consumer receives a refund for an unauthorized ACH debit, ACH rules permit the consumer's financial institution to recover the amount of the unauthorized payment by returning the debit item to the originating financial institution within the time permitted.

In the case of checks, a financial institution may not charge a customer's account for a check that is not properly payable from that account. The customer has a right to a re-credit for an unauthorized check so long as the customer makes the claim within the time frame permitted by the UCC and the account agreement. Unlike Regulation E, the UCC does not contain specific re-credit procedures that a financial institution must follow. With respect to the allocation of losses for unauthorized checks between financial institutions, the risk of loss falls generally on the paying financial institution, which historically has been in the best position to determine the validity of the drawer's signature. Under the UCC, a paying financial institution becomes accountable for a check unless it returns the check by its midnight deadline.^[15] With the exception of an RCC, if a paying financial institution re-credits a customer's account for an unauthorized check, generally it cannot make a claim against a previous financial institution for an unauthorized drawer's signature after the midnight deadline has passed.

In response to the perceived risk of fraud, legal initiatives have shifted the risk related to unauthorized RCCs from the paying financial institution to the bank of first deposit. This shift is based on the theory that, for unauthorized RCCs, the bank of first deposit is in the best position to know its customer (the creator of the RCC) and to determine the legitimacy of its customer's deposits. A UCC revision that reallocates this risk for RCCs has not yet been widely adopted by the states. Among the states that have enacted amendments to the UCC, the definitions and warranties are not uniform in their scope or requirements. Under the pre-existing provisions of the UCC, the paying financial institution, not its customer, is responsible for unauthorized checks. Providing the paying financial institution with the ability to recover against the financial institution that presented the unauthorized RCC can make it easier for customers to obtain re-credits.

The Federal Reserve Board amended Regulation CC effective July 1, 2006, to reallocate the risk of loss resulting from unauthorized RCCs. Under the amendments, any financial institution that transfers or presents an RCC warrants that the person on whose account the check is drawn authorized the issuance of the check in the amount and to the payee stated on the RCC. The warranty applies only to financial institutions and does not directly create any new rights for checking account customers. Also, any financial institution that received an RCC from another financial institution has up to a year to make a claim against the transferring financial institution for an unauthorized RCC. Similarly, the Board amended Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire (Regulation J) in 2006 to clarify that the new warranties apply to RCCs collected through the Reserve Banks. In conjunction with Regulation CC, Regulation J shifted the liability for losses attributable to unauthorized RCCs to the depository financial institution where the check is first cashed or deposited.

Because RCCs are cleared in the same manner as traditional checks, and because nothing unique identifies a check as an RCC unless the signature block on the check is

examined, there is currently no efficient way of measuring the volume or use of RCCs.

Electronically Created Payment Orders

An electronically created payment is a new retail payment practice in which a merchant takes payment instructions for goods and services and places them in an electronic template that creates an electronic file for processing through the check clearing networks. Unlike traditional checks or RCCs, electronically created payment orders do not begin with a paper item. However, they are similar to RCCs in that they are typically initiated with Internet or telephone instructions from the consumer and bear no direct evidence of the customer's authorization. Because these transactions are not originally captured from paper check items, the laws and regulations pertaining to check collection do not apply.

Ordinarily, electronic debits that a consumer uses to acquire goods or services are cleared through the ACH network, which includes a transaction code that clearly indicates the nature and source of the transaction. When a financial institution permits the creation of electronic payment orders, substantial risk-management oversight for unauthorized returns and other unlawful activity is lost because the check-clearing networks do not provide the level of technological and organizational controls of those in the ACH network. This lack of systemized monitoring of the electronically created payment orders increases the susceptibility to fraud by Web-based vendors and telemarketers.

The Federal Reserve Banks handle electronic check images only if they were created from an original paper check. On June 15, 2008, the Federal Reserve Banks revised Federal Reserve Bank Operating Circular 3 (Circular 3) ^[16] to clarify that a depository institution that sends an electronic check file to the Reserve Banks is liable for the legitimacy of the items in that file. Reserve Banks only accept applicable liability and offer certain warranties for Check 21 transactions that begin with an original paper check item. Because electronically created payment orders generally are indistinguishable from electronic images of paper checks, collecting banks, such as the Reserve Banks, may not be able to avoid accepting the electronically created payment orders. However, pursuant to the revised Circular 3, the bank that sends the item to the Reserve Bank ultimately assumes liabilities and provides warranties for its legitimacy.

Remote Deposit Capture

Remote Deposit Capture (RDC), the digital processing of paper checks and monetary instruments at remote locations for deposit and clearing through the check (image) or ACH networks, has expanded rapidly in recent years and is being used at financial institutions and at customer locations. ^[17]

Although remote deposit-taking is not a new activity, RDC should be viewed as a new delivery system and not simply as a new service. Prior to implementing RDC, senior management should identify and assess the legal, compliance, and operational risks associated with the new system. They should ensure that RDC is compatible with the institution's business strategies and should understand the return on investment and management's ability to manage the risks inherent in RDC. Management should incorporate their assessments of RDC systems, including products and services, into existing risk assessment processes.

With RDC, the depository and collecting financial institutions may choose either to send or accept a substitute check or to engage in electronic check presentment (ECP) where data and images captured from the original checks are used to complete payment transactions. RDC includes deposit capture at the financial institution's teller line and backroom processing, at ATMs, and at customer locations. RDC at customer locations allows the customer to make deposits by scanning items on its own premises and sending either the image of the deposit item for processing through the check clearing networks or merely the deposit data for processing and clearing through the ACH network. RDC also may include the electronic capture of deposit information comprised of cash or other items such as electronic deposits made through a remote safekeeping arrangement at the customer location or through another intermediary.

Financial institutions have a greater degree of control over RDC activities deployed at wholly owned or controlled locations. Based on the RDC configuration used and on the customer's operations, RDC at a customer location increases the financial institution's legal, compliance, and operational risks to varying degrees. Legal and compliance risks could be significant depending on the effectiveness of controls and legal agreements that are in place. The use of RDC by international correspondents' customers is increasing. RDC is effectively replacing correspondent cash letter pouch activity. BSA/ AML controls over RDC pouch activity should also cover RDC and should be commensurate with the increased volumes. Operational risks at the customer location include unauthorized access to technology systems and electronic data images, an inability to maintain system compatibility with financial institution systems, ineffective controls over physical deposit handling and storage procedures, inadequate record retention programs, and exposure to money laundering and fraud.

The Management Booklet of the IT Handbook and the FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual ^[18] provide additional descriptions of risk management processes.

Check Clearing Houses

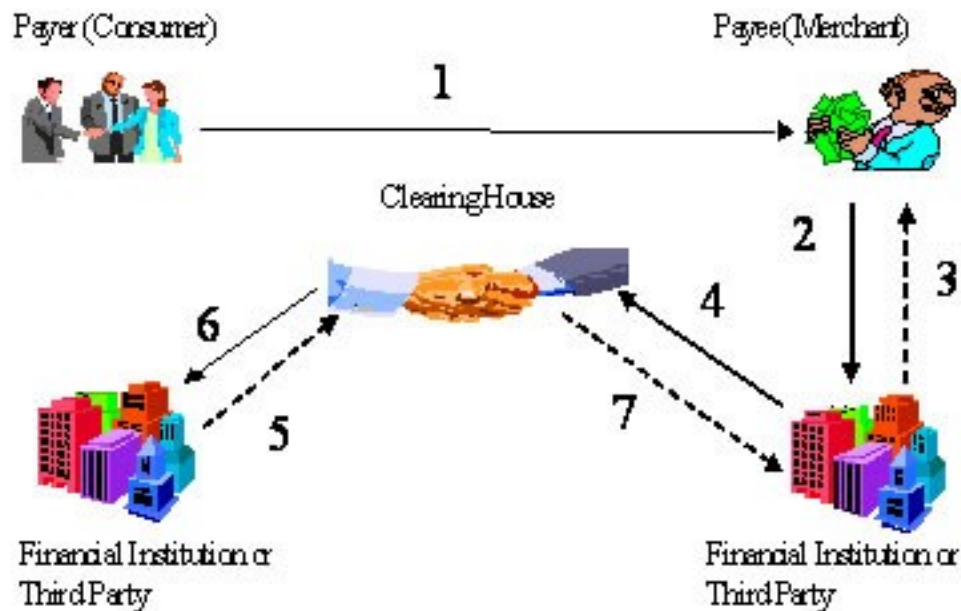
Financial institutions clear and settle checks in different ways depending on whether the checks are "on-us" (checks deposited at the same institution on which they are drawn) or interbank or transit checks (the payer and payee have accounts at different financial institutions). On-us checks do not require interbank clearing or settlement. Interbank or transit checks can clear and settle through direct presentment, a correspondent financial institution, a clearing house, or other intermediaries such as the Reserve Banks.

Under direct presentment, depository financial institutions can present checks directly to the paying financial institution. The paying financial institution may settle with the depository financial institution through a pre-arranged settlement agreement or by sending Fedwire® funds transfers through the Reserve Banks. ^[19]

Correspondent financial institutions, acting on behalf of other depository financial institutions (known as respondents), can settle the checks they collect by using accounts on their books or by using their Reserve Bank reserve account. Smaller depository institutions typically use the check-collection services of correspondent financial institutions or the Reserve Banks.

Financial institutions can also clear checks through a Reserve Bank or through an independent clearing house where they have formed voluntary associations that

establish an exchange for checks drawn on them. With the advent of Check 21, a number of vendors have begun to offer processes and systems for imaging, transferring, archiving, and retrieval of checks. Many financial institutions participating in check clearing houses use the Federal Reserve's National Settlement Service (NSS) to effect settlement for checks exchanged each business day.^[20]



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 2: Check Clearing and Settlement

Figure 2 depicts the typical interbank check clearing and settlement process through a Reserve Bank or clearing house. In step 1 the consumer uses a check to pay a merchant for goods or services. The merchant, after obtaining authorization for the check, accepts the check for payment.^[21] At the end of the day, the merchant accumulates the checks and deposits them with its financial institution for collection (steps 2 and 3). Depending on the location of the paying institution, the funds may not be available immediately. For deposited checks payable at other financial institutions, the merchant's financial institution uses direct presentment for processing or sends the checks to a Reserve Bank, clearing house, or correspondent financial institution (steps 4 and 6). The check or an electronic presentment file is sent to the consumer's financial institution, and the financial institution's account at the correspondent or Reserve Bank is debited (steps 5 and 7).^[22]

Return items are checks that are rejected by the paying financial institution for reasons such as insufficient funds, a closed account, a stop-payment order, fraudulent signature, or failure of the paying financial institution. Return items are a major risk associated with the acceptance of check deposits. The institution that takes a check for deposit may be exposed to credit risk if it releases funds to the depositor and the paying financial institution later returns the check because its customer does not have sufficient funds or

for other reasons.

Regulation CC obligates financial institutions to make deposited funds available for customer withdrawal in accordance with mandatory schedules. Thus, a depository financial institution may be required to make funds available to the customer before an unpaid check is returned to the depository financial institution. When the depository institution receives a return item, it will charge back its depositing customer's account for the item although it had already made the funds available to the customer.

The Automated Clearing House (ACH)

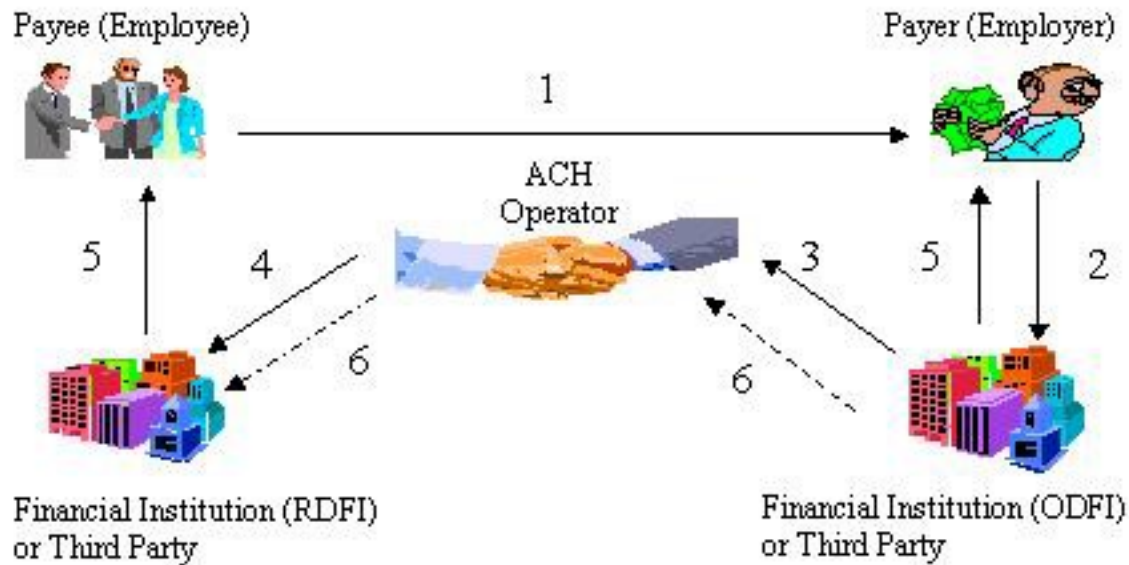
An ACH is an electronic network for the exchange of payment instructions among financial institutions, typically on behalf of customers. ACH transactions are payment instructions to either debit or credit a deposit account. They are batch-processed, value-dated electronic funds transfers between originating and receiving financial institutions. ACH transactions can either be credits, originated by the account holder sending funds (payer), or debits originated by the account holder receiving funds (payee). Financial institutions may contract with third-party service providers to conduct their ACH activities. Unaffiliated independent third parties now generate significant ACH payment activity. NACHA is responsible for the administration, development, and enforcement of the NACHA Operating Rules and sound risk management practices for the ACH Network. ^[23]

The ACH Network

ACH transactions are sent in batches by financial institutions and third-party service providers to ACH operators for processing one or two business days before settlement dates. The ACH operators deliver the transactions to the receiving institutions at defined times. The Electronic Payments Network (EPN), one of the two national ACH operators, is a private processor with a significant share of the national market. ^[24] The Reserve Banks process the remaining share of the market. ACH operators charge a small fee per-transaction to both the originating and receiving depository institutions.

In all ACH transactions, instructions flow from an originating depository financial institution (ODFI) to a receiving depository financial institution (RDFI). An ODFI may request or deliver funds. Transaction instructions and funds are linked using record keeping codes. If the ODFI sends funds, it is a credit transaction. Examples of credit transactions include payroll direct deposit; Social Security payments; dividend and interest payments; and corporate payments to contractors, vendors, or other third parties. If the ODFI requests funds, it is a debit transaction and funds flow in the opposite direction. Examples include collection of insurance premiums, mortgage and loan payments, consumer bill payments, and corporate cash concentration transactions.

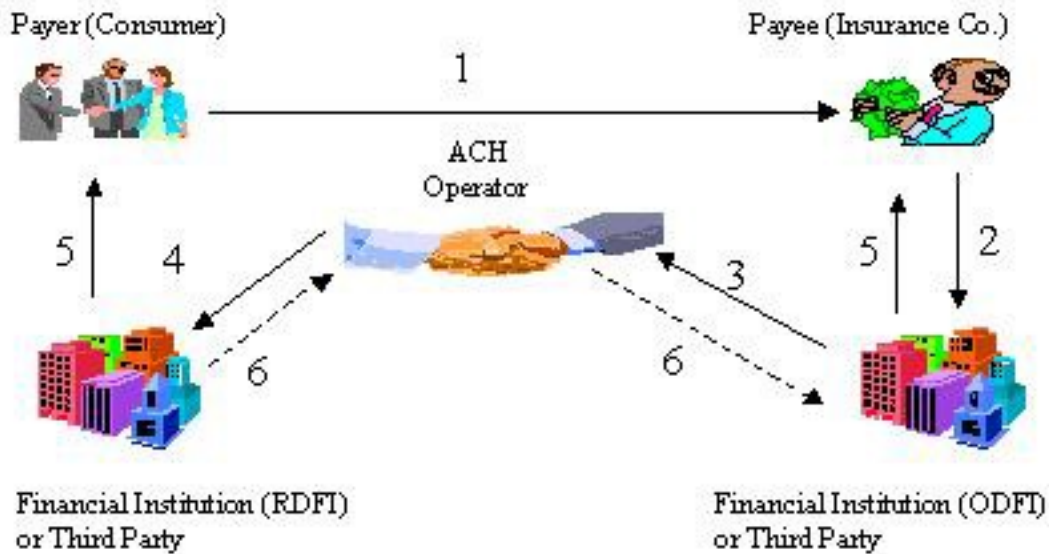
When the ACH files are distributed, financial institutions originating credit payments have a binding commitment for payment to the ACH operator. Settlement for Reserve Bank ACH credit transactions is final at 8:30 a.m. Eastern Time (ET) on the settlement day, when the credits are posted to receiving depository financial institution accounts. Settlement is final for ACH debit transactions, assuming the RDFI has sufficient funds and there are no returns, when posted at 11:00 a.m. ET on the settlement day. ^[25]



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 3: ACH Credit Clearing and Settlement

Figure 3 depicts a typical ACH credit transaction. In this example, the payer is the employer and the payee is the employee. The payee authorizes an employer to deposit his or her paycheck through direct deposit (step 1). The ODFI is the employer's financial institution and the RDFI is the consumer's financial institution. The employer submits its direct deposit payroll ACH files to the ODFI (step 2). The ODFI verifies the files and submits them through the corresponding ACH operator (step 3). The ACH operator routes the transaction to the payee's financial institution, the RDFI (step 4). The RDFI makes the funds available to the payee by crediting his or her account (steps 5). The ACH operator settles the transaction between the participating financial institutions (step 6). If the ACH operator is the EPN, final settlement is made using the Reserve Bank's NSS. If the ACH operator is the Federal Reserve, final settlement is made directly to the financial institution's reserve accounts at a Reserve Bank.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 4: ACH Debit Clearing and Settlement

Figure 4 depicts a typical ACH debit transaction, in this case a recurring monthly insurance premium remittance. The payer sends the ACH payment information and authorization to the payee, in this case an insurance company (step 1). The payee submits this information to its financial institution (step 2), which routes the transaction to an ACH operator (step 3). The ACH operator routes the transaction to the receiving financial institution (step 4). Funds are made available to the payee and the payer's account is debited (step 5). The ACH operator settles the transactions between the participating financial institutions (step 6). Final settlement is performed as described in Figure 3.

An ODFI or an RDFI may outsource ACH processing functions to a third-party service provider, an entity that performs any processing functions on behalf of the ODFI, the originator, or the RDFI, including creation of ACH files or acting as a sending or receiving point. A financial institution may provide the third-party service provider with its Electronic Transaction Identifier (the institution's unique routing number that is used in the ACH network). Third-party senders, customers of the ODFI that provide services to originators, send ACH files on behalf of an originator. ^[26] In a third-party sender model, the ODFI does not have a direct customer relationship with the originator and must rely upon the third-party senders' warranties regarding its originators. The lack of customer knowledge of the originators poses additional risk to the ODFI.

Historically, there was little risk in the ACH system because it was a closed system with recurring transactions and relatively few originators. However, advances in technology

and changes in NACHA Operating Rules resulted in significant changes in the nature and volume of ACH activity, with the most pronounced growth being in nonrecurring payments, potentially increasing the risk of ACH transactions for both financial institutions and their customers. In addition to the primary ACH transactions, retailers and third parties use the now open ACH system for a variety of nonrecurring transactions including:

- ACH check conversion
 - Account receivable (ARC) entries. Many financial institutions operate retail lock boxes for their corporate customers as well as for their own payments collection. Lock boxes receive large volumes of check payments. With ARC, the checks are converted to ACH payments through the transmission of the MICR information on the checks. This data is batch processed for collection through the ACH network. ARC has improved the efficiency of lock-box operations by eliminating the transport of paper checks and increasing the speed of payment collection. While ARC has only been in use since 2001, in 2006 it accounted for 16 per cent of all ACH transactions and was one of the fastest growing segments of the ACH network. Recent statistics, however, indicate that ARC is currently decreasing.
 - Point of Purchase (POP) and Back Office Conversion (BOC) entries. Like ARC entries, POP and BOC entries are created by capturing the check MICR information and sending the transaction through the ACH. The most common application is with checks drawn on consumer accounts. Some retailers and third-party service providers have been converting checks to ACH transactions at the POP or during BOC. BOC was introduced in March 2007 as a new payment solution that allows merchants to collect checks in batches and convert them into debits through the ACH at a central location rather than at the POS. BOC is similar to POP and ARC in that it facilitates the conversion of consumer checks to electronic formats. BOC merely consolidates the electronic conversion process from the individual checkout lines to the back office.
- Internet-originated (WEB) and telephone-initiated (TEL) ACH payments
 - Consumers and retailers can initiate ACH transactions through the telephone and the Internet. These ACH transactions are an alternative to providing a credit card or signature-based debit card number.
- Re-presented check (RCK) entries
 - A physical check that was presented but returned because of insufficient funds may be re-presented as an ACH entry.

NACHA Rule and Product Changes

Over the past few years, NACHA has mandated several important rule changes to expand the use of the ACH network. Some of the more significant changes include:

- Development of a framework to support broader use of international ACH credit and debit transactions and to identify and report international ACH transactions subject to OFAC restrictions. (Effective September 2009^[27]).
- Acceptance of certain business checks for conversion to ACH debits.
- Back-office processing of eligible checks to ACH debits by retailers and billers (BOC entries).
- Use of the ACH network for presentment of bills to consumers.
- Implementation of more stringent network enforcement rules that include more substantial fines for certain violations and permit the ACH Rules Enforcement Panel to direct an ODFI to suspend an originating third party sender.
- Requirement that companies identify themselves within the ACH transaction by the name that is known to, and readily recognized by, the consumer.^[28]

NACHA also requires that every financial institution conduct an annual internal or external audit of compliance with the ACH rules no later than December 31 of each year, and that the audit be made available to NACHA upon request. While the requirements for the "ACH Rule Compliance Audit" do not prescribe a specific methodology, NACHA does identify specific criteria that must be considered during the annual audits (NACHA Operating Rules, Appendix Eight). Financial institutions and third-party service providers should have processes in place to ensure their understanding of, and compliance with, these and future rule and product changes.^[29]

Card-Based Electronic Payments

There is a growing array of card-based electronic payment systems available for retail use. Historically, these payments have been linked to a payee's or payer's existing account relationship with a financial institution. Card-based electronic payments can be defined in three ways, depending on the timing of the payment:

- "Pay Later" payments occur after receiving the goods or services and typically refer to credit payments. A credit card enables a consumer to access a credit line account at a financial institution.
- "Pay Now" payments occur when the goods or services are received and generally are associated with debit payments. Debit card payments are related to an existing transaction account at a financial institution.
- "Pay Before" refers to payments for goods or services with prepaid or stored-value cards, which are loaded with buying power before the purchase of goods or services occurs. The account associated with the pre-paid debit card may be the liability of a financial institution.

Both credit and signature-based debit card transactions are typically processed in batch mode at the POS, and settlement is delayed until the batches are processed at the end of the day. PIN-based debit card transactions, although processed in real time at the POS, typically settle at the end of the day using the ACH. Merchants often prefer that customers use PIN-based debit cards due to the lower costs associated with these transactions over the costs for signature-based credit and debit cards. With PIN-based transactions, the consumer must apply the pre-established PIN to validate the transaction. Each of these types of card payments is described below.

In the United States, almost all cards are magnetic-strip-based, while in Europe and Asia, consumer account information is often stored on a computer chip embedded in the card. These computer-chip-based systems have more security features than the magnetic strip systems; therefore, more financial institutions and merchants in the U.S. are adopting chip processing infrastructure. Consumers have welcomed recent initiatives with chip-based contactless cards so, the growth in these chip-based-cards is expected to continue.

In general, credit cards have revolving credit arrangements that allow consumers to make purchases and be billed later. Most credit card accounts allow the consumer to carry a balance from one billing cycle to the next and make a minimum payment in each billing cycle (e.g., two to three percent of their total balance) rather than requiring payment of the full balance.

A charge card is a specific kind of credit card that has a short-term, fixed-period credit arrangement. The balance on a charge card account is payable in full when the statement is received and cannot be rolled over from one billing cycle to the next. This arrangement exposes the issuing institution to less credit risk than open-ended accounts.

Financial institutions are important participants in various credit card systems. They issue and distribute cards, clear and settle the associated payments, and act as, or sponsor, merchant acquirers. ^[30] There is an increasing concentration of both credit card issuers and processors within the marketplace as larger issuers are bringing processing functions in-house. Some large institutions have exited the credit card issuance and processing businesses due to lack of economies of scale.

This booklet groups credit or charge cards in three categories: general-purpose credit cards, co-branded/affinity cards, and private label (store) cards.

General Purpose Credit Cards

General-purpose cards have the logo of one of the bankcard companies on the front. ^[31]

These cards are associated with the consumer's or cardholder's revolving credit account at a financial institution or other business. The revolving credit line is capped or limited based on the creditworthiness of the consumer. These cards can be used at any location that accepts credit cards from the particular bankcard company and include bankcards and closed-loop cards. Bankcards require agreements and transaction processing arrangements among participants, while closed-loop cards may not.

- Financial institutions issue bankcards in conjunction with the three major credit card

association networks, Visa, MasterCard, and American Express. MasterCard, Visa, and American Express operate "open" networks in which financial institutions can compete in card-issuing and merchant acquiring. The card-issuing financial institution and the merchant acquirer can be different organizations. Firms that serve as both the card issuing agent and the merchant acquirer issue closed loop credit cards.

Co-Branded/Affinity Credit Cards

Some merchants and organizations form marketing arrangements with financial institutions to issue general-purpose credit cards with the merchant or organization name on the front of the card. These cards are termed co-branded or affinity cards and the card accounts may be part of the bankcard company networks.

Co-branded cards typically offer consumers a rewards program. Organizations such as sports teams, schools, or service organizations issue affinity cards jointly with a financial institution that offers compensation in return for marketing to the merchant's customers or the organization's members. The institution might base its compensation on the number of account applications, the number of accounts activated, account volume and income, or other defined benchmarks.

Private Label (Store) Credit Cards

In some cases, financial institutions might issue a card jointly with a merchant. These cards are known as private label or store cards. Consumers can use them only at the merchant whose name appears on the front of the card. These cards do not carry a bankcard company logo, and the merchant typically plays a limited role in the issuance of the card or managing the credit relationship. ^[32]

Bankcard Companies

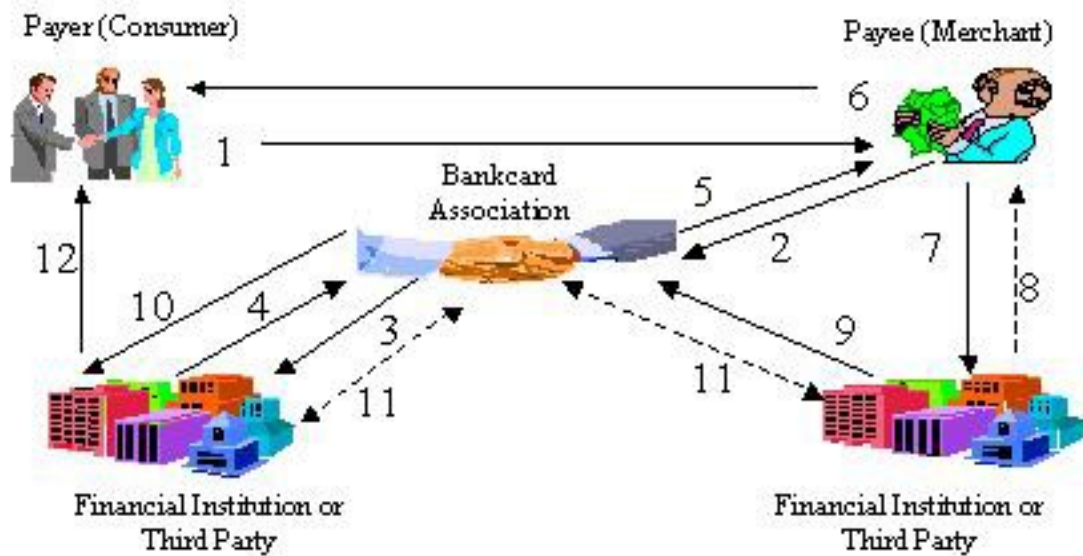
The two major bankcard companies, Visa and MasterCard, account for the majority of credit and debit cards in use. Both organizations began as bank service companies, owned by principal-member financial institutions. They provide separate, but similar operating policies, procedures, and controls for bankcard issuance, acquiring, and settlement activities. The companies own the credit card trademark, granting membership to financially sound financial institutions that apply. Only members are allowed to issue cards bearing the company logo, and they pay transaction and membership fees for use of the bankcard association logo and services.

Each company has three primary types of membership: Visa has principal, associate, and participant memberships; MasterCard has principal, affiliate, and agent memberships. Each membership type conveys different privileges. Principal membership allows members to solicit cardholders and issue cards, solicit and sign merchants, and sponsor other financial institutions for membership in the company. Associate/affiliate and participant/agent members can perform all of the principal membership functions except sponsor other members.

Card issuers are financial institutions that have permission to issue bankcard company credit cards. Acquiring financial institutions and sponsored third parties have contracts with merchants that accept a bankcard company's products. Acquiring financial institutions accept and process transactions from those merchants through the company's network interchange payment system. The cost of technology infrastructure

and the level of transaction volume are high for bankcard-acquiring institutions. Most rely on third-party service providers.^[33] Under the bankcard company's bylaws, acquiring financial institutions are responsible for the actions of all contracted third-party service providers; therefore, they are expected to monitor carefully the providers' compliance with the companies' operating rules.

The bankcard companies set interchange fees, which are paid by the merchant acquirer to the issuing financial institution. The merchant acquirer typically passes this fee along with a discount or acquirer fee for processing services to its merchants. Bankcard issuing institutions generate their revenue from the interest charged on revolving balances, and from the interchange, late, over-limit, cash advance, and card fees. Merchant-acquiring institutions, which assist in clearing and settling credit card transactions, generate most of their revenue from the acquiring and other processing fees (e.g., charge-back processing and account maintenance) they charge to the merchant.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 5: Credit Card Clearing and Settlement

Figure 5 illustrates the payment and information flows for a typical credit card transaction. In this example, the consumer pays a merchant with a credit card (step 1). The merchant electronically transmits the data, at the POS and through the bankcard company's electronic network, to the card issuer for authorization (steps 2 and 3). If approved, the merchant receives the authorization to capture funds, and the cardholder accepts liability by signing the credit voucher (steps 4, 5, and 6). In cases involving purchases under \$25, the cardholder does not have to sign. The merchant receives

payment, net of fees, by submitting captured credit card transactions to its financial institution in batches or at the end of the day (steps 7 and 8). The merchant acquirer forwards the sales draft data to the bankcard company, who forwards the data to the card issuer (steps 9 and 10). The bankcard company determines each financial institution's net debit position. The bankcard company's settlement financial institution coordinates issuing and acquiring settlement positions. Members with net debit positions (generally issuers) send owed funds to the company's settlement financial institution, which transmits owed funds to the merchant acquirers. The settlement process takes place using a separate payment network such as Fedwire® (step 11).^[34] The card issuer will then present the transaction on the cardholder's next monthly statement (step 12). The cardholder makes a payment for the charges incurred in accordance with the cardholder agreement.

Debit and ATM Cards

Debit cards are associated with an existing transaction account at a financial institution. The card enables consumers to access their accounts for a variety of transactions. Debit cards are either online (i.e., PIN-based) or off-line (i.e., signature-based).

- Online (PIN-based) debit cards have been available for several decades and have seen significant growth since the early 1990's. Online debit cards use a PIN for customer authentication and online access to account balance information. At present, financial institutions authenticate customers by matching the PIN with the account number directly through a merchant's terminal. Debit card transactions are authorized in real time at the POS using the same electronic funds transfer (EFT) networks that handle ATM transactions and are typically settled at the end of the day using the ACH network. Customers may also receive cash at the POS because messaging between the financial institution and the retailer confirms funds availability. Merchants prefer PIN-initiated card transactions as the processing fees are substantially lower. Also, credit risk is shifted to the customer as the merchant's responsibility for authentication is greatly reduced.
- Off-line (signature-based) debit cards were introduced in the late 1980's by Visa and MasterCard. Consumers are using them increasingly at merchant locations that accept bankcards. Off-line debit card systems authenticate consumers through a written signature or other authenticating action. The transactions are processed in batch mode through the same bankcard networks as credit card transactions and typically settle at the end of the business day. Generally a cardholder can use an off-line debit card anywhere that accepts a similar online transaction.

The use of biometric technology as a means to authenticate payments is also growing because of its convenience and perceived security features. Available technologies allow customers to pay for purchases by placing a finger on a sensor, which links the image to the customer's account using a simple method of finger scanning at check out. Societal implications and security concerns surrounding the use of biometric identification may act as impediments to market acceptance.

Financial institutions issue ATM cards to consumers to provide online access to account information and to allow consumers to make withdrawals and deposits at ATMs.

Consumers typically enter a PIN for authentication at an ATM, although other authentication methods such as biometric technology are available. Consumers may use an ATM deployed by other financial institutions or third parties but typically will pay fees to the ATM owner and their own financial institution. Many financial institutions now offer ATM cards that can also be used as debit cards for POS transactions at participating merchants.

Decoupled Debit Cards

Decoupled debit cards permit a financial institution to issue a debit card to consumers regardless of where their demand deposits or other transaction accounts are held. The term "decoupled" is derived from the separation of the traditional relationship between the debit card issuer and the financial institution that provides the transaction deposit account. The decoupled debit card transaction between the consumer and merchant is processed through one of the card-branded networks or an alternative proprietary network. Instead of using the EFT networks used for debit card products, the issuer uses the ACH network to debit the consumer's account for settlement.

By decoupling the debit transaction from the bank where the consumer has the depository relationship, the intermediary can capture the interchange revenue from the card transaction. A part of this product's initial appeal was the cost efficiency derived from bundling transactions prior to entry into the ACH network for settlement. However, a recent NACHA Rule Interpretation issued on November 9, 2007 ^[35] prohibits the aggregation of individual debit transactions prior to settlement through the ACH, and instead requires the issuer to pay ACH origination fees on each discrete transaction conducted during the course of a day. The interpretation was issued in response to concerns that bundling transactions through the ACH might mask risks that are transparent in individual transactions and unintentionally subvert risk management tools used by financial institutions that receive payment through the ACH. Decoupled debit card programs that rely on transaction bundling may need to be re-engineered to comply with the new interpretation.

The risk profile for decoupled debit card issuers differs from a debit card program because payments are settled through the ACH, creating a delay from the time the card transaction is initiated and exposing the issuer to credit risk. With a traditional debit card, a financial institution can verify the availability of funds before the transaction is authorized. With decoupled debit transactions, credit risk exposure may arise from faulty account verification or insufficient deposit account balances. Financial institutions that issue decoupled debit products should implement risk management programs to mitigate and control these new risks associated with the nontraditional customer relationship.

EFT/POS Networks

EFT/POS networks process, route, clear, and settle ATM and online POS debit card transactions by linking financial institution card issuers and merchant acquirers, consumers, merchants, and third-party service providers through telecommunication gateways. The primary functions of the networks include routing transactions through central switching gateways, acting as clearing houses to settle network member on-us transactions, and forwarding "foreign" nonmember transactions for processing. Both credit card and signature-based debit card transactions are processed in batch mode at the POS, and settlement is delayed until the batches are processed at the end of the day. PIN-based debit card transactions typically settle at the end of the day using the ACH, although they are authorized in real time at the POS.

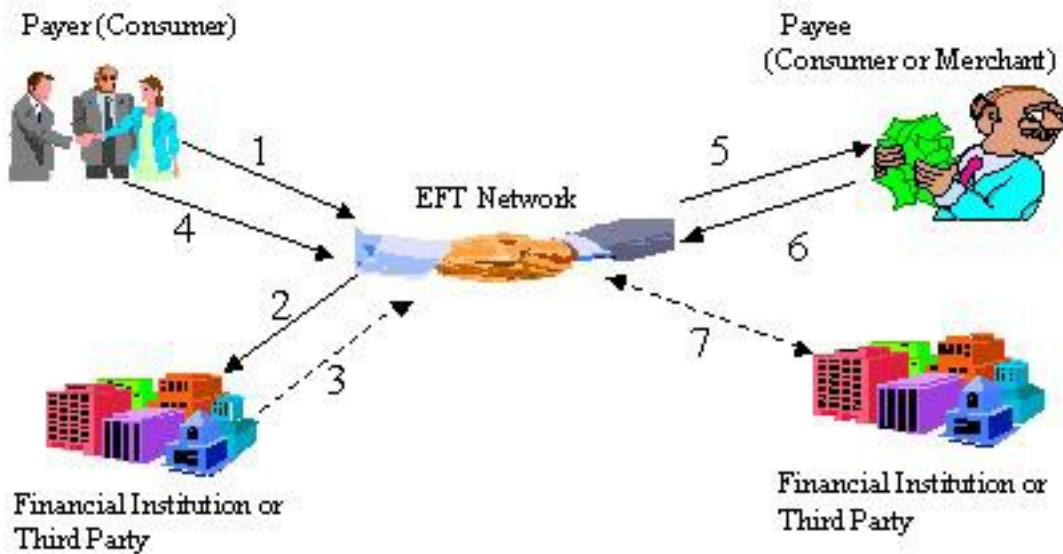
Most financial institution and nonbank ATM networks are connected to regional and national EFT/POS networks. Most regional EFT/POS networks are joint ventures owned and controlled by competing financial institutions, some function as cooperatives, and some are owned and operated by a single firm as a profit-making enterprise.

Visa and MasterCard own and operate the two national EFT/POS networks: (1) Visa's Plus and MasterCard's Cirrus ATM networks, and (2) Visa's Interlink and MasterCard's Maestro POS networks. The national networks serve as a bridge between regional networks, allowing them to route transaction information among them.

Membership in regional and national EFT/POS networks facilitates universal access to financial institution card-based electronic services and provides participant financial institutions with an interchange system offering authorization, clearing, and settlement services. Acquirers collect interchange fees from network members (issuers) to cover operating costs. With ATM transactions, the issuer pays fees to the acquirer, in contrast to credit and debit card networks in which the acquirer pays fees to the issuer.

Many financial institutions often rely on third-party service providers to conduct ATM and debit card payment processing. Third-party service providers provide a range of retail payment-related services, including card issuing, merchant, account maintenance and authorization, transaction routing and gateway, off-line debit processing, and clearing and settlement services. Although merchant acquiring financial institutions may use third-party service providers to perform many acquiring activities, the acquiring financial institution remains responsible for all third-party service-provider merchant activities.

Independent sales organizations (ISOs) provide third-party services to install and operate ATM and POS terminals for financial institutions and merchants. Representing merchants and community financial institutions, an ISO typically contracts with third-party service providers for a variety of services including support of ATM and POS terminals, transaction processing, and cash restocking. Some EFT/POS networks require an ISO to be sponsored by a financial institution member of the network.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 6: PIN-based Debit Clearing and Settlement

Figure 6 describes a generic, online, PIN-based, debit card transaction. The consumer enters a PIN to authorize the transaction (Step 1). The merchant's financial institution requests authorization from the consumer's financial institution through the EFT/POS network (Step 2 and Step 3). The consumer's financial institution, or in some cases the regional network, verifies availability of funds and debits the consumer's account (step 4). The EFT/POS network contacts the merchant and authorizes the purchase (Step 5).

Typically, the acquiring financial institution does not credit the merchants' account with the entire amount of the transaction (similar to credit card clearing). Rather, the merchant receives the transaction amount, net of applicable fees and other expenses assessed by the acquiring financial institution and other intermediaries to the transaction (Step 6). For settlement, at the end of the business day, the regional EFT/POS networks determine the net debit and credit positions of the participating financial institutions and settle their positions using the ACH (Step 7).

Prepaid (Stored Value) Cards

The market for prepaid cards, sometimes called stored value cards, is one of the fastest growing segments of the retail financial services industry. While the terms prepaid cards and stored-value cards are frequently used interchangeably, differences exist between the two products. Prepaid cards are generally issued to persons who deposit funds into

an account of the issuer. During the funds deposit process, most issuers establish an account and obtain identifying data from the purchaser (e.g., name, phone number, and etc.). Stored-value cards do not typically involve a deposit of funds as the value is prepaid and stored directly on the cards. Because its business model requires cardholders to pay in advance, it substantially eliminates the nonpayment risk for the issuing financial institution. The functionality of this product is leading to a wide range of card programs that operate in either closed or open-loop systems, and program innovation has resulted in the development of systems that operate in both structures. Closed-loop systems are generally retailer/issuer business models, while general-purpose cards issued by financial institutions tend to operate in open-loop systems. Open-loop system prepaid cards are processed using the same systems as the branded network cards - MasterCard, Visa, American Express, and Discover - and offer the same functionality.

In the past, prepaid cards were mostly issued by nonfinancial businesses in limited deployment environments such as mass transit systems and universities. In recent years, prepaid cards have grown significantly as financial institutions and nonbank organizations target under-banked markets and overseas remittances. Technological innovations in the way information is stored (e.g., magnetic strip or computer chip), the physical form of the payment mechanism, and biometric account access and authentication are converging to create efficiencies, reduce transaction times at the POS, and lower transaction costs.

There are several types of prepaid cards, including gift, payroll, travel, and teen cards. Either the consumer or an issuer funds the account for the card. When a consumer uses the card to make a purchase, the merchant deducts the amount of the purchase from the card. Transaction authorization can take place through an existing network, a chip stored on the card, or information coded on the magnetic strip. Once the stored value in the card is exhausted, customers may either replenish the value or acquire a new card.

In addition to cards, stored-value payment devices are emerging in a variety of other physical forms, most notably key fobs. With the recent introduction of contactless payment technologies, use of chips (smart cards), radio frequency identification (RFID), and near field communication (NFC) payment devices are becoming more innovative. Initiatives are underway to introduce mobile phones with integrated microchips that can initiate a payment when waved over a specially-equipped reader. The integrated chip can store value, authenticate a consumer, or contain consumer preferences and loyalty program information that can be used for marketing purposes.

Prepaid cards may be subject to legal and regulatory risks. For example, the Federal Reserve Board's final rule on Regulation E, issued August 30, 2006, extended its applicability to prepaid cards used for consumer's payroll. The Federal Reserve Board noted that it will monitor the development of other card products and may reconsider Regulation E coverage as these products continue to develop. State laws vary widely with regard to fees. Additionally, financial institutions should ensure that prepaid card product programs comply with the BSA and anti-money laundering guidance.

Payroll Cards

Payroll cards provide a means for paying a consumer's wages or other compensation in an access device with the functionality of a debit card. The card is loaded with the customer's payroll information on a magnetic strip or microchip and can be used to access an account that the employer establishes with a financial institution. The

employee can use the payroll card to withdraw the funds at an ATM and to make POS purchases without a banking relationship. Some payroll cards may offer features such as convenience checks and electronic bill payment. Payroll cards are often marketed to employers as a cost-effective means of providing wages to employees who lack a traditional banking relationship. Their low-cost structure and debit-like functionality make them attractive as an alternative to direct deposit to more transient consumers. The Federal Reserve Board has amended its Regulation E to apply to payroll cards.

Payroll cards are supported by the Visa and MasterCard networks and can be used in every way that other branded cards are used. Employers are increasingly adopting payroll cards, and the growth is expected to continue because of their cost advantage to employers and financial institutions. Third-party service providers have sought opportunities in this market and may be engaged for card issuance, processing transactions made on the payroll card account, providing a range of program administration services for financial institutions or employers, and offering customer services to cardholders. Figure 7 illustrates the various relationships in an open-system payroll card program.

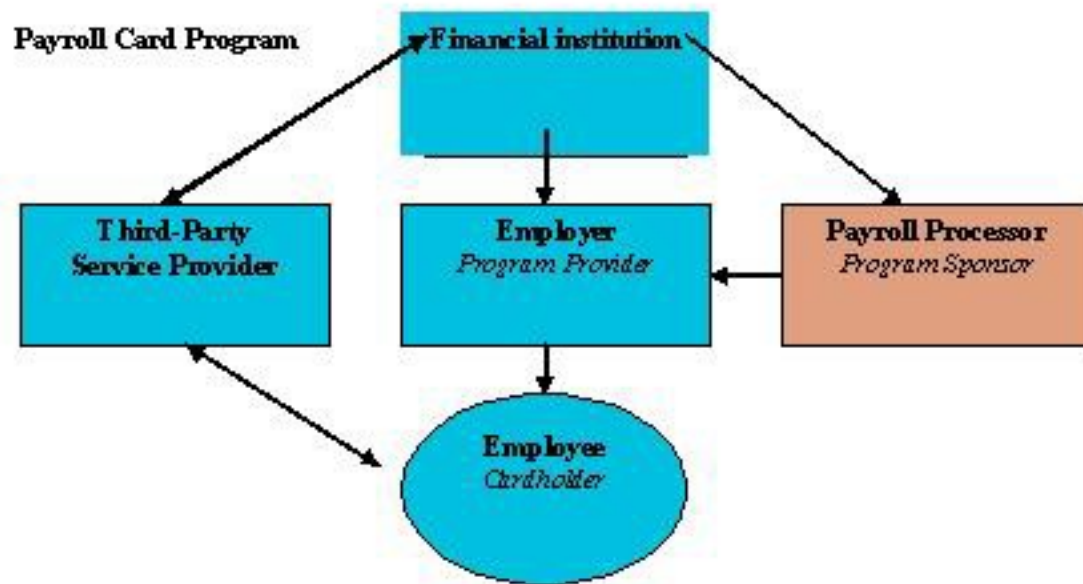


Figure 7: Open-system payroll card program

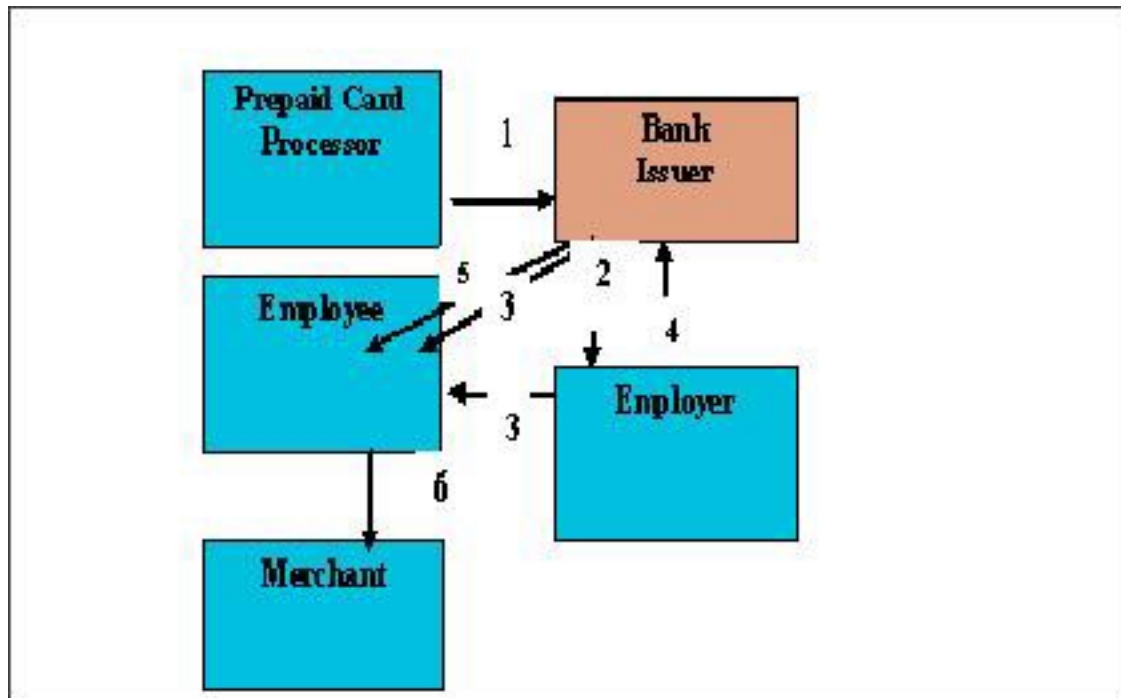


Figure 8: Stored value card product designed for corporate payrolls

Figure 8 describes a stored value card used in a payroll program. A stored value processor works with a financial institution to establish a payroll card program (Step 1). The issuer (financial institution) manages the card issuance and transaction processing. The financial institution offers the payroll card services to employers (Step 2). Either the financial institution or the employer distributes the payroll cards to employees (Step 3). The employer tells the financial institution the amount to credit to each employee's payroll card account (Step 4). On the pay date, the financial institution posts the funds to the employees' accounts (Step 5), allowing them to make purchases at any merchant that accepts the card's branding, e.g., Visa, MasterCard (Step 6).

General Spending Reloadable Cards

General spending card programs are offered by both financial institution and nonbank program providers or sponsors and are typically targeted to a particular consumer segment. Nonbank program providers usually sell this type of card and may have a relationship with a money service business or retailer, who, in turn, acts as agent for a nonbank program provider. See Figure 9 for a typical structure. Check-cashing businesses and convenience stores are examples of agents used by nonbank program providers. All network-branded prepaid cards must be issued by a partnering financial institution that is a member of the Visa or MasterCard networks or by American Express or Discover. There is a growing group of market participants associated with these programs and a developing range of potential functionality.

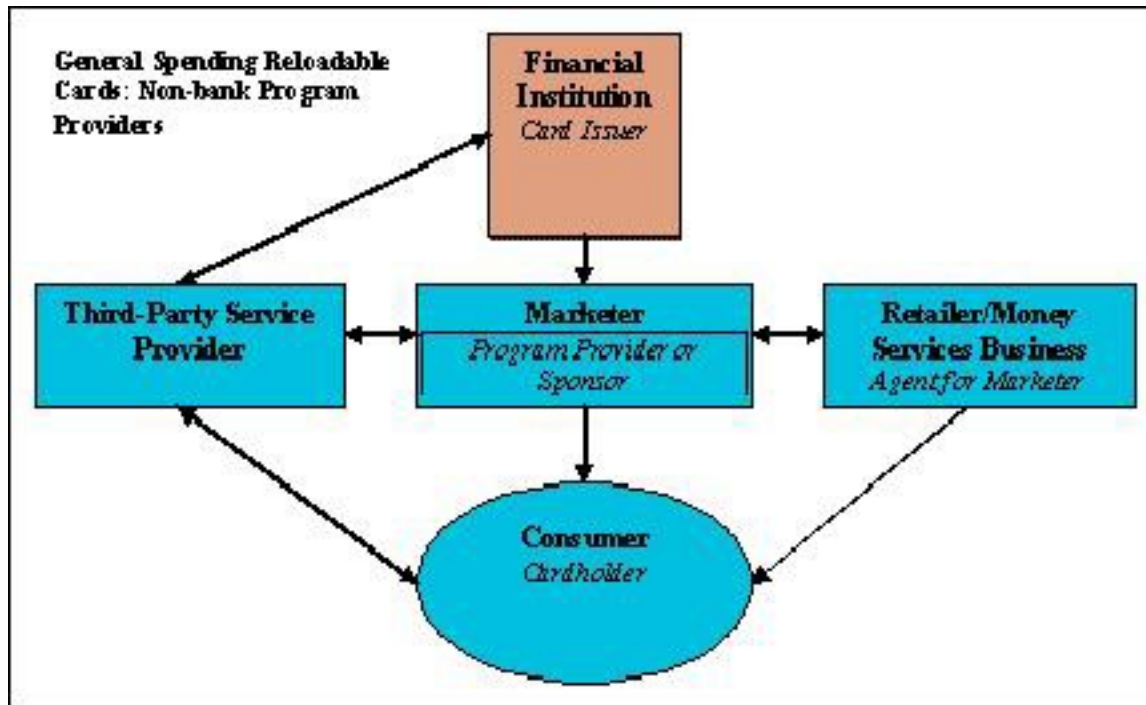
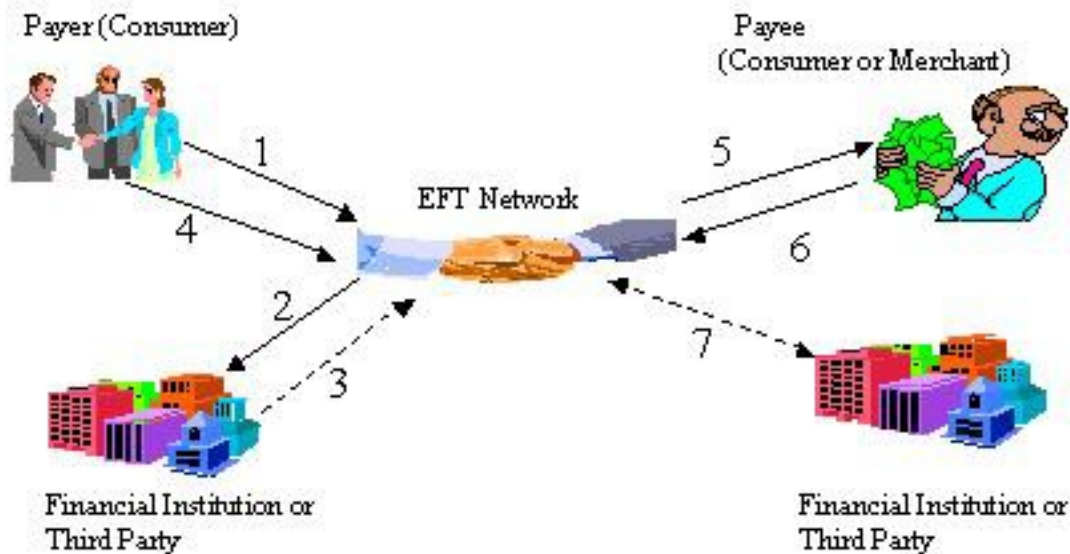


Figure 9: General spending card program offered by nonbank providers

Prepaid card transactions typically follow the "four corner" pattern in Figure 10. The consumer purchases a prepaid card (Step 1 and Step 2). When the consumer pays for goods or services with the card, electronic notations or tokens transfer from the card to the merchant's cash register (Step 3, Step 4, and Step 5). The merchant contacts the computer network of the financial institution that issued the prepaid card and presents the tokens for payment (Step 6). The network notifies the consumer's financial institution to pay the appropriate sum to the merchant's financial institution, and net settlement occurs at the end of the business day (Step 7). The financial institution keeps a percentage of the payment (the discount) as compensation for the services provided.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 10: Stored Value Card Clearing and Settlement

There are many configurations of third parties and financial intermediaries, and there is a significant number of prepaid cards in circulation for which the four-corner diagram is not sufficient. The financial intermediary may hold the funds supporting the circulating stored value in a pooled account, with a third-party keeping the record of the individual transactions. Financial businesses that are not traditional financial institutions may be the issuers and may distribute the cards through retailers.

If the prepaid card is not a smart card, the associated funds are kept in a separate account. When a customer uses the prepaid card, the merchant sends a message to the record-keeping entity to determine whether the balance is sufficient to cover the transaction. If funds are available, the third party or financial institution processes the transaction.

This account arrangement may be used for smart cards also, with the accounts debited when the merchant presents tokens for payment. Although financial institutions issue prepaid cards and maintain account records, third parties may be involved in maintaining individual account records also.

Three general-spending prepaid card programs that increasingly are offered by financial institutions include branded remittance cards, teen cards, and gift cards.

Remittance Cards

With the growing demand for global person-to-person money transactions, an increasing number of bank-issued cards are being used to make remittances. In many cases, the sender of the remittance lives in the U.S. and uses a financial institution to electronically transfer money to a pre-established, branded prepaid card account. A financial institution in the sender's or recipient's country issues a prepaid card to the recipient. The recipient can use the card to obtain cash at an ATM or goods and services at a merchant POS. Alternatively, the sender may use a branded prepaid card to send funds to a recipient via the Internet. The recipient receives the funds either in cash or in credits made to an existing prepaid card account or a bank account.

Teen Cards

Another stored-value product gaining favor among consumers is the teen card that is marketed to help parents instill financial responsibility in their children while monitoring and supervising their spending. The consumer typically funds the prepaid card with the issuing financial institution through a withdrawal from a deposit account or by charging a credit card.

Gift Cards

Gift cards were initially offered by retailers as a replacement for paper-gift certificates and operated in closed-loop payment systems. In recent years, financial institutions noted the rising popularity and market potential and included gift cards in their product offerings thereby competing with retailers. Gift cards issued by a financial institution typically are card network branded and operate in an open-loop payment system, making them functional at ATMs and at any POS that accepts network debit and credit cards.

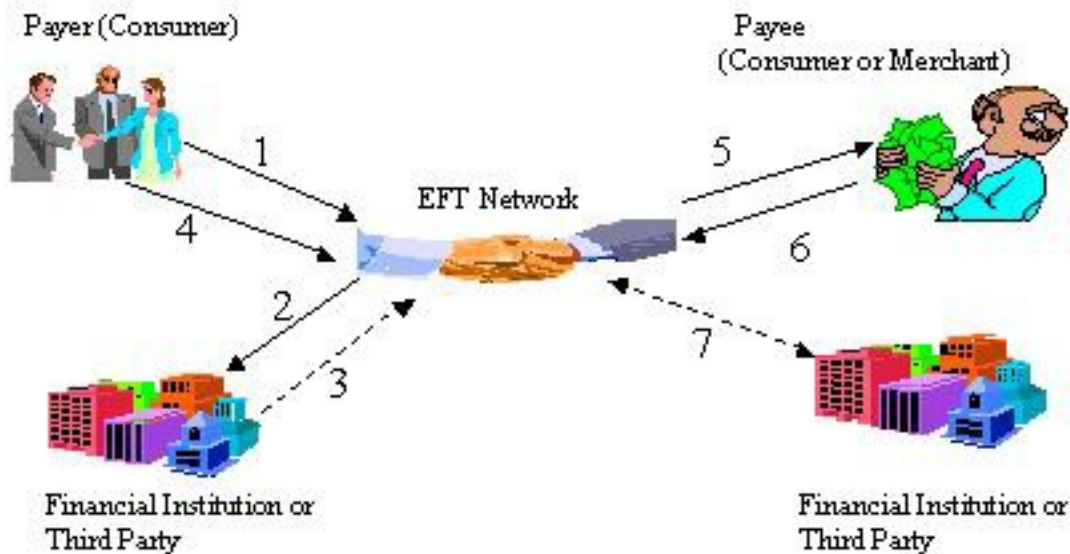
Online Person-to-person (P2P), Account-to-Account (A2A) Payments and Electronic Cash

Other electronic payments include person-to-person, account-to-account, electronic cash, and electronic benefit transfers. These payment instruments are usually associated with an established consumer deposit account and facilitate consumer access to recurring or one-time debit and credit transactions and a variety of federal, state, and local government benefit programs.

Online P2P or e-mail payments typically use traditional payment networks to transfer funds electronically from one consumer to another. Though these payments are named for their ability to send funds among individuals online, the majority of P2P payments are Internet purchases at online auctions or small businesses. In most cases, P2P transfers use existing retail payment systems to add and withdraw funds from accounts. The simplest case is when the person making a payment and the receiver maintain accounts at the same bank. This type of payment is called an "on-us" transaction. They are settled by posting accounting entries on the books of one financial institution. P2P transfers also may occur outside the traditional payment networks and, in their simplest form, may take place as an exchange of cash between two individuals. As technology advances, the transfer of funds through the use of proximity devices, such as mobile telephones and personal digital assistants (PDAs), is likely.

Most P2P services charge to the receiver of the funds a fee that varies depending upon

various factors, including payment method and the sender's credit history. Payments made with funds that originated from either ATM or ACH transactions are less expensive than payments made with funds originated from credit cards. P2P systems may offer to the receiver an opportunity to obtain funds through a check and for an additional fee.



Legend: Solid lines represent the flow of information and dashed lines represent the flow of funds.

Figure 11: Online P2P Clearing and Settlement

Online P2P payments typically occur using the process described in Figure 11. The sender of the funds must have an account with the P2P service provider (Step 1). Depending upon the service, the funds may come from an existing credit card or transaction account or may be drawn from a previous balance with the online P2P payment provider (Step 2 and Step 3). The sender can designate the e-mail address of the intended funds recipient (Step 4). The P2P network transfers the funds to the receiver's account as an "on-us" transaction. Once the funds reach the receiver's account, notice of the transaction is sent through e-mail to the receiver (Step 5). The receiver of the funds must join the service if it does not already have an account (Step 6). The online P2P payment service can disburse the funds from the receiver's P2P account through an ACH payment, a check payment, an EFT credit, prepaid card, or a credit to a credit card account (Step 7).

Account-to-account (A2A) payments are similar to P2P payments. They involve the transfer of funds from one customer's account to another account at either the same or another financial institution. Like P2P payments, A2A transfers can be initiated through the customer's Internet banking service, a biller's payment Web site, or by telephone instruction from the customer. Unlike P2P transfers, consumers must access an existing

retail payment account (deposit account) at a financial institution in an A2A transaction. To complete a transaction, the customer must know the recipient's account number or some other identifier. A2A payments can be effected on the ACH or ATM networks. On the ACH networks, funds are cleared and settled within two to three days. The ATM networks may allow same-day funds availability although settlement may not occur for two or three days. Same-day transfers using the ATM networks are usually less expensive than traditional wire transfers.

P2P payments are a growing segment of the A2A market. The success of the P2P online auction model is attributed to the consumers' demand for convenient and reliable P2P transactions. P2P payments may include transaction accounts and may be conducted through the use of proximity devices such as mobile telephones or PDAs. P2P payments are expected to grow as more reliable and convenient payment methods are introduced.

Financial institutions and retailers are also developing electronic cash-payment instruments. Similar to P2P payments, individuals can transfer electronic cash value to other individuals or businesses, generally through the Internet. Consumers can use the cash payment instruments for purchases at retailers' Web sites or they can transfer cash to other individuals through e-mail. Pre-funded accounts that consumers can use for online auction payments are among the most recent applications. In these applications, individuals use a credit card or signature-based debit card number to pre-fund the Web certificate or electronic account, and recipients redeem the value from the issuer.

Electronic Benefits Transfer (EBT)

EBT systems allow recipients of government benefits to authorize transfers from their benefits accounts to health care providers and retailers. The federal government and several states routinely use these accounts to issue food stamps and other benefits. The government distributes all food stamp benefits using this technology and, while the average transaction value is low, total transaction volumes are significant. The institution holding the account authenticates transactions using PIN technology. EBT programs now use cards with either magnetic-strip or microchip technology. Since cards using chip technology have larger storage capacities than cards with a magnetic strip, they can handle more complex transactions. Security measures can be encoded on the card strip or microchip as well to help prevent unauthorized use.

Emerging Retail Payment Technologies

This section discusses several emerging retail payments technologies that financial institutions are implementing or considering. The success of emerging retail payment methods depends upon four key drivers: reliability, cost, convenience, and speed. In terms of the preferences by consumers, merchants, and payment processors, the key drivers are technological advances, convenience, and lower transaction costs. The evolution of such preferences is facilitated by traditional financial institution relationships and established payments networks and infrastructure. Internet, mobile, and contactless payments may be used alone or together to facilitate electronic transactions, further reducing the use of paper checks. The use of currency is expected to retain some appeal because of its anonymity; however, the substitution of electronic payment vehicles for cash micro payments (transactions under \$5.00) is expected to increase.

While the environment for emerging payments is highly dynamic, the most important

emerging payments today are electronic bill presentment and payment (EBPP), P2P, A2A, and stored-value instruments. Several more recent emerging payment mechanisms are contactless payments, biometrics, and proximity payments as well as the format and transmission mechanics used to effect these payments.

Contactless Payment Cards, Proximity Payments and Other Devices

Contactless cards and key fobs have an embedded computer chip with financial and personal information used for payment transactions, and they employ RFID technology for payment transmission. The contactless cards include a microcontroller (or equivalent intelligence) and internal memory and have the ability to secure, store, and provide access to data on the card. The microcontroller also supports the use of improved security features including authenticated information access and information privacy. Traditional plastic cards are easily transitioned to these new contactless cards. Other smart-card technologies provide similar capabilities but do not have the radio frequency interface that would enable them to be read quickly and conveniently at a short distance from the reading mechanism.

Proximity payments are POS transactions made with a mobile device like a cellular telephone, smart card, PDA, or virtually any device that can house a microchip. If the payment is executed with a mobile phone, it may be referred to as an M-payment. Proximity payments are faster, cheaper, and easier than traditional payment mechanisms such as cash or credit card type transactions, particularly for micro payments. Many of these transactions use the same credit/debit card network, and provide lower costs to institutions and to merchants.

Proximity payments and contactless cards permit the consumer to maintain physical control of the access device rather than relinquishing such control to an operator at a POS. Bankcard companies and governmental agencies have become the leaders in facilitating these transactions. Currently, there are multiple transmission types in use, and several are discussed below. Other transmission types are undergoing market test trials.

Financial institutions offering advanced payment technologies (i.e., commercial POS systems to merchants or consumer proximity devices) need to perform the same due diligence and vendor management as they would on any service provider. This includes ensuring an appropriate level of security in the devices.

Biometrics for Payment Initiation and Authentication

Biometric payment services allow a consumer to make purchases or to cash checks using a biometric identifier such as a finger scan linked to his or her personal identification information, accounts at a financial institution, or loyalty programs. Other biometric methods include voice scanning and iris and retinal imaging. Biometric technologies are used increasingly for consumer account authentication. However, a biometric identifier alone is only a single factor, and it may need to be combined with other technologies or factors for proper authentication of high-risk banking transactions.

^[36] FFIEC Guidance "Authentication in an Internet Banking Environment - Supplement," June 2011 www.ffiec.gov/press/pr062811.htm As new payment systems emerge, industry demands for anti-fraud measures may result in greater use of biometrics.

Emerging Network Technologies

The previously discussed emerging payment systems rely upon, and may be integrated with, underlying network communication technologies and protocols. If not properly implemented, new and emerging network communication technologies may expose the payment device or system to additional vulnerabilities. This is particularly true with any network that relies upon broadcast technology to send and receive information. Even close proximity wireless devices, such as RFID, have been found to be vulnerable to eavesdropping at distances greater than they were designed for. Care should be taken to ensure that the underlying network communication technology has security appropriate to the information being transmitted. Currently, there are four types of short-range wireless connectivity technologies that can be used to connect payment devices to POS devices. These include: Infrared, RFID, NFC, and Bluetooth.

Infrared

Infrared communication technology works similarly to a television remote control as information is sent from a device to a payment terminal via a frequency that is invisible to the naked eye. These devices can have signals that are stronger than other contactless technologies and can work from several yards away. Security concerns arise regarding the ability to compromise a transmission because of the strength of the signal. This concern is somewhat mitigated because there must be a direct line of sight for the transmission to work. The Infrared Financial Messaging Group (IrFM) is a consortium of technology and financial companies (including Visa) that work together to promote uniform and interoperable standards ^[37] for infrared devices. These standards include encrypted channels.

Radio Frequency Identification

RFID is a method of remotely storing and accessing data on devices called RFID tags/transponders. An RFID tag can be incorporated into a plastic card (as with contactless cards), a fob, or other device. RFID tags also can be embedded into any product to track inventory. RFID tags contain antennas that enable them to communicate via radio frequency with an RFID transceiver. The technology protocol most widely used for RFID is the ISO 14443 standard. This standard is very general and can be used for multiple types of media and a broad range of hardware.

Near Field Communication

NFC is another short-range communication technology similar to RFID, but based on the ISO 18092 standard. NFC chips can be embedded in a mobile device such as a telephone to enable it to act as a contactless payment card. NFC has additional functionality such as the ability to act as a reader of other NFC devices, thus enabling two consumer devices to share data or transact payments with each other. NFC chips can also be integrated with other applications within the mobile device to permit transactions from multiple accounts.

RFID and NFC have become very flexible solutions for alternative payments. Financial institutions are adding RFID tags to credit and debit cards to speed transactions. In some parts of the world, consumers can link their credit or debit accounts to cell phones enabled with RFID or NFC technology to make purchases at retail sites equipped with payment readers.

Bluetooth

Bluetooth is a close-range wireless radio frequency communication protocol that has been implemented in a wide range of technologies. Bluetooth uses a stronger signal than RFID or NFC and is detectable at greater distances. There has been limited adoption of this protocol.

Retail Payment Systems Risk Management

Action Summary

Financial institutions engaged in retail payment systems should establish an appropriate risk management process that identifies, measures, monitors, and limits risks.

Management and the board should manage and mitigate the identified risks through effective internal and external audit, physical and logical information security, business continuity planning, vendor management, operational controls, and legal measures.

Risk management strategies should reflect the nature and complexity of the institution's participation in retail payment systems, including any support they offer to clearing and settlement systems. Management should develop risk management processes that capture not only operational risks, but also credit, liquidity, strategic, legal, and compliance risks, particularly as they engage in new retail payment products and systems. Management should also develop an enterprise wide view of retail payment activities due to cross-channel risk. These risk management processes should consider the risks posed by third-party service providers.

Financial institutions should tailor their risk management strategies to the nature and complexity of their participation in retail payment systems, including any support they offer to clearing and settlement systems. Financial institutions must comply with federal and state laws and regulations, as well as with operating rules of clearing houses and bankcard networks. From the initiation of a retail payment transaction to its settlement, financial institutions are exposed to certain risks. For individual retail payment transactions, risks resulting from compliance issues and potential operational failures including fraud are always present. Operational failures can increase costs, reduce earnings opportunities, and impair an institution's ability to reflect its financial condition accurately. Participation in retail payment systems may expose financial institutions to

credit, liquidity, and operational risk, particularly during settlement activities. In addition, a financial institution's credit, liquidity, and operational risks may be interdependent with payment system operators and third parties.

Risk profiles vary significantly based on the size and complexity of the financial institution's retail payment system products and services, IT infrastructure, and dependence on third parties. All financial institutions should maintain an effective internal control environment commensurate with the level of retail payment products and services offered. Effective internal controls should include financial, accounting, technical, procedural, and administrative controls necessary to minimize risks in the retail payment transaction, clearing, and settlement processes. These measures reduce operational and credit risks, ensure individual transactions are valid, and mitigate processing and other errors. Effective controls also ensure supporting IT and network infrastructure promote retail payment transaction integrity, confidentiality, and availability. Financial institutions engaging in retail payment system services should be aware of the risks inherent in the activity.

Financial institutions have always offered a variety of retail payment services; however, recent technological advances are expanding the opportunities for the development of innovative payment products and services. Financial institutions should recognize the strategic risk of newer products and services, which may lack consumer acceptance. Often, participants will also face uncertainty regarding how state and federal laws and regulations will apply to new payment systems. The ongoing shift from paper to electronic payments is increasing the participation of nonbanks in various payment functions, such as payment processing. Financial institutions should have a comprehensive and effective vendor and third-party service provider risk management and oversight program. ^[38]

Payment System Risk (PSR) Policy

Payment and securities settlement systems are critical components of the nation's financial system. The smooth functioning of these systems is vital to the financial stability of the U.S. economy. The Federal Reserve Board has developed the PSR policy to address risks that payments and securities settlement systems present to the financial system and to the Reserve Banks.

The Reserve Banks are exposed to credit risk when they process wholesale and retail payments for financial institutions holding reserve accounts, just as financial institutions assume credit risk when offering retail payments to their customers. Part of the Federal Reserve's PSR Policy seeks to control and reduce credit risk to the Reserve Banks by controlling financial institutions' use of Federal Reserve daylight overdrafts.

A daylight overdraft occurs when there are insufficient funds in a financial institution's Federal Reserve account to cover the institution's payment activity, such as outgoing Fedwire® funds transfers or ACH credit originations, as outgoing payments are posted during the day.

To control daylight overdrafts, the PSR policy establishes limits, or net debit caps, on the amount of Reserve Bank daylight credit that a depository institution may use during a single day and over a two-week reserve maintenance period. These limits are determined jointly through assessments by the depository institution and its Reserve Bank. The limits reflect the overall financial condition and operational capacity of each

institution using Reserve Bank payment services.

Financial institutions may be monitored on an ex post (i.e., end of day) or real-time basis. Under the Federal Reserve's ex post monitoring procedures, an institution with a daylight overdraft in excess of its maximum daylight overdraft capacity or net debit cap may be contacted by its Reserve Bank. The Reserve Bank may counsel the institution and discuss ways to reduce its excessive use of intraday credit. Each Reserve Bank retains the right to protect its risk exposure from individual institutions by unilaterally reducing net debit caps, imposing collateralization or clearing balance requirements, rejecting or delaying certain transactions, or, in extreme cases, taking the institution off-line or prohibiting it from using Fedwire. In addition, the Reserve Banks assess fees for daylight overdrafts above a certain deductible amount. ^[39] A Reserve Bank will monitor an institution's position in real time when the Reserve Bank believes that it faces excessive risk exposure, for example, from institutions with chronic overdrafts in excess of what the Reserve Bank determines is prudent. In addition, the Reserve Bank will reject or delay certain transactions that would exceed the institution's maximum daylight overdraft capacity or net debit caps, and take other prudential action, including requiring collateral.

Institutions that are monitored in real time must fund the total amount of their ACH credit originations in order for the transactions to be processed by the Reserve Bank, even if those transactions are processed one or two days before settlement. ^[40]

The financial institution's board of directors is responsible for PSR policy compliance and should ensure that management establishes sound internal operating practices, including compliance with applicable banking laws, and carefully manages retail payment system-related financial risks. At a minimum, a financial institution's board of directors and senior management should:

- Understand the financial institution's practices and controls regarding the risks of processing transactions for both its own account and the accounts of its customers and respondents;
- Manage its Federal Reserve account effectively and use daylight credit prudently in accordance with the PSR policy;
- Establish prudent limits on the daylight overdraft or net debit position in its Reserve Bank reserve account and any private-sector clearing and settlement system; and
- Review periodically the institution's daylight overdraft activity to ensure the institution operates within the established guidelines.

Strategic Risk

Strategic risk is associated with the financial institution's mission and future business plans. This risk category includes plans for entering new business lines, expanding existing services through mergers and acquisitions, and enhancing infrastructure (e.g., physical plant and equipment, IT, and networking). The variety of emerging

technologies for retail payments demands integration of payment strategies into the financial institution's overall strategic planning processes. Financial institutions also compete increasingly with highly innovative nonbank entities to provide retail payment services.

This competition benefits the consumer through enhanced product offerings at a lower cost. Conversely, competition places additional pressure on financial institutions to protect profitability through the development of new products and services while managing additional marketing, research, and development costs.

Strategic plans that include significant market expansion or the addition of new products and services may expose financial institutions to increased risks. For example, expanding Internet banking services to include electronic bill presentment and payment services, expanding existing bankcard issuing programs, or entering the merchant bankcard processing business significantly increase the potential risk to the financial institution given the inherent risks associated with these services. Business plans for specific products and services should demonstrate that management has assessed the risks and documented the institution's program to mitigate them. Such plans should address the institution's capability to provide the service. Innovative products and services are emerging quickly and early stages of market introduction may expose financial institutions to undefined and unanticipated risks the need for an enterprise wide view of retail payment activities due to cross channel risk including fraud, money laundering, and IT security breaches. Business models for emerging products that are gaining acceptance abroad, particularly in Asia, may not be introduced as easily in the U.S. because of the differences in infrastructure and applications.

To mitigate strategic risk, management should have a strategic planning process ^[41] that addresses its retail payment business goals and objectives, including supporting IT components. Because financial institutions are increasingly reliant upon third-party service providers for retail payment system products and services, the strategic plan should address comprehensive vendor management.

Credit Risk

Credit risk arises when a party will not settle an obligation for full value. Each retail payment instrument has a specific settlement process that depends on the entities involved. Multiple financial institutions, third-party entities, as well as the payer and

payee are involved with creating, processing, and settling the transaction. If a financial institution uses a third-party service provider, the institution is responsible for the credit risk exposure for the services performed. Financial institutions should have procedures in place to manage the credit risk of third parties using the institution's accounts to settle transactions.^[42]

Credit risk with retail payment systems is evident in ACH, merchant card, and remote deposit processes where the financial institution supplies funds on behalf of a merchant and provisional settlement does not occur for several days. Returns are another source of credit risk for all forms of retail payment systems. Checks and direct debit transfers can be returned by the payer's institution because of insufficient funds, a closed account, a stop payment order, forgery, fraud, or other payment irregularity. The return timeframes vary for different payment instruments. For an ACH debit, the ODFI grants funds availability to the originator on settlement day. The credit exposure exists until the RDFI can no longer return the ACH debit. If not properly authorized, the return time frame for consumer debits under NACHA rules extends to 60 days from the settlement date.

Financial institutions that accept large volumes of retail payments from merchants should understand the nature and degree of credit risk from those relationships. Financial institutions should manage those relationships in the same manner as any credit, subjecting the customers to credit administration processes for due diligence and ongoing monitoring. The risk in large volume relationships, and the institution's legal lending limit and capital position should be recognized in establishing exposure limits for each customer. Financial institutions may mitigate credit risk by requiring pre-funding for credit originators and adequate risk-based reserves for debit originators.

For the ACH system, NACHA rules require each ODFI to conduct appropriate creditworthiness monitoring, establish exposure limits, and periodically review the limits applicable to specific originating customers. Both ODFIs and RDFIs are exposed to credit risk. However, an RDFI's credit risk is minimal because it has the right to return items it is unable to post to customers' transaction accounts within NACHA guidelines and timeframes. ODFIs are ultimately responsible for all transactions entering the payment system regardless if the transaction is a credit or a debit. ODFIs that generate credits have a typical credit exposure of three days, which represents the gap between the submission of the ACH credit file and the funding of the file by the file originator. Such credit risk may be mitigated by requiring pre-funding of the credit file. ODFIs that generate debits have a credit exposure of 60 days due to the potential for returns.

Bankcards have specific procedures for chargebacks, which are amounts disputed by the cardholder and "charged back" or reversed out of the merchant's account. The acquiring financial institution relies on the creditworthiness of the merchant, but if the merchant declares bankruptcy, commits fraud, or is otherwise unable to pay its chargebacks, the acquiring financial institution must pay the issuing financial institution.

The settlement of retail payment transactions (i.e., the transfer of funds between the parties) discharges the payment obligation. The risk that settlement of retail payment transactions will not take place as expected can result in both credit and liquidity risks. Financial institutions should understand and manage credit and liquidity risks related to the settlement of retail payments. This should include preparing for potential credit and liquidity issues resulting from incomplete settlement or operational problems.

Settlement lags occur when financial institutions, due to failure or the inability to fund their obligations, do not settle their obligations when due. Settlement lags result in credit risk until final settlement occurs. Any payment activity undertaken on the basis of

"unsettled" payment messages remains conditional, resulting in risk. Settlement lags may also result in liquidity risk. Until settlement is completed, a financial institution is not certain what funds it will receive through the payment system. As a result, it may not be sure whether its liquidity is adequate. If an institution overestimates the funds it will receive when settlement takes place, it may face a shortfall. If the shortfall occurs close to the end of the day, an institution could have significant difficulty finding an alternate liquidity source.

Financial institutions often allow their corporate customers to incur intraday or "daylight" overdrafts. An institution engaging in this practice is extending credit to its customer. In most cases, the overdraft is eliminated with incoming funds transfers from other institutions (or outgoing securities transfers against payment) by the end of the business day. Daylight overdrafts constitute an extension of credit, no matter how long they remain unpaid. An institution's credit policies should include provisions for approving and monitoring daylight overdraft lines to customers.

Liquidity Risk

Liquidity risk is the current and potential risk to earnings or capital arising from a financial institution's inability to meet its obligations when they come due without incurring unacceptable losses. Liquidity risk related to payment systems is the risk that the financial institution cannot settle an obligation for full value when it is due but rather at some unspecified time in the future. Liquidity problems can result in opportunity costs, defaults on other obligations, and costs associated with obtaining the funds from an alternative source for possibly extended periods of time. In addition, operational failures may also negatively affect liquidity if payments do not settle within an expected time period.

Legal (Compliance) Risk

Legal risk arises from failure to comply with statutory or regulatory obligations. It can result from a financial institution's failure to comply with the bylaws and contractual agreements established with the bankcard networks, clearing houses, and other counterparties with which it participates in processing, clearing, and settling retail payment transactions. Legal risk also arises if the rights and obligations of parties involved in a payment are subject to considerable uncertainty; for example, if the rights of the parties are not clear when a payment participant declares bankruptcy or if a court interprets an applicable law in an unexpected way. In addition, legal risk can occur when customer agreements or contracts do not clearly establish the roles, responsibilities, governing regulations or guidelines, and dispute resolution processes, particularly with regard to RDC. Legal disputes that delay or prevent the resolution of payment settlement can cause credit or liquidity risks at individual institutions. Though unlikely, these disputes also can cause potential systemic risk to the payments system. Legal risk also arises from noncompliance with existing consumer protection statutes, regulations, and case law governing retail payment transactions (e.g., Gramm-Leach-Bliley Act or GLBA, Truth in Lending Act, Regulation CC, and Regulation E). Customer retail payment transaction records and corresponding account information are subject to the GLBA 501 (b) provisions, and financial institutions must establish effective safeguards for protecting their customer information. The bylaws and agreements between clearing house participants and bankcard companies also include specific responsibilities and liabilities.

Financial institutions and third-party service providers that do not comply with the appropriate bylaws and agreements of bankcard companies and clearing houses can be fined or lose their memberships. Thus, financial institutions should assess the risks of accepting such bylaws and agreements in their strategic planning process for new payment offerings. Given the rapidly changing landscape for electronic funds processing, it is paramount for a financial institution to pay close attention to changing legal and regulatory requirements, as well as new network rules that might create unexpected liability for the institution. As financial institutions enter into merchant card, ACH, and remote check processing arrangements with third-party service providers and originators, the institution should ensure that all such arrangements are governed by clearly written contracts which define outsourced responsibilities and liabilities. Financial institutions should carefully review contracts with third parties for outsourced services to ensure that they are not assuming the full risk of loss from failure of third parties to fulfill their contractual responsibilities. Contractual terms may further define responsibilities within the legal framework; and contracts between financial institutions, customers, and third-party service providers may further integrate risk-sharing responsibilities applicable to payments made through a specific clearing or settlement arrangement. In some cases, emerging product development may have insufficient case law to support a completely accurate analysis of the potential risk horizon. The convergence and interoperability of older, more traditional payment methods with newer technologically supported payments may create questions regarding the applicability of law and regulations governing both consumer protection and retail payment transactions. In most cases, older payment technologies for more mature retail payments (checks and credit cards) may co-exist with newer payments technologies requiring financial institutions to maintain several systems. The emergence of hybrid systems that incorporate older technologies with newer payments will require heightened review to mitigate and control legal risks. Hybrid systems and new payment technologies also increase the risk of money laundering as a result of increased volumes, transaction speed, and anonymity. Financial institutions should ensure that due diligence for new payment products or services fully evaluates the applicability of laws and regulations, regulatory guidance, and payment association rules from organizations such as NACHA, Visa, and MasterCard. Recent developments in payments over the ACH system raise legal questions regarding whether payments should be characterized as checks or electronic fund transfers. The same questions arise with respect to RDC and electronically created payment orders. As stated previously, in 2006 the Federal Reserve amended Regulation CC, shifting the liability for losses attributable to unauthorized RCCs to the depository financial institution where the check is first cashed or deposited. The liability creates an economic incentive for depository institutions to perform due diligence on the customers and RCCs. These amendments do not affect the rights of checking account customers, as they are not liable for unauthorized checks drawn on their accounts. The fact that a payment may take several different forms, both paper and electronic, during the course of processing and settlement, creates additional complexity. A payment transaction may be covered by check law, Regulation E, association or clearing house rules, or private agreement, depending on what form the payment takes. Financial institutions should understand the laws and rules that apply to payments they handle and understand the associated legal risks and liabilities they take on with respect to those payments. Bank Secrecy Act (BSA) The BSA requires financial institutions to have BSA/Anti-money laundering (AML) compliance programs and appropriate policies, procedures, and processes in place to monitor, identify unusual activity, and report suspicious activity. As such, all retail payment systems should be reviewed in terms of BSA/AML compliance requirements. The FFIEC BSA/AML Examination Manual includes examiner guidance and expectations for ACH and other payment systems that may require the collaboration of Operational, IT, and BSA examiners. This Booklet does not seek to replicate the guidance and expectations, however, and only a brief summary of this compliance risk is

offered.⁴⁴ Office of Foreign Assets Control (OFAC) OFAC administers and enforces economic sanction programs directed against countries and groups of individuals such as terrorists and narcotics traffickers. All U.S. persons and incorporated entities involved in a payment transaction (i.e., all U.S. citizens and permanent resident aliens, wherever located; all persons and entities within the U.S.; and all U.S. incorporated entities and their foreign branches) are subject to OFAC regulations.⁴⁵ For domestic ACH transactions, the ODFI is responsible for verifying that the originator of the ACH instruction is not a blocked party and for making a good faith effort to determine that the originator is not transmitting blocked funds. The contract between the ODFI and its customer should clearly define the customers' responsibilities to verify that the originator is not a blocked party and to make a good faith effort to determine the originator is not transmitting blocked funds. For high risk originating customers, the ODFI may wish to request that originating customers provide an independent validation of its controls for preventing transmission of funds to blocked parties. The RDFI is responsible for verifying that the receiver of the ACH funds is not a blocked party. For domestic ACH transactions, if ODFIs receive batched transactions from their customers that do not include international ACH transactions, they are not responsible for un-batching transactions and ensuring that they do not process transactions in violation of OFAC's regulations. If the ODFI un-batches the transactions received from its customers, or receives batched international ACH transactions, it is responsible for screening as though it had made the initial batching. For outbound international ACH transactions, on the other hand, the ODFI cannot rely upon the RDFI for OFAC screening. For inbound international ACH transactions, the RDFI is responsible for compliance with OFAC regulations.

Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or external events. Operational risk can arise from a technology failure, human or technical errors in financial models and reporting, or other internal control system deficiencies. In the case of RDC, operational risk (i.e., image/data quality, business continuity, information security, etc.) increases when deposit processing occurs at the customer location which is outside of the financial institution's direct control. As a result, the financial institution could experience delays or disruptions in processing, clearing, and settling retail payment transactions that could lead to credit and liquidity problems at other financial institutions.

Operational risk can also arise from fraud perpetrated by employees or by external sources. A financial institution is exposed to operational risk from fraud when a wrongful or criminal deception can lead to a financial loss for one of the parties involved. While fraud risk in traditional ACH activity is low, new ACH products and services, such as one-time ACH debits from Internet-based and telemarketing merchants (WEB and TEL) pose considerable fraud potential. With traditional ACH activity, financial institutions have employed strong front-end fraud controls for recurring debits they originate. These controls are typically not present with WEB and TEL transactions. The continuing growth of check-to-ACH conversion, check truncation, and the growing use of RCCs, RDC, and electronically created payment orders present new forms of fraud risks. In these situations, liability typically rests with the financial institution where the check is first deposited or the ACH item is originated. In the case of electronically created payment orders, liability rests with the financial institution that sends the file to the Reserve Bank or other correspondent. As operational processes continue to change, financial institutions will need to enhance their internal controls, as described below, to mitigate

operational risk. Existing control mechanisms may not be as effective as necessary.

Newer retail payment mechanisms, particularly using the Internet, also subject customers and financial institutions to fraud risk exposure. All of these highly automated processes typically reflect a reengineering of the existing check processes, and the existing fraud controls may not be adequate. The creation of fraudulent electronic transactions could lead to financial losses if fraudulent balances are successfully exchanged for a readily transferable form of funds, such as currency.

Operational risk controls should include sound information systems, and procedural, administrative and legal measures to prevent or limit financial loss. System measures include monetary and time limits (per transaction, per payment instrument, per client), personal authentication, and encryption techniques to ensure the authenticity and integrity of the payer and transaction information. Additional controls include the use of certified, tamper-resistant equipment (e.g., EFT/POS terminals), logical access controls to verify transactions, online verification of account balances, logging of all transactions and attempts to make a transaction, and the use of serial numbers and check digits.

Financial institutions can create a fraud detection control through a due diligence program for new account acceptance coupled with ongoing, automated monitoring of deposit account transactions. Account monitoring should be facilitated through the use of caps, limits, and triggers to measure activity on an intraday basis. Financial institutions use a variety of automated databases, such as credit bureaus, to review new accounts prior to or soon after opening the accounts. Institutions also use a number of vendor-supported automated algorithms to review deposit account transactions for unusual activity related to kiting or other fraud.

Other procedural measures for reducing fraud include: closely monitoring return rates for all customers, appropriate dual custody and separation of duties for critical payment transaction processing and accounting tasks, payment data verification, clear error processing and escalation procedures, and confidential and tamper-resistant mailing procedures for bankcards and other sensitive material. Account reconciliation processes are vital to early detection of errors and fraud. Administrative measures should include IT audit coverage of operational controls, legal controls (including regulatory compliance and agreements), and personnel issues associated with staffing and training.

In the event of an unauthorized use of a payment card, the cardholder's liability is limited to a specified amount if he or she notifies the card issuer of the theft or loss within a set time limit. To limit their own losses from POS card fraud, the bankcard companies require vendors to match the cardholder's signature on the card with the signature on the payment voucher at the POS. The bankcard companies have also introduced extensive monitoring and reporting controls to limit fraudulent activity.

In a broader view of operational risk management, financial institutions should employ vendor management programs that provide for due diligence of new service providers as well as ongoing monitoring of existing vendors. An effective vendor management program will focus on data security and business continuity.

In addition, a more effective approach to mitigate fraud risk may be to view this risk potential across channels. This requires an enterprise view of the range of retail payments activities. Those payments that use multiple payment channels for processing and clearing are subject to an increased level of fraud risk because traditional fraud detection and prevention measures are designed for single channels. Fraud is more likely to migrate to those channels where fraud detection and prevention measures are

less developed.

Mitigation of Operational Risk

Financial institutions should adopt measures that limit operational risks arising from the processing, clearing, and settlement of retail payments. Financial institutions and technology service providers participating in clearing and settlement arrangements for retail payments should ensure operational reliability for timely completion of daily processing through adequate information systems, internal controls, backup facilities, reliable technology, and adequate staff training and support. Furthermore, these organizations should adopt business continuity plans to minimize and manage the effects of interruptions. Risk analysis should identify confidential assets, critical operations, and potential threats. It should also define safeguards and countermeasures to provide appropriate protection.

Risk from fraud or error from customers that generate high volumes of RDCs, electronically created payment orders, or RCCs can be managed more effectively with the use of activity and fraud monitoring tools for those customers. Financial institutions that originate large volumes of ACH transactions directly or through third-party service providers should also consider these tools as part of their due diligence. Fraud databases and fraud analysis tools can assist financial institutions in detecting and controlling potential fraud risk. Some bankcard associations and Internet banking applications use neural network technologies or behavioral fraud analysis. These technologies utilize specialized software and hardware designed to identify patterns of behavior that enable financial institutions to identify suspicious transactions or spending. The bankcard companies have also developed numerous fraud detection and avoidance systems that member financial institutions can use to reduce losses as a result of fraudulent bankcard use. The growth of e-commerce has led many financial institutions and service providers to develop additional databases that provide early identification of potential fraud.

Identifying, evaluating, and addressing potential legal and compliance risks associated with new payment systems providers can also help mitigate operational risk. For example, a thorough legal review process can ensure that there are clearly defined roles and responsibilities for the financial institution, its service providers, and its customers. Financial institutions should also comply with the regulations and consumer compliance mandates that apply to retail payment services (e.g., Regulation E).

Financial institutions also should have appropriate risk control functions such as audit, information security, vendor management, and business continuity, as discussed in the following sections.

Audit

Action Summary

The board of directors should ensure that an effective internal audit function for the financial institution's payment systems is in place. The audit program should test the quality of retail payment systems internal controls and compliance with laws, regulations, management policies, procedures, and limits. Audit coverage should be

risk-focused and should cover all retail payment systems including third party relationships. Special attention should be given to new retail payment technologies and products.

An effective audit function should include internal and external audit coverage, tailored to the complexity of the financial institution, and based upon an accurate, enterprise-wide assessment of the institution's risk profile. Due to the potentially large transaction volumes and associated dollar value when initiating payments, internal audit coverage is critical for an effective oversight of the financial institution's retail payment systems. Auditors should perform an evaluation of the financial institution's retail payment system business lines on the basis of overall risk to the financial institution. Based on this evaluation, they should develop an appropriate schedule of audits. The audit coverage should be sufficient to validate the internal control environment surrounding the processing, clearance, and settlement of retail payment transactions. Auditors should review accounting controls and assess the effectiveness of transaction processing, clearance, and settlement processing procedures.

The board of directors should ensure the operational and IT audit program tests retail payment system internal controls, management policies, and procedures. IT audit coverage should include the design and implementation of retail payment products, and the supporting IT environment encompassing internal data centers, contingency sites, and network infrastructure. IT audit coverage should verify the adequacy of internal controls in applicable business lines responsible for managing day-to-day retail payment system services. Internal audit should assess the comprehensiveness of the institution's vendor management program to ensure the institution is appropriately managing vendor risk. ^[43] Internal audit should also evaluate payment systems when conducting BSA audits.

Information Security

Action Summary

Financial institutions should implement the appropriate physical and logical security controls to ensure retail payment system transactions are processed, cleared, and settled in an accurate, timely, and reliable manner. Security risk assessments should consider physical and logical security controls for the origination, approval, transmission, and storage of retail payment system transactions. Risk assessments should include service providers, third-party originators, and external networks that process, store, or transport customer data. Physical controls should limit access to only those staff assigned responsibility for supporting the operations and business line centers that process retail payment and accounting transactions. Physical controls should also provide for the ability to monitor and document access to these facilities. Logical controls should include identifying and authenticating retail payment system customers to help ensure the integrity of the payments. Particular attention to data security is required for emerging technologies.

Financial institutions should implement the appropriate physical and logical security controls to ensure retail payment system transactions are processed, cleared, and settled in an accurate, timely, and reliable manner. Retail payment systems contain confidential customer information subject to GLBA section 501(b) security guidelines. Payments data may also be subject to the requirements of the Payment Card Industry Data Security Standard (PCI DSS). ^[44] The board and management are responsible for protecting the confidentiality, integrity, and availability of these systems and data. The privacy risk combined with the funds transfer capability should cause these systems to rank high in all institutions' information security risk assessments. The risk assessments should consider physical and logical security controls for the origination, approval, transmission, and storage of retail payment system transactions.

Physical controls should limit access to sensitive areas to staff assigned responsibility for supporting the operations and business line centers that process retail payment and accounting transactions. Physical controls should also provide for monitoring and documenting access to these facilities.

Management should assign appropriate logical access to staff responsible for retail payment-related services and should base access rights on the need to separate the duties of personnel responsible for originating, approving, and processing the transactions. Appropriate identification and authentication techniques include requiring unique authenticators for each staff member with strong password requirements.

Logical access controls should permit access on a need-to-know basis and should assign access to retail payment applications and data based on functional job duties and requirements. Logical access controls should also protect network access. An institution's risk assessment should require protection of retail payment systems from unauthorized access through appropriate access controls, network and host configuration, operation, firewalls, and intrusion detection and monitoring. The risk assessment should also review the security of all third-party service providers. Some institutions accomplish this by isolating all payment-related applications and systems from other production applications.

A critical element in ensuring retail payment systems integrity is the appropriate identification and authentication of retail payment system customers. Transaction authorization (e.g., the approval of a funds transfer or guarantee of funds) is an essential precondition leading to the interbank transfer of funds. Financial institutions should establish an adequate internal control environment for the issuance of bankcards and related PIN. These controls can minimize processing errors and fraud and protect the confidentiality of customer and institution information.

The use of newer and emerging technologies presents new security challenges. As new retail payment products and services are developed, it may become necessary to modify methods for customer identification and authentication to ensure their effectiveness.

Many electronic banking applications use Internet-based, open network standards and rely on commonly accepted technologies to secure transmissions (e.g., secure socket layer [SSL] or other virtual private network [VPN]). The institution should establish a secure session before consumers can submit their personal banking information, and

should maintain the secure session until the time of final data transmission.

Retail payment systems should incorporate sufficient security procedures and controls to verify the integrity of the data, the confidentiality of the transmission, and the authenticity of the communication partners and data sources. The selection and use of authentication technologies and methods should depend upon the results of a financial institution's risk assessment process. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. Single factor authentication alone is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Using digital certificates, leveraging the public key infrastructure (PKI), employing biometrics and card or token-based techniques can provide cost-effective solutions for augmenting traditional technical controls. ^[45]

Institutions that participate in payment card systems should develop processes to ensure compliance with the PCI DSS. This standard is discussed further in the "Merchant Acquiring" section.

Institutions should have a response program in place that addresses security breaches, including incidents with their third-party servicers. The program should include the investigation, customer notification, if applicable, and reporting processes for regulatory and law enforcement agencies.

Business Continuity Planning

Action Summary

Financial institutions and their TSPs should develop, implement, and test appropriate disaster recovery and business continuity plans capable of maintaining acceptable retail payment-related customer service levels. For financial institutions and service providers with complex retail payment operations, business continuity plans should enable restoration of service within timeframes that are reasonable for internal business units as well as other dependent financial institutions and counterparties.

Effective business continuity planning is an important component in managing operational risk. Financial institutions and their TSPs should develop, implement, and test appropriate disaster recovery and business continuity plans capable of maintaining acceptable retail payment-related customer service levels. Business continuity plans should be based on business impact analyses and the relative importance of retail payment system products and services to the financial institution. ^[46]

For financial institutions offering basic retail payment products and services (e.g., bankcard issuance, check item processing, branch ATM access, Internet banking services), business continuity plans should include appropriate recovery targets for each retail product. The recovery targets should consider the reliance on any third-party servicer in meeting their objectives. Vendor management programs should include provisions for the disruption and restoration of service at service providers, including the consideration of service provider test plans.

For financial institutions and service providers with complex retail payment operations, business continuity plans should enable restoration of service within timeframes that are reasonable for internal business units, other dependent financial institutions, and counterparties. Financial institutions providing significant card issuing, merchant processing, EFT/POS, ACH, and retail payment-related Internet banking services should also test these plans periodically with customer financial institutions and counterparties to ensure plans are sufficient.

Vendor and Third-Party Management

Action Summary

Financial institutions should establish and maintain effective vendor and third-party management programs because of the increasing reliance on nonbank providers. Financial institutions must understand the complex nature of arrangements with outside parties and ensure adequate due diligence for the engagement of the relationships and ongoing monitoring.

Some financial institutions rely on third-party service providers and other financial institutions to provide retail payment system products and services to their customers. Many retail payment services are directly related to core processing financial institution operations (e.g., accessing demand deposit accounts through the use of financial institution-issued bankcards) and may be run in-house through the use of purchased turnkey systems. However, financial institutions outsource many retail payment-related services to third parties, including foreign-based, either to enhance the services performed in-house or to offer new retail payment services that are otherwise not cost effective.

To ensure retail payment operations are conducted appropriately, financial institutions should have comprehensive contract provisions and adequate due diligence processes. They should also monitor service providers for compliance with contracts and service level agreements. Effective monitoring should include the review of select retail payment transaction items to ensure they are accurate and processed timely. The integrity and accuracy of retail payment transactions posted to customer accounts depend on the use of proper control procedures throughout all phases of processing, including outsourced functions.

Regardless of whether the financial institution's control procedures are manual or automated, internal controls should address the areas of transaction initiation, data entry, computer processing, and distribution of output reports. These control considerations apply to processing checks, including through RDC, as well as electronically created payment orders, electronic bankcard, debit card, and ACH transactions. Financial institutions must also maintain effective control over service provider access to customer and financial institution information consistent with GLBA section 501(b). Contractual

provisions should define the terms of acceptable access and potential liabilities in the event of fraud or processing errors.^[47]

Retail Payment Instrument Specific Risk Management Controls

Action Summary

Specific retail payment instruments introduce risks that require effective internal controls and adherence to the relevant clearing house, association, interchange, and regulatory requirements. Financial institutions should address these risks in their information security and business continuity planning programs

Checks

Financial institutions manage the risk exposure to check payment processing by establishing appropriate account opening and monitoring controls. Account opening controls that incorporate information from credit bureau services may mitigate credit risk exposure to criminals and to customers with a history of financial problems. Such screening is also the basis for customer verification in support of BSA/AML compliance and for qualifying customers for RDC. Institutions should perform a credit assessment of those customers for whom they collect large dollar volumes of checks.

Financial institutions use a variety of monitoring tools during check processing as a means of identifying potential fraudulent activity or for early detection of kiting. These automated tools are typically available from major vendors. Institutions should monitor the payment activity of their customers and take appropriate action when credit limits are exceeded or when their business practices may indicate possible fraud or money laundering activity. Institutions that offer commercial customers services for RDC should make such arrangements under contracts that clearly state the liability of the commercial customer in the event of a dispute over the imaged checks.

Regulation CC requires that when a paying financial institution decides to return a check of \$2,500 or more, it must provide a notice of nonpayment to the depository financial institution, in which the check was deposited, to mitigate the depository institution's financial loss in case the customer tries to withdraw funds represented by the returned check. Regulation CC also requires a check to be returned to the depository financial institution expeditiously, regardless of the amount. A paying bank returns a check expeditiously if it returns the check to the depository bank within two business days of presentment (for local checks) or four business days (for nonlocal checks). Alternatively, a bank returns a check expeditiously if it sends the check in the same manner as it (or a similarly situated bank) would have sent the check for forward collection.

Using ECP for payment can reduce risks to depository financial institutions because it permits them to deliver check data to paying financial institutions more quickly than by presenting paper checks. The shorter delivery time permits paying financial institutions to (1) identify checks that cannot be paid and (2) notify the depository financial institution

about those returned checks using an electronic return notice and up to one day earlier than would occur with the physical exchange of paper checks.

Check truncation (the conversion of MICR information to electronic form), on the other hand, introduces the risk of unauthorized changes to converted check information in transmission or in storage. As with RDC, this risk may increase when truncation occurs at the customer location. Financial institutions should develop and implement appropriate information processing safeguards to mitigate this risk. These safeguards should include logical access controls and separation of duties to minimize potential tampering with electronically converted check information and images during processing, and to ensure the MICR and check image databases are protected from unauthorized access. Check truncation also introduces the risk that a customer's account may be debited twice for the same check. This happens either when the MICR data is read, the account is debited, and the check is accidentally sent to the proof/sorter where it is read again and the account is debited a second time or when an electronic check file is inadvertently duplicated. Financial institutions should develop preventive controls to avert checks from being read twice or electronic check files from being duplicated or processed twice, and they should have detective controls to determine whether debits arise from the same check. These controls should also be applied to processes where checks are converted to ACH debits.

Check fraud is a significant factor in losses reported by financial institutions. The leading form of check fraud is check kiting; that is, presenting checks to two or more financial institutions for the purpose of fraudulently obtaining interest-free unauthorized loans. Other types of check fraud include forged, altered, and counterfeit checks. "Positive pay" is a technique that can reduce check fraud by requesting businesses to send electronic files of information to the financial institution on all checks the business has issued. The financial institution compares this information against electronic information regarding checks presented for payment. If a check presented for payment is not included in the positive-pay information, the institution requests the corporation to make a pay/no pay decision.

ACH

ACH operations pose a variety of risks including credit, liquidity, and operational. NACHA and the two national ACH operators (the Reserve Banks and EPN) have clear expectations that financial institutions will manage these risks, particularly when the institutions engage in riskier ACH activities. In recent years, the ACH operators have begun to offer a variety of risk management tools to help control ACH risks. Financial institutions should employ those tools that are commensurate with the risks taken.

The risk of fraud can be mitigated through proper due diligence for all originating customers and strict adherence to ACH and credit policies. Additional mitigation can be achieved by avoiding high risk businesses and customers. Limits should be appropriate for the risks of each customer and the use of pre-funding arrangements or reserves can be effective in controlling losses. Management should review monitoring reports offered by the ACH operators that can assist in early detection of unauthorized ACH transactions.

For ACH credit entries, a financial institution that serves as the ODFI incurs credit risk upon initiating the entries until its customer funds the account. The ODFI is responsible for settling payments originated using its routing number even if the transactions are outsourced to third-party service providers. The RDFI incurs credit risk when it grants

funds availability to its customer prior to the final settlement of the credit entry. For ACH debit entries, the ODFI incurs credit risk from the time it grants funds availability to the originator (usually on the settlement day) until the ACH debit can no longer be returned by the RDFI. If the transaction is properly authorized, returns must be made no later than the second banking day following settlement. If not authorized properly, the financial institution exposure can be up to 60 days from when it sends a periodic statement to the consumer. An ODFI will normally charge back a returned ACH debit to the originator. However, the ODFI may suffer a loss if the originating account has insufficient funds, is closed, or is frozen because of bankruptcy or other legal action.

To manage its credit exposures, an ODFI should establish policies, procedures, and limits that acknowledge the risks certain businesses and customers bring to an ACH operation. Higher risk businesses include gambling and adult entertainment firms. The financial institution's policies should clearly state the types of businesses and customers that are acceptable and should treat all ACH customers as unsecured borrowers that are subject to the institution's standard credit review and approval process. An ODFI should conduct thorough due diligence of its originating customers, including understanding the nature of their businesses and financial condition. For certain customers, pre-funding or reserve arrangements may be necessary to control the risk. On an ongoing basis, an ODFI (and its service providers) should monitor the creditworthiness of its customers, and establish and periodically review ACH exposure limits for them. In addition, an ODFI should implement procedures to monitor ACH entries relative to the originator's exposure limit across multiple settlement dates. Breaches in limits should be reported to the appropriate levels of management. An ODFI should monitor and research frequently the returns, particularly unauthorized returns. The Federal Reserve and EPN can provide such reports to ODFIs.

An RDFI should establish prudent overdraft and funds availability policies and practices to mitigate its credit exposures. Credit risk, with respect to a debit entry, arises if the RDFI allows the debit to overdraw its customer's account. When a financial institution fails to comply with the NACHA rules, it exposes itself to contractual liability and fines. In addition, Regulation E applies to electronic fund transfers, including ACH transactions. The notice, authorization, error resolution, and timing requirements of Regulation E are of particular importance. Noncompliance with Regulation E exposes a financial institution to litigation and civil money penalties. Financial institutions should also monitor their compliance with applicable BSA and OFAC requirements concerning unusual transactions and transactions involving blocked parties.

Financial institutions should understand the impact that ACH transaction risk has on their liquidity. For example, an ODFI may not be able to settle (collect) an ACH debit, or an RDFI may not be able to settle an ACH credit because of fraud, service disruption, or the default of an ACH Network participant. This could impair the financial institution's ability to meet its obligations and result in losses. Financial institutions should consider the volume of their uncollected ACH transactions as part of their liquidity risk management practices. For certain customers, pre-funding arrangements may be used to reduce liquidity risk.

Given the highly automated nature of ACH activities, operational risks should be managed closely. Clear policies and procedures should establish the proper control environment. Exceptions and operational problems, including processing delays and customer complaints, should be monitored in a timely manner. Management and staff should be familiar with NACHA rules and the requirements of the Reserve Banks and EPN. Well conceived and tested contingency plans are vital given the time sensitive nature of ACH transactions. Higher expectations for BSA compliance require additional

attention from management. Audits should be performed on a frequent basis by qualified auditors.

Third-Party ACH Processing

While a financial institution's responsibilities do not change with the use of a technology service provider for ACH processing, its risk exposure may increase as a result of the servicer's direct access to an ACH operator. A TSP may transmit ACH transactions directly to an ACH operator using the ODFI routing number. However, it is the ODFI that warrants the validity of each entry transmitted by the service provider, including the basic requirement that a receiver has authorized all entries. To reduce risk to all parties, the financial institution should establish controls over TSP operations, and the ODFI should maintain control over its settlement accounts. ^[48]

Although the federal regulators do not enforce the NACHA rules, a financial institution subject to them should have appropriate risk-management and control processes to ensure compliance with these rules. For example, NACHA requires TSPs performing ACH processing functions on behalf of an ODFI or RDFI to conduct an annual compliance audit covering the requirements of their rules. The financial institution should review and assess all audits of its service provider's internal controls. NACHA rules also require the ODFI to have contractual agreements with third-party senders specifying that the third-party sender is in compliance with NACHA rules and applicable laws and regulations. NACHA rules further require the ODFI to have an agreement with a TSP that has direct access to an ACH operator. NACHA specifies that the agreement sets out the rights and responsibilities of all parties, including:

- A requirement that the third-party service provider obtain the prior approval of the ODFI before originating ACH transactions for originators under the ODFI routing number. ODFI approval of each originator should be contingent upon the creditworthiness of the originator and the execution of an originator and ODFI agreement.
- ODFI dollar limits for files that a TSP deposits with the ACH operator. The service provider should notify the ODFI of any file exceeding established dollar limits before depositing the file at the ACH operator so that the ODFI can either approve it as an exception or hold it until the next business day.
- A provision that restricts the TSP's ability to initiate corrections to files already transmitted to the ACH operator. The ODFI should restrict correction capability. If the TSP has the ability to make file corrections, the ODFI should authorize and approve any changes to the file totals before the ACH operator releases the file for processing. ^[49]
- A requirement that a third-party sender who enters into an agreement with an ODFI establish the identity of each originator using commercially reasonable methods, warrant that the originators will assume their responsibilities under NACHA rules, and warrant that it will assume the liabilities of the ODFI. ^[50] The lack of a direct relationship between the ODFI and the originator poses a risk to the ODFI. The ODFI should conduct proper due diligence, establish exposure limits, and employ other monitoring procedures to ensure that the business practices of the third-party sender and its merchant clients do not create an undue risk to the ODFI. The ODFI

should be able to substantiate that the third-party sender has sufficient creditworthiness to back the warranties it makes relative to the risk, nature, and volume of ACH transactions; the underlying originators; and the exposure duration.

NACHA also requires participating financial institutions to conduct annual audits of their ACH operations to assess compliance with NACHA rules. These audits can provide examiners with insights into the quality of ACH operations.

Risk Considerations for Business Banking EFT Payments

Financial institutions that offer corporate customers access to Web-based business banking applications to facilitate the direct origination of payments (e.g., ACH credits/debits, wire transfers, etc.) create special risk considerations for the financial institution and its corporate customers. These applications offer corporate customers an efficient way to conduct treasury management activities such as invoice payments and funds transfers. However, these features also increase the velocity in which errors and fraud can subject businesses or the bank to loss and can be the target of malicious software designed to circumvent online authentication methods to obtain credentials that can be used to initiate fraudulent payments.

Ongoing education of corporate customers remains one of the best ways financial institutions can mitigate the risks associated with online business banking applications. This is especially the case for some small businesses and community-based corporate entities (e.g., churches, schools, etc.) where the awareness of payments fraud techniques may be limited and the impact of a fraud can be significant. In addition to providing a secure environment for corporate payments (e.g., strong encryption, transaction risk profiling, etc.), financial institutions can help mitigate corporate payments risk by ensuring their corporate customers understand the importance of good business practices such as payment origination dual controls, daily account reconciliation, and other measures to protect the integrity of the corporate customers computer systems (e.g., virus protection, operating system upgrades, etc.).

Credit Cards

Credit and fraud losses are two of the most significant credit card-related risks to a financial institution. Credit losses due to contractual delinquency and bankruptcy account for the majority of credit card charge-offs. Fraud includes unauthorized use of lost or stolen cards, fraudulent applications, counterfeit or altered cards, and the unauthorized use of a cardholder's credit card number for card-not-present transactions.

Consumer compliance regulations (Regulation Z and Regulation E) and association operating rules (Visa and MasterCard) provide significant consumer protection for fraudulent transactions. According to Regulation E, if cardholders report timely the loss of their credit cards, they are responsible for no more than \$50 of the charges resulting from fraud. Regulation Z provides additional billing error resolution procedures. Visa, MasterCard, Discover, and American Express have zero liability programs, which indemnify card holders for all fraudulent losses in many circumstances. The issuing financial institution or the merchant pays the costs of any fraud involving credit cards. At a minimum, the merchant should obtain an authorization, a cardholder's signature, or an electronic imprint of the card (electronic information on the card) at the POS. The merchant is required by the card companies to cover fraudulent transactions through the

chargeback process if it does not follow the minimum procedures. This has become a significant issue for many online retailers processing card-not-present transactions. The major bankcard companies; however, have introduced services to reduce the liability of the merchants. Under one initiative, issuers will assume losses for fraudulent transactions if the payment was authorized using the bankcard company's authentication procedures.

A control method financial institutions use to reduce risk is the authorization process to approve the credit transaction. For example, when the merchant swipes the bankcard, the issuer can deny authorization of the transaction if the consumer is over his or her credit limit, is delinquent, or if the card has been reported as stolen. Financial institutions can also employ the address verification service (AVS) to verify a cardholder's billing address and other pertinent information. AVS is used for mail, telephone, and Internet transactions.

Employing the appropriate underwriting, account management, monitoring, and collection practices can mitigate credit risk. By setting standards that reduce the probability of delinquency and fraud, financial institutions can more effectively control credit losses.

Debit/ATM Cards

A significant risk with PIN or signature-based debit or ATM cards is that unauthorized individuals will obtain them and make fraudulent transactions. Financial institutions and their technology service providers should mitigate these risks by executing financial institution-merchant and financial institution-customer contracts that delineate each party's liabilities and responsibilities. Institutions should also establish adequate physical safeguards including the installation of surveillance cameras and access/entry control devices. State and federal laws, particularly Regulation E, protect consumers by limiting their liability if they give notice of lost or stolen cards, or of unauthorized EFTs within a specified period.

ATM stand-in arrangements, which enable EFT/POS networks to authorize transactions if a card issuer or processor is unable to authorize and process transactions, also increase the potential for fraud since normal credit limit and authorization procedures are not in effect. Stand-in authorization arrangements should include reasonable credit limits and defined terms of duration to limit potential financial loss.

Card/PIN Issuance

Financial institutions also assume certain fraud-related risks when issuing credit, debit, and ATM cards either in-house or under contract to third parties. Inadequate internal controls or ineffective card and PIN issuance procedures may result in fraudulent customer transactions. Inappropriate separation of duties that allow employees access to both customer account and PIN information exposes the institution to potential employee fraud.

Embossing and encoding blank plastic card stock, if conducted in-house, should be performed in a secure area and include inventory controls, accounting controls for the number of cards used (including test and reject cards), and dual controls for blank card stock storage. Procedures for the interim storage and accounting of card stock should

exist for all cards not under dual control. Adequate controls should also exist for captured cards (cards confiscated by an ATM machine or elsewhere).

Accountability controls should also be established to ensure all cards initially disbursed from the storage area are either delivered to the mail area or destroyed. Returned cards should be handled by a function independent of the mail department. Control cards should be mailed randomly to customers and their delivery should be validated within a few days to ensure that no theft has taken place.

PIN generation should be done at the time of card issuance. Active PIN information should be controlled, including encrypting the information on storage devices. Access to PIN databases should be restricted on a need-to-know basis. Staff access to PIN information should be reviewed periodically to confirm controls are current and working effectively.

The PIN should not appear in printed form, and staff members should not be able to retrieve or display a customer PIN online. PIN mailers should be processed and delivered with the same level of security used for mailing cards, and an active PIN should never be included with the card mailed to a customer.

The PIN should not be transmitted unencrypted, and the PIN system should record the number of unsuccessful PIN entries, restricting access to a customer's account after a limited number of attempts. If a customer forgets the PIN, he or she should select a new one rather than having staff retrieve the old one.

For institutions that outsource these functions to service providers, written agreements should define roles and responsibilities and detail control and problem resolution procedures. Effective vendor management should include a periodic review of service providers control environments and relevant internal and external audit reports.

Merchant Acquiring

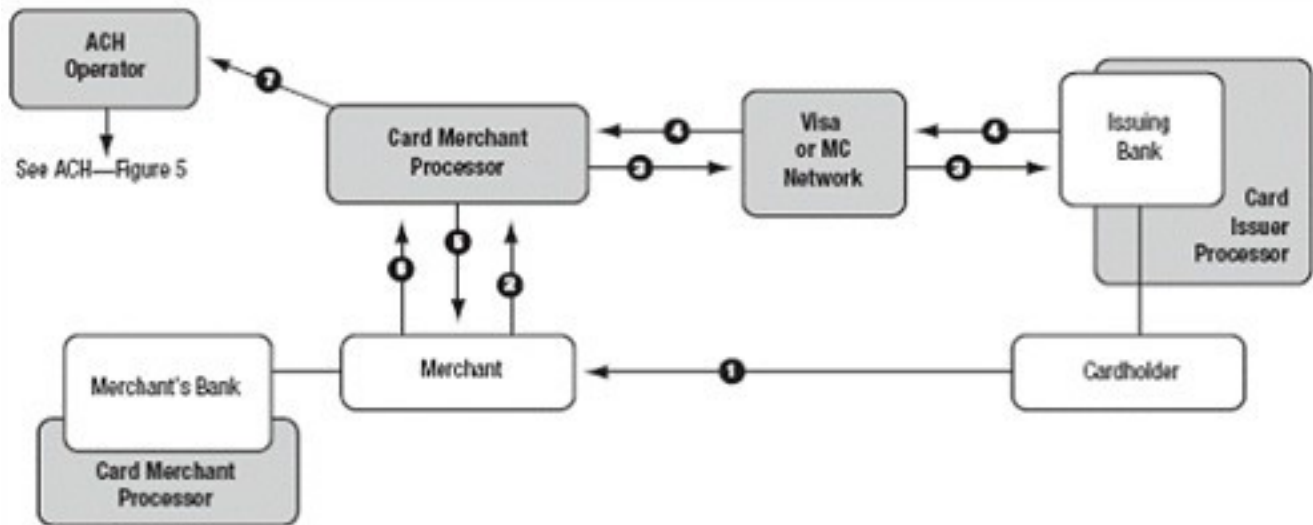
Basic credit card processing participants include the cardholder, cardholder's issuing bank, merchant, merchant's acquiring ^[51] bank, and the credit card association (e.g., Visa, MasterCard, Discover, AMEX, Diners Club).

Merchants wanting to accept card association-branded credit card sales payments must be sponsored by an acquiring bank that is a member of the credit card association. Merchants may maintain a settlement account with their acquiring bank, or settle via ACH transactions between the acquiring bank and the merchant's bank. Acquiring banks typically do not process their merchants' transactions directly so this function may be outsourced to a third-party service provider (merchant acquirer) that performs the data processing functions of authorization and clearing and settlement. Some merchant banks may also engage the services of an ISO or Member Service Provider (MSP) to solicit and sign up merchants and merchant transaction processing services. Regardless of the presence of such third parties, the credit card networks expect the acquiring bank to be the risk-controlling entity throughout the credit card process. This section will address risks from the acquiring bank's perspective.

The credit card transaction process is initiated when the consumer or merchant swipes the customer's credit card through a POS terminal. The credit approval and payment transaction processing is the same for card-not-present (mail order, telephone order, Internet sales) as they are for card-present transactions. Card-not-present retailers have

additional authentication requirements. The terminal reads and electronically transmits the card number, purchase amount, and merchant ID via the appropriate credit card association network. The credit card association forwards the electronic transaction to the issuing bank or its designated processor to verify that the account is valid and that the customer has adequate credit to cover the purchase. The issuing bank responds back through the network with either an authorization or rejection. Once the merchant receives acknowledgement through the POS terminal, the sale is completed or rejected.

Generally, at the end of each business day, a merchant sends his or her daily charge activity in batch form to his or her acquiring bank or its designated processor who forwards the transaction information to respective credit card associations for clearing. Individual transactions are sent to the issuing banks for customer account processing and debiting of the cardholder's account. Settlement occurs through the card association with the transfer of funds from the issuing banks to the respective merchant's bank. The merchant's acquiring bank posts a credit of the net sales proceeds less interchange and charge-backs to the individual merchant account.



Authorization

1. A consumer uses a credit card to pay a merchant.
2. The merchant sends the encrypted transaction data to a card merchant processor (e.g., First Data Merchant Services) for authorization.
3. The card merchant processor sends the transaction data to the consumer's (issuing) bank over the Visa or MasterCard network. The issuing bank is a licensed member of Visa or MasterCard and holds agreements with, and issues cards to, consumers.
4. The issuing bank authorizes the amount and issues an authorization code or declines the transaction.
5. The card merchant processor notifies the merchant that the transaction either has been authorized or declined. The merchant requests the consumer's signature as authorization for the transaction or notifies the consumer that the transaction has been declined.

Processing

6. Once authorized, the transaction must be "captured" by the merchant. The capture uses information from the successful authorization to charge the authorized amount of money to the consumer's credit card. The merchant accumulates captures and credits into a batch, which then will be settled as a group. The merchant submits the batch to the card merchant processor to finalize the transactions. (If the consumer returns goods after a transaction has been captured, a "credit" is generated.)

Settlement

7. The card merchant processor receives the information and settles the batch, then sends ACH items through the ACH operator to the issuing and merchant banks. (See Figure 5; the merchant bank is the ODFI, with the card merchant processor serving as authorized sending point.) The operator settles transactions between the issuing and merchant banks. The merchant bank credits the merchant's account.

Note: Many merchant banks hire a third party (acquiring processor) for bankcard processing. The processor provides credit card processing, billing, reporting and settlement, and operational services to the merchant bank.

Figure 12: Diagram of typical credit card transaction ^[52]

As Figure 12 shows, the credit card process is a technology-driven payments process. The payment process relies almost exclusively on the effective application and monitoring of strong technology standards and practices to protect transactional data integrity and to mitigate operational risks across the entire payments network.

Operational and data integrity risks can arise from improper processing of bankcard

transactions, inadequate internal controls, employee error or malfeasance, and other operational challenges inherent when processing within a multi-participant environment. To ensure these risks are mitigated, numerous technological and operational safeguards must be considered when assessing the acquiring banks' abilities to manage and control risks posed by merchants and contracted third-party payment processors.

A key mitigating factor to data integrity risk is the acquiring bank's responsibility to ensure that magnetic-strip data is not retained by merchants and third-party service providers. Many of the publicized data breaches have occurred because merchants and third-party service providers have retained customer sensitive data. Generally it is not acceptable for any participant to retain magnetic-stripe data on a post-transaction basis. Bankcard company rules prohibit-post transaction storage of full-track data (Track 1 and Track 2), CVV2/CVC2/CID/CAV, and, if applicable, the PIN block. CVV2/CVC2/CID/CAV are terms used by the various bankcard companies to refer to a unique check value that is printed on the back of the card and/or encoded in the magnetic strip. Track 1 and Track 2 data is encoded on the magnetic strip and contain information such as account number, cardholder's name, card expiration date, and service codes. Merchants and third-party service providers are allowed to store the cardholder's name, account number, and expiration date on a post-transaction basis as long as the information is encrypted, hashed, or truncated. Merchants and third-party service providers should have transaction data access protected using strong passwords and should have all data-access activity logged and available for independent review. Servers holding cardholder data should be hardened to minimize the risk of unauthorized access. Cardholder data should never be stored on a server connected to the Internet.

Historically, merchant responsibility for reporting a data breach has not been governed universally by any one entity, law, or set of guidelines other than bankcard company rules. In recent years, many states have passed legislation with various requirements for merchants reporting data breaches and various forms of financial liability.

Merchants relying on Web-based applications to conduct business should ensure that the applications are developed using IT industry secured-coding guidelines. All sensitive data transmitted via public networks must be encrypted using IT industry-standard encryption or higher. This also applies to all wireless transmissions, especially at the merchant retail level. Retail card payments containing sensitive customer information and processed using an unencrypted wireless transmission have been captured by fraudsters simply by sitting in the retailer's parking lot with a laptop computer.

Acquiring banks are ultimately responsible for any risks posed to the payment system by their sponsored merchants and third-party service providers. Management and the board of directors of all participants, including the acquiring banks, must have a clear understanding of the risk associated with acquiring activities and must understand their obligations under credit card association rules.

The credit card associations require acquiring banks to ensure that their merchants and third-party service providers comply with the Payment Card Industry Data Security Standards (PCI DSS). For third-party service providers and large merchants, PCI DSS compliance validation must be performed annually by a Qualified Security Assessor that has been approved by the PCI Security Standards Council. Smaller merchants must validate compliance annually through completion of a self-assessment questionnaire. It is not uncommon within the industry for a large number of merchants, and even some third-party service providers, to be in noncompliance with PCI DSS, potentially exposing their acquiring bank to risk and financial loss from fraud, lawsuits, and fines. Additionally, issuing banks that use third-party service providers for transaction

processing are required by the card associations to ensure that their providers are in compliance with PCI DSS.

There are six categories of PCI compliance security standards. ^[53]

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

Requirement 5: Use and update regularly anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Test security systems and processes regularly.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security.

In addition to protecting cardholder information, the credit card payment process requires acquiring banks to maintain strong credit practices over their commercial customers (merchants). The credit risk incurred by acquiring banks is similar to that of ACH ODFIs in that the acquiring bank bears the financial obligation if the merchant fails to pay.

As with any line of credit, acquiring banks are responsible for ensuring credit screening of current and prospective merchants. The acquisition of new merchants is called "merchant boarding" and may be done by the acquiring bank or, more frequently, by a third party such as an ISO. The acquiring bank is responsible for due diligence of new merchants regardless of whether the bank or a third party performs the merchant boarding. The screening process should include physical inspection of premises; a credit history review; background check; and a review of business plans and operations, including projected sales volumes, chargeback activity, and type of sales (card-present or card-not-present). For online merchants, the screening process should include a

review of Web site content and functionality. Additionally, phone, mail and Web-based merchants should be monitored closely to ensure no illegal or high-risk business activity is being conducted. Of particular concern are Web sites that present higher levels of repudiation rates which could result in higher levels of credit losses.

The main source of credit risk to acquiring banks are chargebacks resulting from cardholder disputes that merchants cannot honor. When the merchant is unable to pay its chargebacks due to bankruptcy or fraud, the acquiring bank must cover the chargeback and pay the issuing bank. Acquiring banks should manage carefully the merchant portfolio and employ appropriate underwriting, chargeback processing, and fraud monitoring.

The acquiring bank is also ultimately responsible for credit and fraud risks presented by merchant accounts acquired through ISOs or MSPs. The ISO or MSP cannot be a member of a credit card association but can represent an acquiring bank in a merchant relationship. Acquiring banks must register their ISOs or MSPs with the credit card associations, and a written merchant agreement must be in place outlining the relationship, roles, responsibilities, and liability of each of the parties - ISO or MSP, merchant, and merchant acquirer.

Acquiring banks have a number of options to monitor and control credit risks in order to minimize fraud losses at the merchant level. Acquiring banks should have reports providing information such as: average sale-ticket size for the business being conducted, chargeback level and frequency, inactive merchants, percentage of manually keyed transactions to total transactions, same dollar amounts in submitted batch, large number of even dollar-amount transactions, increasing percentage of declined or referred authorizations to total sales, and continuous or frequent zero balance in DDA accounts. These reports may also be useful for identifying potential money laundering red flags.

If an acquiring bank has concerns regarding a merchant, it has the ability to delay funding, install a front-end fraud monitoring system, acquire bank statements and credit reports, and visit the merchant's place of business. Acquiring banks can also require a reserve balance be held, generally as a percentage of credit card receipts, and it can require the merchant to purchase chargeback insurance.

Examiners should assess the actions the acquiring bank has taken to ensure third-party service providers, ISOs or MSPs, and merchants are protecting the bank's interest.

EFT/POS and Credit Card Networks

Financial institutions should have accurate audit trails for all transactions at each network switch point. The audit trails should identify the originating terminal and destination. To ensure accurate transaction posting, the financial institutions should have adequate procedures in place to control transaction activity if the EFT/POS network becomes inoperable. Also, financial institutions should document and monitor procedures for balancing and settling transactions to ensure that they adhere to interchange policies. Each participant in the switch should receive adequate transaction journals and exception reports necessary to facilitate final settlement for the institution.

A financial institution should establish stand-in processing arrangements with peer financial institutions as part of its disaster recovery and business continuity plans to ensure availability of the service. Additionally, it should have adequate oversight and

contract provisions for all outsourced services to ensure continuity of expected service levels. Agreements between switch or network participants should delineate each party's liabilities and responsibilities. The agreements should detail basic control items concerning normal and contingency processing and assign responsibility for corrective action. Grievance procedures and arbitration policies are also an important part of participant agreements.

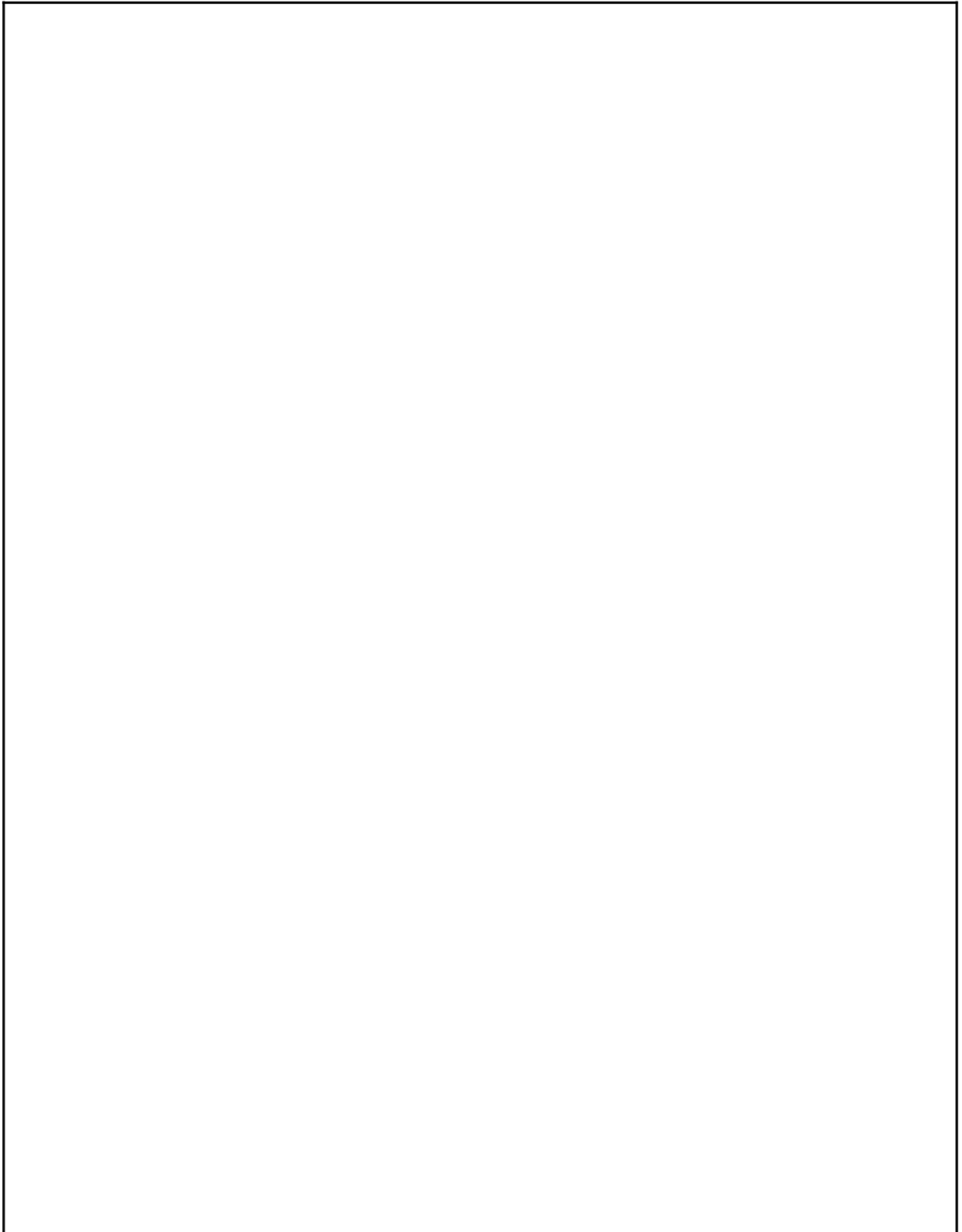
Internet and Telephone-Initiated ACH

Financial institutions originating ACH debit entries through the Internet should ensure they are in compliance with NACHA requirements. NACHA rules establish a WEB standard entry class (SEC) code for Internet-initiated ACH debit entries to which a number of requirements apply. The rules apply to originators and also affect the ODFI and its service providers. Under these rules, financial institutions must use the WEB SEC code to identify all ACH debit entries to consumer accounts that a receiver authorizes through the Internet. This code applies to both recurring and single entry ACH debits. In addition, an ODFI that transmits WEB entries must warrant that its originators have met certain NACHA standards.

Financial institutions offering TEL origination services on behalf of their customers are exposed to substantial risk from merchants that may be engaged in fraudulent or deceptive business practices. Therefore, these institutions should adopt applicable NACHA risk management practices.

Endnotes

[1]	This booklet uses the terms "institution" and "financial institution" to describe an insured bank, savings association, and credit union, as well as TSPs providing services to a financial institution.
[2]	This booklet references specific services and brand names including those trademarked by their respective companies. These references are intended solely to provide a retail payment systems overview and should not be construed as an FFIEC endorsement of any product or service noted herein.
[3]	www.ffiec.gov/exam/check21/ .
[4]	See "Nonbanks in the Payments System," March 6, 2003, and "A Guide to the ATM and Debit Card Industry," April 7, 2003, describing payment flows and clearing and settlement arrangements at: www.kansascityfed.org/home/subwebnav.cfm?level=3&theID=10724&SubWeb=10658#2003 .
[5]	NACHA is the body that establishes the rules and procedures governing the exchange of automated clearinghouse payments.
[6]	This booklet addresses the risks and controls associated with the bill payment transaction. See the IT Handbook E-Banking Booklet for the risks and controls associated with the front-end bill payment application used to initiate bill payments.
[7]	Interoperability refers to the ability of diverse retail payment systems to exchange data with a minimal loss of integrity. Many retail payment systems lack consistent protocols defining the data and the data fields in each system. Consequently, data cannot be readily moved from one system to another without manipulation.
[8]	For further information, see the American National Standards Web site at www.ansi.org/ .
[9]	Truncation is the process of removing a paper check from its processing flow. In truncation, both sides of the paper check are scanned to produce digital images. If a paper document is needed, these images are inserted into specifically formatted documents containing a photo-reduced copy of the original checks called a "substitute check."
[10]	The term "bank" includes any depository institution as defined in 12 U.S.C. 461 (b) (1)(A).
[11]	See www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf for FFIEC Guidance on Risk Management of Remote Deposit Capture.
[12]	It is important to note that check conversion requires appropriate disclosures to the check writer and is not available for all checks.



[13]	A remotely created check (sometimes called a "demand draft") is a check, often created by a payee or its service provider, drawn on a customer's bank account. The check often is authorized by the customer remotely, by telephone or on-line and therefore does not bear the customer's handwritten signature.
[14]	A demand draft created by the paying bank is not an RCC. See definition of RCC in Regulation CC.
[15]	The "midnight deadline" for the return of a check is midnight on the next banking day following the banking day on which the check is presented.
[16]	See www.frb services.org/files/regulations/pdf/operating_circular_3.pdf for Operating Circular No. 3: Collection of Cash Items and Returned Checks, effective July 15, 2008.
[17]	See www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf for FFIEC Guidance on Risk Management of Remote Deposit Capture.
[18]	See www.ffiec.gov/bsa_aml_infobase/default.htm .
[19]	See the IT Handbook Wholesale Payment Systems Booklet for a discussion of Fedwire®.
[20]	See www.frb services.org/nationalsettlement/index.html .
[21]	Check authorization is typically performed by a third-party service provider.
[22]	The original or a qualifying substitute check is needed for presentment unless agreed to otherwise.
[23]	See www.nacha.org/ for further information on NACHA.
[24]	EPN is a subsidiary of The Clearing House (formerly known as the New York Clearing House Association).
[25]	See www.frb services.org/files/regulations/pdf/operating_circular_4.pdf for Federal Reserve System Operating Circular No. 4 on "Automated Clearing House Items."
[26]	NACHA typically uses the acronym TPSP to designate third-party service providers. Generally, TPSPs are not the same as technology service providers (TSPs), the term the FFIEC uses to denote third-party entities that provide technology services to financial institutions. It is possible that a particular TPSP may also be a TSP, but for the purposes of this booklet, no such connection is made.
[27]	See NACHA International Transactions Executive Summary: http://www.nacha.org/IAT_Industry_Information/docs/IAT%20Executive%20Summary%207%203108.pdf

-
[28]	The ODFI reporting requirements also requires ODFI to provide NACHA with information pertaining to each originator or 3rd party sender return rates which exceed a defined threshold.
[29]	More information about these rule changes and other developments, including proposed rules changes and pilot projects, may be found at the NACHA Web site: www.nacha.org .
[30]	"Merchant acquirer" is a broad term used to describe a number of industry participants including third-party service providers, independent sales organizations (ISOs), and other agents. The operating regulations of the major payment card networks require these nonbank entities to be sponsored by a member financial institution (acquiring bank) and to register with the payment network.
[31]	For purposes of this booklet, the bankcard systems, MasterCard and Visa,, are referenced interchangeably as companies and associations.
[32]	Some private label (store) credit card retailers actively manage card issuance and credit relationships through affiliated financial institutions.
[33]	Non-financial institution processors must be sponsored by financial institutions to process merchant transactions.
[34]	Each business day, the association's settlement financial institution receives information from the association about issuer and acquirer positions, sending Fedwire® 1031 draw-down messages to all of its issuers with instructions to fund their settlement accounts for those amounts. The association's settlement financial institution debits issuer accounts for those amounts and credits the appropriate acquiring financial institution accounts. If an issuer does not fund its account on time, the association will intercede, cover the short position, and assess a penalty fee on the issuer.
[35]	NACHA Rules Interpretation: Proper Use of SEC Codes and Aggregation of Transactions, Issued November 9, 2007, effective: August 4, 2008. This interpretation provides that transactions may not be aggregated unless specific circumstances exist; specifically, they must be aggregated under the WEB or PPD codes if the transactions are accumulated in an account for more than 14 days.
[36]	FFIEC Guidance "Authentication in an Internet Banking Environment," October 2005 www.ffiec.gov/press/pr101205.htm
[37]	See http://irda.affiniscap.com/associations/2494/files/Publications/FM_Exec_Summary.pdf
[38]	See the IT Handbook Outsourcing Technology Services Booklet.
[39]	For more details, see www.federalreserve.gov/paymentsystems/psr/relpol.htm .
-

[40]	See the IT Handbook Wholesale Payment Systems Booklet for additional information on National Settlement Service and PSR policy.
[41]	See the IT Handbook Management Booklet
[42]	Insured depository institutions are subject to Regulation F (Limitations on Interbank Liabilities, 12 CFR Part 206) which requires institutions to monitor and limit their exposures to correspondents.
[43]	See the IT Handbook Audit Booklet.
[44]	More information on PCI Data Security Standards may be found at the website: www.pcisecuritystandards.org .
[45]	FFIEC Guidance "Authentication in an Internet Banking Environment," October 2005 & "Authentication in an Internet Banking Environment - Supplement" June 2011.
[46]	See the IT Handbook Business Continuity Planning Booklet.
[47]	See the IT Handbook Outsourcing Technology Services Booklet.
[48]	See the IT Handbook Outsourcing Technology Services Booklet.
[49]	The ACH operator usually requires an authorization from the ODFI before processing a file. Failure to receive ODFI authorization will result in the ACH operator deleting the file, giving the ODFI control over its exposure from files originated or subsequently changed by a TSP.
[50]	Automated Clearing House Rules: Article 2.1.1, Article 5.2, and Article 5.3.
[51]	Some industry publications include service providers, ISOs, and other agents in their definition of a merchant acquirer. Regardless of the term used, all participants require sponsorship by a member financial institution also known as the acquiring bank.
[52]	Source: Nonbanks in the Payments System, 2003, page 24, Federal Reserve Bank of Kansas City.
[53]	PCI Security Standards Web site: www.pcisecuritystandards.org .

Appendix A: Examination Procedures

EXAMINATION OBJECTIVE: Examiners should use the following Tier I and Tier II Retail Payment Systems examination procedures to evaluate the policies and procedures, business processes, personnel, and internal control systems of financial institutions and technology service providers. Retail payment system services include checks and share draft item processing, bankcards, payment cards, ACH, EFT/POS networks, electronic bill payment, person-to-person (P2P) and account-to-account (A2A) payment systems, and many other products and services resulting from emerging advances in technology. The examination scope should be based upon the risk profile of the financial institution or the technology service provider. The risk profile is determined through an assessment of the entity's risk environment and quality of risk management practices. This assessment should consider the formal policies and procedures established to provide these services, as well as the effectiveness of the financial institution's underlying internal control environment, including information security, business continuity, disaster recovery, and vendor management programs.

Retail payment services expose financial institutions to numerous risks, including legal, compliance, strategic, operational, credit and liquidity. Depending on the complexity of retail payment system activity, the scope of the examination may require an integrated team approach that includes the knowledge, skills, and expertise of, IT, credit, and compliance specialists.

The examination procedures may be part of either an IT or safety and soundness examination. Examiners can use the procedures in their entirety or in a modular fashion to focus on particular retail payment system products, services, or business lines. Depending on the size, complexity and risk profile of the financial institution or technology service provider, not all of the procedures may be necessary to develop overall conclusions. The examination of retail payment services may also support the institution's BSA/AML examination, which requires an evaluation of related risks in retail payment services.

The primary objectives of the Tier I procedures are to evaluate the effectiveness of the internal controls and risk management processes implemented by the financial institution or the technology service provider. Examiners should use the Tier II procedures to expand the scope of the examination further if the risk profile or organization's complexity requires additional information to establish comprehensive and accurate examination conclusions.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Assess the level of risk in retail payment systems function.

1. Determine the types of retail payment products and services offered. Consider the following:

- The types of customers using the products and services.
- The geographic service footprint (e.g., international usage)
- Check processing, particularly check imaging, remotely created checks (RCCs), and remote deposit capture
- ACH, including third-party originations, TEL, WEB, ARC, POP, and BOC
- Card issuance
- Card processing
- Merchant acquisition and processing

2. Determine whether new retail payment products and emerging technologies pose increased risk due to the lack of maturity of the respective control environments. Consider:

- New retail payment products and services that have been introduced within the past year.
- Whether the institution introduced any existing products into new markets within the past year.

3. Determine if the quality of management and staff, and the staffing levels are adequate for the specific retail payment products and processes the institution provides.

- Obtain and review the following:
 - Reports showing staffing levels, turnovers, and trends.
 - Biographies of managers and key staff
- Consider:
 - The levels of skill and experience of key managers and staff, particularly in terms of the sophistication and complexity of the products, processes, and systems.
 - Whether the institution has appropriate depth of management and staff.
 - The adequacy of staffing levels for peak operating periods.

Management and staff turnover.

4. Determine if the quality of process design and control points are adequate for existing retail products, and if these factors are considered for new products. Consider whether:

- There is adequate capacity for current and planned transaction volumes.
- Processes are clearly designed.
- Processes are automated.
- There is a reasonable degree of manual intervention.
- Any processes have been re-engineered during the past year.
- Processes are outsourced or performed at the customer location.

5. Evaluate the use of in-house and outsourced data processing systems to support retail payment products and processes. Consider:

- How stable are existing systems.
- How current are existing systems.
- Whether there is adequate capacity for current and planned transaction volumes.
- Whether the institution uses leading edge technologies or only mature technologies.
- To what extent are systems outsourced.
- Whether outsourcing arrangements are governed by contracts and service level agreements.
- Whether vendors are considered to be industry-recognized leaders.

Objective 2: Establish the scope and objectives of the examination of the retail payment systems function.

1. Review previous reports of examination for comments relating to retail payment systems. Review:

- Regulatory reports of examination, including consumer and compliance information.
- Prior examination work papers, including any documentation obtained through on-going supervision.
- Internal control self-assessments completed by business lines.
- Internal and external audit reports, including annual attestation letters.
- Regulatory, audit, and information security reports from service providers.

- Trade group, bankcard company, interchange, and clearing house documentation relating to services provided by the financial institution, particularly the NACHA required annual security audit and bankcard company self assessments.
- Supervisory strategy documents, including risk assessments.

2. Review past examination reports for comments relating to the institution's internal control environment and technical infrastructure. Review:

- The institution's processing architecture, including processing outsourcing arrangements.
- Internal controls, including physical and logical access controls in the data entry area, data center, and item processing operations.
- Electronic Funds Transfer (EFT)/Point of Sale (POS) network controls.
- Comments related to controls over Remote Deposit Capture (RDC).
- Inventory of computer hardware, software, and telecommunications protocols used to support check item processing, EFT/POS transaction processing, ACH, and bankcard issuance and acquiring transaction services.

3. Review the financial institution's risk and control assessments for comments relating to retail payment systems. Review the following risk assessments:

- External and internal audit;
- Management controls;
- Information security;
- Business continuity;
- Regulatory compliance; and
- BSA/AML.

4. Identify and obtain during discussions with management of financial institution or service provider:

- A description of the retail payment system activities performed and scope of operations, including check item processing, RDC, lock-box services that provide ACH check conversion or check truncation, ACH, bankcard issuing and acquiring,

clearance, settlement, and EFT/POS network activity.

- Operational reports for retail payment system activities, including transaction volumes, dollar amounts, and trends. Where possible, compare levels and trends with peer financial institutions. Significant increases may indicate a change in risk to the financial institution and management awareness should be evaluated.
- Organization charts of retail lines of business to determine reporting relationships and how the collective retail lines of business are structured and managed.
- The retail payment system functions performed through outsourcing relationships and the financial institution's level of reliance on those services.
- Any significant changes in retail payment system policies, personnel, products, strategy and services since the last examination, particularly the introduction of new and emerging electronic retail payment systems incorporating RDC, wireless, telephone, web-based purchasing and bill payment, prepaid cards, or P2P and A2A payment systems.
- A listing of all payment processing and clearing house settlement arrangements in which the financial institution participates. Include any bilateral retail payment clearing arrangements the institution may have with other institutions that are outside traditional clearing houses such as FedACH and EPN. Evaluate the methodology used by the financial institution in assessing its operational and settlement risk from these arrangements.
- Documentation of any related operational or credit losses incurred, reasons for the losses, and actions taken by management to prevent future losses for each retail payment system.
- A network diagram of the transaction flow from the merchant end of the network, through any intermediary processors, to the financial institution, for all types of payment channels.

5. Review the financial institution's response to any retail payment systems issues raised at the last examination and any internal audits conducted since last review. Determine:

- Adequacy and timing of corrective action.
- Resolution of root causes rather than specific issues.
- Existence of outstanding issues.

Objective 3: Assess the quality of oversight and support provided by the board of directors and management.

1. Determine the quality and effectiveness of the financial institution's retail payment systems management function. Consider:

- The alignment of the institution's business plans with its technology and operational plans for retail payment systems.
- Data center and network management and the quality of internal controls over internal ATM networks and gateway connectivity to regional, national, and international EFT/POS and bankcard networks.
- Departmental management and the quality of internal controls, including separation of duties and dual control procedures, for bankcard, ATM and debit card, ACH, check items, and electronic banking payment transaction processing, clearance, and settlement activity.
- Departmental management and the quality of information security and GLBA 501(b) compliance policies relating to retail payment system-generated customer data.

2. Assess management's ability to manage outsourced relationships with technology service providers. Consider:

- Process utilized to encrypt transactions while in route between technology service providers and the institution.
- Adequacy of contract provisions including service level, performance agreements, responsibilities, liabilities, and management monitoring.
- Management's determination of the service provider's compliance with applicable financial institution and consumer regulations and with third-party requirements (e.g., NACHA, GLBA, bankcard company, and interchange).
- Adequacy of contract provisions for personnel, equipment, and related services.
- Quality of management information systems (MIS) and reports needed to monitor the technology service provider's performance appropriately.

3. Evaluate the adequacy and effectiveness of financial institution and service provider contingency and business continuity planning. Consider:

- Ability to recover transaction data and supporting books and records based on retail payment system business line requirements and time lines.
- Level of testing conducted to ensure adequate preparation.
- Stand-in arrangements established with other financial institutions in the event of an ATM and/or POS system outage. preventing card fraud and abuse.
- Alternative access mechanisms in the event of an outage to primary access to bankcard, ACH, and other retail payment networks.

4. Evaluate retail payment system business line staff. Consider:

- Adequacy and quality of staff resources, including certifications such as an Accredited ACH Professional (AAP).
- Effectiveness of policies and procedures outlining department duties, including job descriptions.

Objective 4: Assess the quality of policies, procedures, and limits supporting retail payment services.

1. Review policies, procedures, and limits for supporting all retail payment services.

- Determine if there are written policies.
- Determine if the policies reflect the current business and processes.
- Determine if the policies establish reasonable limits.

2. Review staff training programs and determine if they are appropriate for supporting policies.

3. Determine whether the institution monitors compliance with policies, procedures, and limits.

- Determine if exception monitoring reports are elevated to appropriate levels of management.

Objective 5: Assess the quality of management information systems and reports used to manage retail payment services.

1. Review management reports for all retail payment services including reports from service providers.

- Determine if the reports are appropriate to the businesses and processes in terms of scope and frequency.
- Determine if the reports are reviewed at the appropriate levels of management.

Objective 6: Assess the quality of risk management and support for bankcard issuance and acquiring (merchant processing) activity.

1. Evaluate financial institution adherence to bankcard company rules and bylaws and regulatory requirements.
2. Evaluate whether card issuance processing is outsourced to a third party. If yes, evaluate the vendor management controls in place to govern the activities listed in steps 3 and 4.
3. Review internal procedures employed for each bankcard product and assess:
 - The integrity of plastic card and PIN issuance processing.
 - Whether processing includes appropriate separation of functions in card issuance, PIN issuance, control and storage of card stock, and the maintenance of software controlling PIN generation.
 - Whether the institution has established procedures focusing on controls preventing card fraud and abuse.
4. Determine whether the audit function periodically performs an inventory of all bankcards at each location owned or operated by the institution and that each location is included in the audit program, either directly or indirectly (e.g., as part of a branch audit).
5. Determine whether management has established inventory systems that include quality control activities such as self-monitoring for data accuracy.
6. Review a sample of consumer contracts for each bankcard service to ensure they describe adequately the responsibilities and liabilities of the institution and its customers (compliance with Regulation Z).
7. Evaluate the effectiveness of internal clearance and settlement activity as it relates to customer bankcard transactions. Consider the adequacy of:
 - Financial and accounting controls in place to clear and settle transactions.
 - Periodic reconciliation of all account postings.
 - Timely clearance or charge-off of missing items or out-of-balance situations.
8. Evaluate the effectiveness of internal credit monitoring and card authorization performed by the financial institution. Consider the adequacy of:
 - Policies and procedures for underwriting, account management, and collection activities.
 - Card authorization procedures to mitigate fraudulent use.

- MIS reports and behavioral fraud analysis.

9. For financial institutions directly involved in, or outsource, bankcard acquiring (merchant processing) services, determine the appropriateness of controls over merchant services and ISO/MSP relationships. Consider the adequacy of:

- New merchant approval and acceptance process, termination procedures, and underwriting guidelines for merchant accounts with particular attention to Web and telephone-based businesses.
- Testing of web-based business to validate site's content.
- Industry-standard MIS reports to identify negative trends and potential fraudulent activity. Potential indicators of fraud or money laundering include: a large number of manually keyed transactions, even dollar amount transactions, average sale ticket size as compared to history, same dollar amount repeated frequently in a single batch, or continuous or frequent zero balances in DDA account.
- The financial institution's use of a front-end fraud detection application either in-house design or purchased.
- Credit approval and monitoring procedures for all new and established merchant accounts. Consider use of Dun & Bradstreet reports, bank statements and credit reports.
- Chargeback processing procedures and controls, including trend, volume, age, and losses associated with merchant chargebacks.
- Agent bank programs (where the financial institution performs merchant processing for other institutions), and the level of liability assumed by the acquiring financial institution.
- Protection and storage of cardholder data and compliance with card company rules and guidelines on what data can and cannot be stored.
- Programs for requiring and monitoring merchant's and processor's compliance with card company and association standards such as PCI Data Security Standards. Review assessment document and process for completion.
- Policies and procedures relating to customer accounts that may have been the subject of security breach at the merchant/ISO location (i.e., reissue cards, monitoring and customer notification).

Objective 7: Assess the quality of risk management and support for EFT/POS processing activity.

1. Evaluate the financial institution's compliance with interchange rules and bylaws.
2. Review internal procedures employed for generating active ATM cards. Consider:

- The integrity of PIN issuance and processing, including appropriate separation of functions between card issuance, PIN issuance, and card stock control and storage.
- The maintenance of software controlling PIN generation. The review should focus on controls preventing card fraud and abuse resulting in financial loss to the institution.

3. Determine whether the audit function periodically performs an inventory of unused ATM card stock at each location owned or operated by the institution and that each location is included in the audit program, either directly or indirectly (e.g., as part of a branch audit).

4. Review a sample of consumer contracts for ATM services to ensure they adequately set forth responsibilities and liabilities of the institution and the customer. Evaluate compliance with applicable regulations.

5. Evaluate the effectiveness of internal clearance and settlement activities as it relates to customer ATM transactions. Consider whether:

- Appropriate financial and accounting controls are in place to clear and settle ATM transactions.
- Reconciliation is performed periodically for all account postings.
- Processes have been established for handling disputed items.

Objective 8: Assess the quality of risk management and support for ACH processing activity.

1. Evaluate the financial institution's adherence to NACHA and clearing house operating rules and regulations.

2. Review operational reports showing monthly or quarterly ACH debit and credit activity and, if possible, compare levels with peer financial institutions. If ACH activity is greater than peer, determine whether institution is an originating institution (ODFI). Obtain reports listing those customers for which they originate and the volumes (number of items and dollars) originated. Be sure to ask for all customers that use the ODFI's originating account number with the Federal Reserve or EPN.

3. If the institution has bilateral clearing arrangements with other institutions, review the underlying contracts and determine how the institution monitors compliance with the contracts.

4. If the institution uses a technology service provider, determine whether it performed appropriate due diligence prior to engagement and has appropriate contractual agreements governing the relationship. Determine whether the institution monitors compliance with the governing contract. Determine if the institution has an adequate business continuity plan in the event the technology service provider experiences a service disruption.

5. If the institution is an ODFI and permits third-party sender payments, determine whether it requires the third-party sender to establish the identity of each originator using commercially reasonable methods to warrant that the originators will assume their responsibilities under NACHA rules and to warrant that it will assume the liabilities of the ODFI. Determine whether the ODFI has established limits and monitoring of the third-party sender's creditworthiness relative to its underlying originators and the nature and type of ACH activity that it warrants.
6. Determine whether the ODFI's contractual agreements with each originator clearly define the specific terms for funds availability.
7. Determine whether the institution has taken steps to ensure that originators are properly educated about their obligations for handling ARC and POP source documentation and all other NACHA rules.
8. Review policies and procedures for acquisition of originating customers and determine the appropriateness of these policies for the risk profile and risk management capabilities of the financial institution. Determine whether the policies identify and seek to limit exposure to higher risk customers; such as, adult entertainment and online gambling firms, adult bookstores, escort services, and massage parlors.
9. Review policies and procedures in place to monitor originating customer balances for credit payments (e.g., payroll) to ensure payments are made against collected funds or established credit limits and daily caps. Also determine whether payments in excess of established credit limits and daily caps are properly authorized.
10. Determine whether the institution treats deposits resulting from ACH transmitted debits on other accounts as uncollected funds until there is reasonable assurance the debits have been paid by the institution on which they were drawn. Also, determine whether management monitors drawings against uncollected funds to ensure they are within established guidelines.
11. Review a sample of contracts authorizing the institution to originate ACH items for customers and determine whether they adequately set forth the responsibilities of the institution and customer. Determine:
 - Whether contracted technology service providers originating customer entries are also customers of the financial institution.
 - Whether the agreements include recognition of all relevant NACHA requirements.
 - Whether ACH clearing houses, of which the financial institution is a member, stipulate the funding arrangements (outgoing), Expedited Funds Availability Act (Regulation CC), UCC Article 4A (credit transfer only), and Electronic Funds Transfers (Regulation E).
12. Determine whether the institution has a process in place for monitoring and acting on returned items, that includes third-party vendors, where applicable..
13. Determine whether the institution uses risk management reports that are appropriate to the ACH activities and level of risk.

14. Determine whether ACH activities are considered in the institution's overall business continuity plans and insurance program.
15. Determine whether management monitors originating customers for unreasonable numbers of unauthorized ACH debits. If the volume of unauthorized ACH debits is high, it could expose the institution to greater loss.
16. Determine whether management has addressed international ACH requirements, where applicable.

Objective 9: Assess the quality of risk management and support for electronic banking related retail payment transaction processing.

1. Determine the extent to which the financial institution engages in retail payment systems, including bill payment, prepaid cards, wireless systems, contactless payment devices, remote check capture, lock-box services that provide ACH check conversion or check truncation, and P2P and A2A payments. Consider:

- Strategic plans relating to the introduction of new retail payment system products and services.
- The development of internal pilot programs and partnerships with technology service providers introducing new retail payment systems and delivery channels.
- The extent to which existing Internet and e-banking products and services include new retail payment mechanisms.

2. Evaluate the financial institution's ability to manage the development and implementation of new retail payment services, focusing on effectiveness of internal controls and provisions of consumer compliance regulations. Consider:

- Information security, including identification and authentication systems, in the deployment of any smart cards, wireless payment devices, EBPP, P2P and A2A product offerings.
- Customer disclosure and compliance information for retail payment systems using new technologies.
- Technical resources to effectively manage retail payment systems including Internet technologies, telecommunications protocols, and operations support.

3. Evaluate the financial institution's ability to incorporate new retail payment product offerings into its existing retail business lines and its effectiveness in including these product offerings in its traditional retail payment operations. Consider:

- The integration of new retail payment product offerings into existing clearance,

settlement, and accounting functions.

- Whether the financial institution relies on technology service providers for some or all of these services.

Objective 10: Assess the quality of risk management and support for checks.

1. Determine whether the accounting department handles check return item processing appropriately, reconciling all aged items.

2. If the institution offers its customers RDC services, review the appropriateness of:

- Due diligence procedures for new and existing retail customers.
- Due diligence procedures for new and existing third-party processing customers (ensure processors perform adequate due diligence over their originating retail customers).
- Underlying contracts for:
 - Assignment of liability in the event of returned, disputed, or fraudulent items.
 - Limitations or reasonable parameters regarding activity volumes, including returns.
 - Ongoing transaction activity monitoring procedures.

3. Determine whether the institution uses electronic check presentment (ECP) for payment. If yes, determine:

- The effectiveness of the financial institution's ECP implementation, including logical access controls over electronic files storing MICR and related information.
- Whether the financial institution is using positive pay.
- Whether the logical access controls over the electronic files sent by commercial businesses are adequately controlled.

Objective 11: Assess the quality of risk - management of new and emerging technology risks.

1. Determine the institution's processes for evaluating and deploying new and emerging technologies for retail payment systems. Of particular concern are retail payment products and services that do not use established networks such as ACH, or that extend operational processes to the customer location, as with RDC. Determine:

- Whether the institution conducts risk assessments prior to deployment of new and emerging technologies.
- Whether the processes involve the institution's compliance functions, including consumer compliance, BSA/AML, GLBA 501(b), and third party requirements (for example, NACHA, MasterCard, and Visa).
- Whether risk assessment and compliance status are communicated to senior management and the board of directors.

2. Assess the vendor management program over the technology service providers offering new and emerging technologies for retail payment systems. Determine:

- The adequacy of due diligence performed on the technology service provider.
- Whether management regularly reviews the financial status of the technology service provider.
- Whether management receives independent audits, third-party review, or data information security reviews performed on the technology service provider.
- Whether the information exchanged with the technology service provider is documented and meets the bank's requirements.
- Whether the dispute resolution process between the technology service provider and customer is documented and meets the bank's requirements.
- Whether MIS received from the technology service provider is adequate.

CONCLUSIONS

1. Determine the need to conduct Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.

2. From the procedures performed, including any Tier II procedures performed:

- Document conclusions related to the quality and effectiveness of the management of the retail payment systems function.
- Determine and document to what extent, if any, the examiner may rely upon retail payment system procedures performed by internal or external audit.

3. Review your preliminary conclusions with the examiner-in-charge (EIC) regarding:

- Violations of law, rulings, regulations, and third-party agreements.
- Significant issues warranting inclusion as matters requiring board attention in the report of examination.
- Potential impact of your conclusions on the Uniform Rating System for Information Technology (URSIT) composite and component ratings.
- Where necessary, communicate relevant conclusions to the EIC for the BSA/AML, or retail credit, or compliance examinations.

4. Discuss your findings with management and obtain proposed corrective action, within reasonable timeframes, for significant deficiencies.

5. Document your conclusions in a memo to the EIC providing report-ready comments for all relevant sections of the FFIEC report of examination (ROE) and guidance to future examiners.

6. Organize work papers to ensure clear support for significant findings and conclusions.

TIER II OBJECTIVES AND PROCEDURES

Examination Objective: The Tier II Retail Payment Systems Examination Procedures provide additional validation steps to verify the effectiveness of a financial institution's internal control processes over ACH, EFT/POS network, check item, electronic banking-related retail payments, and bankcard processing, clearance, and settlement. These procedures assist in achieving examination objectives, and examiners may use them in their entirety or selectively, depending upon the scope of the examination and the need for additional verification.

Examiners should coordinate this coverage with other examiners involved in assessing the institution's information systems, operations, information security, business continuity planning, and vendor management effectiveness to avoid duplication of effort and to ensure there is an adequate understanding of the control environment as it pertains to retail payment business lines.

The procedures provided in this section should not be construed as requirements for control implementation. The selection of controls and control implementation should be guided by the risk profile of the institution. Therefore, the controls necessary for any single institution or any given area may differ from those noted in the following procedures.

The Tier II Retail Payment Systems Examination Procedures provide additional validation procedures verifying the effectiveness of a financial institution's internal control processes over ACH processing, EFT/POS network processing, check item processing, electronic banking-related retail payments processing, and bankcard processing, clearance, and settlement. These procedures assist in achieving examination objectives, and examiners may use them in their entirety or selectively. Examiners should coordinate this coverage with other examiners involved in assessing the institution's information systems, operations, information security, and vendor management effectiveness to ensure there is an adequate understanding of the control environment as it pertains to retail payment business lines and to avoid duplication of effort.

A. EFT/POS and Bankcard Agreements and Contracts

1. If the financial institution is a participant in a shared EFT/POS network or if it contracts with third-party bankcard-issuing or -acquiring processing service providers, determine whether:

- Contracts with regional EFT/POS network switch and gateway operators and bankcard processors clearly set forth the rights and responsibilities of all parties, including the integrity and confidentiality of customer information, ownership of data, settlement terms, contingency and business recovery plans, and requirements for installing and servicing equipment and software.
- Adequate agreements are in place with all technology service providers supplying services for retail EFT/POS and bankcard operations (plastic cards, ATM equipment and software maintenance, ATM cash replenishment) that clearly define the responsibilities of both the service provider and the institution.
- Agreements include a provision of minimum acceptable control standards, the ability of the institution to audit the technology service provider's operations, periodic submission of financial statements to the institution, and contingency and business recovery plans.
- Contracts and agreements clearly define responsibilities and limits of liability for both the customer and financial institution and include provisions of the Electronic Funds Transfer Act (Regulation E) and the Expedited Funds Availability Act (Regulation CC) for deposit activities.

2. Determine whether management periodically reviews individual sites providing retail EFT/POS and bankcard services to ensure policies, procedures, security measures, and equipment maintenance requirements are appropriate.

3. For retail EFT/POS and bankcard transaction processing activities contracted to third-party service providers, assess the adequacy of the review process performed by management regarding annual financial statements, audit reports, and Payment Card Industry (PCI) Data Security Standard assessment.

B. Personal Identification Numbers (PINs)

1. Assess staff access to PIN data. Ensure there is separation of duties between staff responsible for card operations and staff responsible for preparing or issuing bankcards.

2. Assess the adequacy of the PIN generation process. Ensure there is separation of duties between staff responsible for PIN generation and staff responsible for opening accounts or with access to customer account information.

3. For new PIN issuance, assess the adequacy of control procedures including accountability assigned to staff initiating such transactions.

4. Assess the adequacy of PIN generation and issuance procedures to determine whether they preclude matching an assigned PIN to a customer's account number or bankcard.
5. Assess the adequacy of threshold for PIN access attempts to customer account information and funds. The threshold parameter should be set at a reasonable number of unsuccessful attempts.
6. Assess the level of PIN encryption when stored on computer files or transmitted over telecommunication lines.
7. If resets are allowed, assess the adequacy of procedures and controls for PIN/password resets. The use of single-use and temporary PIN/password is preferred.
8. Assess the adequacy of procedures for prohibiting PIN information from being disclosed over the telephone.
9. Assess staff access to PIN-related databases and determine if management restricts access to authorized personnel. Assess database maintenance activities to ensure management closely supervises and logs staff access.
10. Assess the adequacy of customer PIN selection criteria, focusing on whether the institution discourages or prevents customers from using common words, social security numbers, sequences of numbers, or words or numbers that can easily identify the customer.

C. Information Security

1. Evaluate the logical and physical security controls to ensure the availability and integrity of production retail payment systems applications. Determine:
 - Whether the physical and logical security controls established for retail payment transaction processing, clearance, and settlement services maintain transaction confidentiality and integrity.
 - Whether physical controls limit access to only those staff assigned responsibility for supporting the operations and business line centers processing retail payment and accounting transactions.
 - Whether physical controls provide for the ability to monitor and document access to all retail payment operations facilities.
2. Evaluate the effectiveness of all logical access controls assigned for staff responsible for retail payment-related services. Determine:
 - Whether management bases controls on separation-of-duties principles routinely implemented for the processing of financial transactions.
 - Whether management bases access controls on a need-to-know basis.

- Whether management bases assigned access to retail payment applications and data on functional staff job duties and requirements.
- Whether identification and authentication schemes include requiring unique logon identifiers with strong password requirements.
- Whether displayed credit and debit card account data are partially masked to prevent full account numbers from being copied.
- Whether network servers are satisfactorily hardened against the risk of internal or external hacking.
- Whether servers simply used for data storage are unnecessarily connected to the Internet.
- Whether sensitive customer information stored electronically is encrypted; if so, at what encryption level.
- Whether internal audit or other third-party have conducted a security review.

3. Evaluate the security procedures for periodic password changes, the encryption of password files, password suppression on terminals, and automatic shutdown of terminals not in use.

4. Assess whether the institution encrypts telecommunications lines used to receive and transmit retail customer and financial institution counterparty data. If not encrypted, evaluate the compensating controls to secure retail payment data in transit. Assess whether any connecting technology service provider's networks used to transport transactions are transporting transaction data in the clear (not encrypted) or use weak forms of encryption.

5. Assess whether merchants use sufficient encryption for wireless sales terminal activity transmitting sensitive customer information.

6. Assess whether customer information being stored is beyond that required by industry standards.

D. Card Issuance

1. Assess bankcard issuance activities, and review control procedures. Determine whether management:

- Issues bankcards only as requested.
- Periodically inventories bankcards.
- Maintains adequate controls for activating new accounts.

2. Assess effectiveness of the dual control procedures for blank card stock in each of the encoding, embossing, and mailing steps.

3. Assess adequacy of physical access controls for card encoding areas. Management should allow access to authorized personnel only.
4. Assess whether inventory controls for plastic card stock make them physically secure.
5. Assess whether management restricts the use of bankcard encoding equipment to authorized personnel only.
6. Assess adequacy of procedures for issuing cards from more than one location (e.g., branches) to ensure there are accountability and bankcard control procedures at each card-issuing location.
7. Assess adequacy of institution card-mailing procedures. Ensure the institution mails the card and associated PIN to customers in separate envelopes. Also ensure that the return address does not identify the institution.
8. Assess whether mailing procedures provide for a sufficient time between the card and PIN mailings.
9. Assess adequacy of returned card procedures. Determine whether adequate controls are in place to ensure returned cards are not sent to staff with access to, or responsibility for, issuing cards.
10. Assess whether there is appropriate follow-up to determine whether the correct customer received the card and PIN.
11. Assess the adequacy of control procedures (e.g., hot card lists and expiration dates) to limit the period of exposure if a card is lost, stolen, or purposely misused.
12. Determine whether the institution destroys captured and spoiled cards under dual control and maintains records of all destroyed cards.
13. Assess whether the institution adequately controls test or demonstration cards.
14. Assess whether management maintains satisfactory controls over the issuance of replacement or additional cards to the customer (e.g., temporary access cards issued to the customer).
15. Assess the adequacy of the vendor management program to determine whether the institution reviews card issuance services contracted to third parties for compliance with appropriate bankcard control procedures.

E. Business Continuity Planning

1. Assess the adequacy of the financial institution's business continuity plans for a partial or complete failure of each retail payment system. Determine whether the plans include:
 - Recovery of all required components linking the institution with third-party network switch, gateway, or related third-party data centers and bankcard processors.
 - Information relative to the volume and importance of the retail payment system activity to the institution's overall operation.
 - Provisions for acceptable store and forward procedures to protect against loss or

duplication of data and to ensure full recovery within reasonable timeframes.

- Provisions for secured transport and off-site storage of sensitive customer information.
- Stand-in arrangements with other financial institutions, allowing for interim bankcard processing in the event of an outage.
- Adequate testing of plans accounting for various recovery scenarios.

F. EFT/POS and Bankcard Accounting and Transaction Processing

1. Assess the adequacy of reconciliation processes for general ledger accounts related to bankcard and debit card transaction processing activity. Determine whether:

- Accounting reconciles bankcard and ATM transaction activities daily.
- Retail payment system supervisory personnel periodically review reconciliation and exception item reports.
- Accounting periodically reconciles accounts used to control rejects, adjustments, and unposted items.

2. Assess the adequacy of the daily settlement process for institutions participating in shared EFT/POS networks or gateway systems.

3. Assess the adequacy of transaction reconstruction procedures. Transaction files should be duplicated or otherwise retained for a minimum of 60 days, as required by Regulation E, in order to identify unauthorized transactions.

4. Assess the adequacy of the investigative unit in place to address customer inquiries and control non-posted items, rejects, and differences. Management should periodically receive aging reports that list outstanding items.

5. Assess the adequacy of separation of duties for the bankcard and EFT/POS account posting process including receipt of transactions, file updates, adjustments, internal reconciliation, preparation of general ledger entries, posting to customers accounts, investigations, and reconciliation with third-party service provider network switches and card processors.

6. Assess the effectiveness and accuracy of the adjustment process (e.g., changes to deposits and reversals) relating to retail EFT/POS and bankcard transactions processed by staff.

7. For institutions involved in bankcard issuing or acquiring services, determine whether the institution has established:

- Proper accounting controls for the balancing, settling, and reconciliation of all bankcard and acquiring accounts under its control.

- Appropriate credit and liquidity risk measures for the bankcard and acquiring business lines.
- Appropriate controls for the processing of customer or merchant transaction flows.

G. EFT/POS Operational Controls

1. Assess the effectiveness of personnel responsible for internal ATM processing. Determine whether there are:

- Controls prohibiting staff members who originate entries from processing and physically handling cash.
- Proper control of all source documents (e.g., checks for deposit) maintained throughout the daily processing cycle relative to:
 - Input preparation,
 - Reconciliation of item counts and totals,
 - Output distribution, and
 - Storage of the instruments.

2. Determine whether terminal and operator identification codes are used for all retail ATM and POS transactions.

3. Assess the adequacy of controls in place to prevent customer charges from exceeding the available balance in the account or approved overdraft lines.

4. Assess the adequacy of access controls for terminals used to change customer credit lines and account information.

5. Determine whether retail EFT equipment keyboards or display units are properly shielded to avoid disclosure of customer IDs or PINs.

6. Determine whether receipt issuance ensures customers receive a receipt showing the amount, date, time, and location for retail EFT transactions in compliance with Regulation E.

7. Assess whether each retail EFT transaction is assigned a sequence number and terminal ID to provide an audit trail.

8. Assess whether the institution regularly updates hot card or customer suspect lists and distributes them to branch banking locations.

9. Assess the adequacy of verification procedures for telephone-initiated payments or transfers and ensure confirmations are promptly sent to customers and merchants.

10. Assess the adequacy of security devices and access control procedures for EFT/

POS, bankcard, and acquiring processing facilities to ensure appropriate physical and logical access controls are in place.

H. ACH ODFI and RDFI Responsibilities

1. Determine whether agreements between the ODFI and originators adequately address

- Liabilities and warranties,
- Responsibilities for processing arrangements, and
- Other originator obligations such as security and audit requirements.

2. Determine whether the ODFI has established procedures to monitor the creditworthiness of its originator customers on an ongoing basis. Determine whether:

- The ODFI assigns credit ratings to originators.
- Competent credit personnel perform monitoring, independent of ACH operations.
- Written agreements with originators require the submission of periodic financial information.

3. Determine whether the ODFI has established ACH exposure limits for originators. Determine whether:

- The limit is based on the originator's credit rating and activity levels.
- The limit is reasonable relative to the originator's exposure across all services (lending, cash management, foreign exchange, etc.).
- Limits have been established for originators whose entries are transmitted to the ACH operator by a technology service provider.
- Written agreements with originators address exposure limits.
- A separate limit for WEB entries and other high-risk ACH transactions, as warranted, has been established.

4. Determine whether the ODFI reviews exposure limits periodically. Determine whether:

- The ODFI adjusts limits for changes in an originator's credit rating and activity levels.

- Increases in an originator's ACH debit return volume trigger a re-evaluation of the exposure limit.
- The ODFI reviews the limits in conjunction with the review of an originator's exposure limit across all services.

5. Determine whether the ODFI has implemented procedures to monitor ACH entries initiated by an originator relative to its exposure limit across multiple settlement dates. Determine whether:

- The monitoring system is automated and accumulates entries for a period at least as long as the average ACH debits return time (60-75 days).
- Entries in excess of the exposure limit receive prior approval from a credit officer.
- WEB entries and other high-risk ACH transactions (as warranted) are accumulated and monitored separately, yet integrated into the overall ACH transaction monitoring system.

6. Assess the RDFI's overdraft and funds availability policies and practices and determine whether they adequately mitigate its credit exposures to ACH transactions.

7. Determine the adequacy of the ODFI's practices regarding originators' annual or more frequent security audits of physical, logical, and network security. Determine whether:

- The ODFI receives summaries or full audit reports from the originators.
- The audits are adequate in scope and performed by independent and qualified personnel.
- Corrective actions regarding exceptions are satisfactory.

8. Determine how the ODFI or RDFI manages its relationship with technology service providers. Determine whether:

- The service provider's financial information is obtained and satisfactorily analyzed.
- Service-level agreements are established and monitored.

9. Determine whether the ODFI allows technology service providers direct access to an ACH operator. Consider whether agreements between the ODFI and the service providers include:

- A requirement that the service provider obtain the prior approval of the ODFI before originating ACH transactions for originators under the ODFI routing number.
- The establishment by the ODFI of dollar limits for files that the service provider deposits with the ACH operator.
- A provision that restricts the service provider's ability to initiate corrections to files that have already been transmitted to the ACH operator.
- Provisions regarding warranty and liability responsibilities.
- Appropriate handling of files (physical and logical access controls).

10. Determine whether the RDFI has established procedures to deal with consumers' notifications regarding unauthorized or improperly originated entries or entries where authorization was revoked.

11. Determine whether the RDFI acts promptly on consumers' stop-payment orders.

12. Determine whether the RDFI has procedures that enable it to freeze proceeds of ACH transactions in favor of blocked parties (under OFAC sanctions) for whom the RDFI holds an account.

13. Determine whether the financial institution considers the volume of its uncollected ACH transactions as part of its liquidity risk management practices.

14. Determine whether management and personnel display adequate knowledge and technical skills in managing and performing duties related to ACH transactions.

15. Review results from the financial institution's NACHA rule compliance audit. Determine:

- The independence and competence of the party performing the audit.
- Whether the board or its committee reviewed and approved the audit.
- Whether responsibilities for high-risk entries, such as WEB, were included in the scope.
- Whether corrective actions on audit exceptions are satisfactory.

I. ACH Accounting and Transaction Processing

1. Assess the adequacy of logs maintained for ACH payments received from, and delivered to, each customer.

2. Assess the adequacy of the balancing procedures used for all ACH payments received and whether they include balancing to the aggregate payments sent to an ACH operator.

3. Determine whether the institution balances all payments received from an ACH operator to the aggregate of payments delivered to customers.
4. Determine whether the institution verifies and authorizes the source of all ACH files received for processing.
5. Determine whether the institution reconciles all general ledger accounts related to ACH activities on a timely basis.
6. Determine whether ACH supervisory personnel perform reconciliation and regularly review exception items.
7. Determine whether the institution reconciles the ACH activity and pending file totals daily with the ACH operator.
8. Assess the effectiveness of the reconciliation with third-party service providers preparing ACH transaction files and ensure daily reconciliation.
9. Assess the effectiveness of ACH holdover transactions and determine whether the institution adequately controls them.
10. Determine whether accounting staff reconciles individual outgoing ACH batches before merging them with other ACH transactions.
11. Determine whether there are separate accounts to control holdovers, adjustments, return items, rejects, etc. and whether they are periodically reconciled.
12. Assess the effectiveness of the investigation unit to address customer inquiries and control return items, rejected/unposted items, differences, etc. Determine whether the unit periodically generates aging reports of outstanding items for management.
13. Assess whether management adequately tracks exceptions to credit limit policies and legal contracts.
14. Determine whether exception reports (e.g., rejects, return items, and aging of open items) receive appropriate management attention.
15. Assess the adequacy of separation of duties throughout the ACH process including origination, data entry, adjustments, internal reconciliation, preparing general ledger entries, posting to customer accounts, investigations, and reconciliation with ACH operators.
16. Determine whether adjustments (e.g., added payments, stop payments, reroutes, and reversals) to original ACH instructions are received in an area that does not have access to the original data files.
17. Assess whether controls are appropriate for the adjustment process, including authorization (e.g., signature verification and callbacks on telephone instructions) and whether the institution maintains adequate records (e.g., logs and taping of telephone calls) of individuals making requests.
18. Determine the adequacy of the customer profile origination and change request process. Consider whether requests:

- Are in writing or equivalent confirmation for online activities.
- Identify the originating personnel.
- Document supervisory approval.
- Are verified by staff unable to make changes.

J. ACH Funding and Credit

1. Assess the adequacy of the process for releasing payments to an ACH operator, and determine whether assurances are obtained that sufficient collected funds (e.g., on deposit or prefunded) or credit facilities are available. The institution should monitor customer intraday and interday positions based on defined thresholds.
2. For third-party service providers contracted to process outgoing ACH transactions, determine whether there are procedures to monitor ACH activity and ensure that funds are collected (collected balances, prefunding, credit lines) before the institution settles with the ACH operator.
3. For prefunding arrangements in place for customers without credit lines, determine whether management blocks funds (held for disposition) or maintains them in separate accounts until the transaction date.
4. For non prefunded arrangements determine whether the institution places blocks on outgoing payments to deposit accounts, applies them as reductions to credit lines, or includes them in the overall funds transfer monitoring process.
5. Determine whether management approves payments resulting in extensions of credit lines or drawings against uncollected funds and retains documentation to support the approvals. Determine whether the institution performs credit assessments of customers originating large dollar volumes of ACH credit transactions. Credit assessments should also be reviewed periodically to evaluate creditworthiness of the customer and current economic conditions.
6. Determine whether management treats ACH debits deposited as uncollected funds and whether they monitor any draws against these funds for debits originated by high-risk customers.
7. Determine whether management approves draws against uncollected ACH deposits and maintains documentation to support approvals for debits originated by high-risk customers.
8. Determine the adequacy of Internet and telephone ACH transaction processing procedures and determine whether there are appropriate authentication controls and procedures to ensure the proper identities of parties invoking ACH transactions.
9. Assess the adequacy of management's risk assessment of ACH services in terms of the importance of this function to the overall corporate treasury services function.
10. Ensure that the financial institution obtains and analyzes all audits conducted by the ACH service provider, pursuant to the NACHA rule compliance audit requirement.

K. Web and Telephone-Initiated ACH Transactions

1. Determine whether the financial institution has adopted adequate policies and procedures regarding ACH transactions involving Internet-initiated (WEB) entries. Determine whether they:

- Are in writing and approved by the board or a designated committee.
- Adequately address ODFI or RDFI responsibilities.
- Establish management accountability.
- Include a process to monitor policy compliance.
- Include a mechanism for periodic reviews and updates.

2. Determine whether the ODFI has implemented telephone-initiated (TEL) ACH entries. Determine whether:

- There are significant return rates for these transactions.
- The institution adheres to NACHA guidelines concerning merchant management and their business practices.
- Written agreements are in place with all originators submitting TEL transactions, and include adequate consumer (receiver) authentication and authorization.
- The institution makes tape recordings of all consumer oral authorizations.
- The institution provides written notice to the consumer, prior to settlement date for the TEL entry, confirming the terms of the oral authorization.

3. Determine whether the ODFI requires its originator to employ a commercially reasonable method to authenticate the consumer/business. Determine whether:

- Documentation of the method is adequate.
- The frequency of the review of commercially reasonable standards is sufficient.

4. Determine whether the ODFI conducts risk assessments of its originators and whether they reflect a reasonable exercise of business judgment. Consider whether the risk assessment includes evaluations of:

- Receiver authorizations.
- Originator's Internet security capability, including;
 - Commercially reasonable fraudulent transaction detection systems and routing number verification,
 - Secure customer Internet sessions, and
 - Annual (or more frequent) security audits based on risk.
 - Frequency of risk assessments.
 - Documentation and approval standards.

L. ACH Contingency Plans

1. Evaluate the adequacy of the ACH contingency plan; determine whether the financial institution has tested it and whether it includes provisions for partial or complete failure of the system or communication lines between the institution, ACH operators, customers, and associated data centers.
2. Based on the volume and importance of ACH activity, evaluate whether the plan is reasonable and whether it provides for a reasonable recovery period.
3. Determine whether the institution duplicates or retains transaction files for input reconstruction for a minimum of 24 hours. Note that NACHA rules require the retention of all entries, including return and adjustment entries, transmitted to and received from the ACH for a period of six years after the date of transmittal.
4. Determine whether data and program files are adequately secured, retained, and backed up at off-premises facilities, including secured transport mechanisms for those resources.
5. Determine whether the center has established and tested procedures to recover and restore data under various contingency scenarios.
6. Determine whether the frequency and methods of testing contingency plans are adequate.

M. Check 21

(A more comprehensive set of examination procedures that are designed to test transactions can be found at the FFIEC Check 21 InfoBase at www.ffiec.gov/exam/check21/default.htm.)

1. Determine whether:
 - The institution manages check return items effectively and whether there are significant numbers of return items.
 - The institution records source-document images for recovery if the originals are lost

in transit.

- The institution reconciles batch-dollar totals after processing.
- Reject items are properly segregated from other work.
- Exception items are controlled and tracked adequately.
- Item processing duties are segregated appropriately.

2. If a financial institution has begun to image checks or retrieve imaged checks pursuant to Check 21, determine whether the institution has the following:

- Consumer awareness program.
- Customer service - training and education process.
- Procedures for expedited re-credit.
- Procedures to qualify returns of substitute checks.
- Procedures to identify duplicate checks.
- Procedures for statement preparation and processing.
- Procedures for item repair.
- Procedures for managing corporate customers wanting to submit substitute checks.

3. If the financial institution is a reconverting institution pursuant to Check 21, determine whether it has the following:

- Procedures to identify, measure, and monitor fraud risk.
- Security features for substitute checks.
- Procedures for retention and retrieval of original items.
- Procedures for identifying/controlling duplicate checks.
- Procedures or processes to control substitute check shrinkage.
- Procedures and processes to manage quality.
- Procedures and processes to manage endorsements (includes electronic).
- Procedures and processes to manage re-presentments.
- Procedures to ensure full MICR line is on all substitute checks.

- Procedures and processes to control cash letters.

4. If the financial institution accepts RCCs from retail business customers or payment processing customers, assess the appropriateness of, and adherence to, policies and procedures regarding customer due diligence, customer contracts, third-party service provider's due diligence, and activity/transaction monitoring. Consider the following elements relative to the institution's retail customers, its payment processing customers, and any processors' retail customers:

- Customer due diligence performed at the initiation and periodically throughout the business relationship, including;
 - Assessment of risk exposure associated with the customer's underlying business models;
 - Review of operational history of customer (e.g., length of time in business and relocations of operations);
 - Performance of background checks on customer's principals and/or key operators.
 - Execution of contracts with customers containing provisions addressing;
 - Customer's agreement to operate in accordance with applicable laws and regulations (i.e., FTC Telemarketing Rule, UCC provisions);
 - The parties' responsibilities and warrants under Regulation CC;
 - Customer activity and/or transaction parameters and limits, including expected/allowable unauthorized return levels;
 - Auditing and/or access rights to customers' marketing scripts and consumer authorization/verification files;
 - The financial institution's ability to terminate the business relationship.
 - Routine monitoring and reporting of customer activity and transaction levels, including;
 - The integrity and timeliness of MIS reports on individual and aggregate customer activity/transaction and exposure levels;
 - Established management accountability throughout the business life, including an established process to report monitoring conclusions and exceptions to executive management;
 - Periodic re-assessment of customer exposure and/or transaction limits in association with customer due diligence and contract reviews;
 - The application of independent quality assurance or internal audit reviews to customer relationships in general and to customer monitoring activities in particular;

- Performance of on-site verification of customer authorization files where warranted.

N. Remote Deposit Capture Risk Management

1. Identify the key elements of the RDC environment.

- Identify the bank staff, customers, and technology service providers (if applicable) involved in the RDC function. Obtain and review reports of RDC volume (number of transactions and dollar ranges) for the financial institution as a whole and for individual customers.
- Obtain and review the topology of the financial institution's network, and determine the components involved in the RDC process. Identify the network interfaces with customers using RDC and the technology controls in place.
- Obtain and review the financial institution's data flow or process flow diagram, including relationships with any third-party service providers (if applicable) and the relationships with RDC customers. Identify when the diagram was last updated, and assess whether it is consistent with the system currently implemented.
- Identify whether the RDC system has the following features or functionality:
 - Duplicate item detection.
 - Scanner options (simplex/duplex, MICR/OCR, franking/spraying, CAR/LAR, etc.).
 - Interoperability with existing systems and/or ancillary applications (e.g., QuickBooks).
 - MIS and reporting (audit logs, activity reports).
 - Image quality.
 - Ability to change routing number, account number, and amount.
 - Least-cost routing functionality (conversion into different payment stream).
 - ABA validations (to identify deposits drawn on US versus foreign financial institution).
 - Ability to integrate with BSA/AML systems and processes.
 - Ability to integrate with OFAC systems.
 - Integration with enterprise-wide BCP.
 - Information security (authentication, access controls, encryption, etc.).

2. Assess the RDC strategic planning and the risk assessment process.

- Obtain and review the financial institution's strategic plan for the implementation of RDC.
- Review board or board committee minutes involving discussion and approval of RDC implementation. Note the date of approval.
- Summarize the key objectives of the strategic plan, including:
 - The rationale for offering RDC (e.g., maintaining existing customers or attracting new customers; maintaining existing geographic footprint or penetrating new market/geographic area; wholesale only [merchant/commercial] or retail [consumer]).
 - The type of RDC to be offered (e.g., thick vs. thin client) or if multiple types will be offered to a single client.
 - The use of technology service providers.
 - Other key objectives.
 - Describe the risk assessment process. Identify the financial institution's participants (e.g., representation from such functions as credit, IT, compliance, deposit operations, internal audit, and legal).
 - Obtain and review the most recent risk assessment related to RDC. Evaluate the quality of the risk assessment and whether it encompasses factors such as:
 - Scope of product implementation.
 - Type of customer (e.g., commercial, retail, foreign correspondent).
 - Type of cash letter instrument and the geographic location of the originator.
 - Financial institution position in payment process and settlement channels used (bank of first deposit vs. nonbank of first deposit).
 - Current and anticipated volume of RDC transactions (number and dollar amounts of transactions).
 - Customer role and responsibility in the RDC process.
 - Customer ability to download and retain nonpublic information (NPI).
 - Financial institution's approved technology service providers and equipment.
 - Clearing and settlement channels: image exchange, ACH, or both.
 - Ability to integrate RDC into:
 - Anti-money laundering systems and processes.
 - BCP.

- Information security planning.
- Staffing and customer support.
- Determine whether the RDC risk assessment is updated on a periodic basis as technology, market, customer base, industry, or processes change. Identify the date of the last risk assessment or update.

3. Customer due diligence and suitability.

- Describe the process, the financial institution staff involved, and the decision criteria the financial institution uses to conduct a due diligence review to qualify potential customers for the RDC delivery system. Consider the following:
 - The function and level of the financial institution's staff who conduct the due diligence, and those who have the authority to approve a customer for RDC;
 - How the financial institution risk rates existing customers, on a recurring basis, and how they qualify potential customers;
 - The information the financial institution reviews for potential customers such as:
 - Customer application.
 - Financial analysis.
 - Years in business (for commercial customers).
 - Loan/deposit history.
 - Credit score.
 - Business practices.
 - Sufficiency of staff.
 - Compliance with PCI standards (when appropriate).
 - Publicly available reports for customers that are companies (e.g., Dun & Bradstreet).
 - Visa/MasterCard terminated merchant file or ChexSystems reports, when appropriate to the customer
 - Whether the financial institution has procedures that address customer identification as explained in the BSA/AML manual.
 - Whether the financial institution has procedures to address foreign correspondent relationships and international cash letter pouch activity as explained in the BSA/AML manual.
 - Describe the process and criteria used by financial institution management to

evaluate the RDC customers' information security infrastructure and risk management processes.

4. Vendor Management

- Where technology service providers are used, determine whether RDC is included in the institution's vendor management program.
- Describe any service-level agreements between the financial institution and its service providers, and determine whether management of these relationships conforms to the Outsourcing Technology Services booklet.
- Determine whether any of the financial institution's RDC customers use a service provider in the RDC process. If so, evaluate how the financial institution manages risks, and whether the process is adequate.

5. Contracts and Agreements

- Determine whether legal counsel was involved in drafting any RDC-related contracts or agreements with technology service providers or customers.
- Obtain and review a sample contract or agreement between the financial institution and the RDC customer and technology service provider, where applicable. Consider whether contracts or agreements address the following:
 - Governing laws, regulations, guidelines, payment system rules, and other operational considerations relevant to traditional deposit processing.
 - Roles, responsibilities, and performance standards of the parties, including those related to the sale or lease of equipment needed for RDC at the customer location.
 - Liabilities, warranties, and indemnifications of all parties.
 - Types of items that may be transmitted.
 - Processes and procedures that the customer must follow (e.g., image quality).
 - Funds availability, collateral, collected funds, and reject/return requirements.
 - System maintenance and administration guidelines (e.g., change control and logical access administration).
 - Dispute resolution.
 - Information security requirements and procedures.
 - Security incident reporting.

- Customer service and technical support.
- Responsibility for network connectivity.
- Establishment of controls, such as deposit limits, overdraft limits, and payment on uncollected funds.
- Retention requirements and physical and logical security over deposit items and electronic files at the RDC customer location.
- Business continuity planning requirements, including the back-up of data and periodic testing of such plans.
- Limiting high-risk customers to one account for RDC.
- Authority of the financial institution to mandate specific internal controls at the customer's location(s); audits of customer operations; and requests for additional customer information, as necessary.
- Authority of the financial institution to terminate the RDC relationship.

6. Insurance

- Determine whether financial institution management assessed the availability, coverage, and suitability of insurance related to RDC. If coverage has been obtained, describe.

7. Physical and Logical Access Controls

- Describe how financial institution management ensures that appropriate physical security controls exist at the RDC customer location, such as:
 - Building security.
 - Check storage.
 - Ensuring appropriate controls over portable RDC-related equipment, such as computers and scanner equipment and software.
 - Transport mechanisms for moving data to off-site storage locations.
- Describe how financial institution management ensures that appropriate logical security controls exist at the RDC customer location, such as:
 - Encrypted data transmission and storage.
 - Multifactor or other strong authentication.
 - Access level controls.

- Password security parameters.
- Equipment enrollment.

8. Separation of Duties

- Describe how financial institution management has established appropriate separation of duties for the system administration and security monitoring functions. For example, does one person assign users or rights and another review the activity reports?
- Describe how the financial institution and its RDC customers have implemented appropriate separation of duties controls over the remote capture and transmission process.
- Determine whether the financial institution performs any data entry functions (e.g., adjusting dollar amounts), and whether there is an independent review or reconciliation.
- Determine whether the financial institution requires separation of duties at the RDC customer location and how it monitors for compliance. If separation of duties is not mandatory or possible, describe any required compensating controls required at the RDC customer location.

9. Oversight and Monitoring

- Obtain and review the financial institution's policies and procedures for RDC. Assess whether they define the function, responsibilities, operational controls, vendor management, customer due diligence, BSA/AML compliance monitoring, and reporting functions, etc. Identify the date they were last reviewed and approved by the board or a board committee.
- Identify the financial institution staff members who perform periodic monitoring of RDC customer activity and describe the process used.
- Determine the frequency and process for management review of logical and physical access privileges and audit trails/logs.
- Identify and describe the monitoring reports used by the financial institution to manage risk. Obtain copies of reports used and review the monitoring process with appropriate financial institution staff. Discuss with appropriate financial institution staff the internal processes for responding to established threshold breaches and any escalation process. Examples include:
 - Duplicate Presentment Report (to detect duplicate batches prior to submission);
 - Daily Batch Totals Report;

- Velocity Exception Report (to detect merchant spikes in volume or exceeding approved dollar limits);
- Large Item Report (exception report to detect whether transactions are outside of normal parameters); and,
- Customer Activity Report (detailed log of activity by merchant, including batch delivery date, time, value, receipt acknowledgement, and merchant operator ID).
- Identify and describe the RDC customer risk management reports recommended by financial institution management. Discuss how financial institution management validates that RDC customers review the reports. Examples include:
 - Pending Batch Report (items queued for processing for reasonableness and timeliness reviews);
 - Batch Total Report (allows the merchant to reconcile processed RDC work to the batch prepped for submission to the FI);
 - Return Item Report (alerts management to operational deficiencies, e.g., poor image quality);
 - Duplicate Presentment Report (to detect duplicate batches prior to submissions); and,
 - FI Reports (report would provide list of received imaged items).
- Select a sample of RDC customers and review the nature of account activity relative to the business type.

10. Training

- Determine whether financial institution management has established a training program to ensure that all parties involved are trained appropriately. If yes, describe the training programs for financial institution and customer staff.
- Determine whether the financial institution provides or plans to provide customer technical service or support to the RDC customers. If yes, discuss whether the financial institution considered the need for, or has added, additional staff.
- Determine whether the financial institution provides the merchant/consumer customers with a procedural or instructional document and a user guide for the application/scanner.

11. Change Management

- Determine whether the financial institution has enhanced its change management program to address the procedures involved in the RDC function and ensure ongoing compatibility between financial institution and customer systems. Describe the coordination process.
- If the financial institution maintains the application in-house, describe how it ensures that all relevant operating system and application patches are up-to-date.
- Describe how financial institution management ensures that RDC customers implement an effective change management program to maintain updated and patched network and desktop operating systems, RDC application, anti-virus, etc.

12. Records Management

Assess the process by which financial institution management verifies customer compliance with contract requirements related to the secure retention, storage, and destruction requirements for physical deposit items and electronic files.

13. Business Continuity Planning (BCP)

- Determine whether the financial institution's BCP has been updated to address:
 - The financial institution's relationship with the RDC service provider and BCP assurance.
 - The financial institution's relationship with the RDC customer.
 - Determine whether the financial institution's BCP testing activities include:
 - RDC systems and processes.
 - RDC customers.
 - Technology service providers, where appropriate.

14. Fraud

- Describe how financial institution management monitors for fraud associated with RDC.
- Describe how the financial institution attempts to mitigate fraud risks (e.g., duplicate check detection, establishing deposit limits, safeguarding checks).
- Describe how the financial institution monitors items that originated in foreign countries (i.e., foreign locations owned or controlled by customers of the financial institution or items received and processed by correspondent banks).

O. Vendor Management

Assess the adequacy of vendor management program over a service provider that provides a new and emerging retail payment technology. (Select one or more projects involving the development and deployment of a new and emerging retail payment technology and complete the following procedures.)

1. Review documentation supporting the business case for the application

- Scope and nature;
- Standards for controls;
- Minimum acceptable service provider characteristics;
- Monitoring and reporting;
- Transition requirements;
- Contract duration, termination, and assignment; and
- Contractual protections against liability.

2. Assess the extent to which the institution

- Reviews the financial stability of the technology service provider;
- Analyzes the service provider's audited financial statements and annual reports;
- Assesses the service provider's length of operation and market share;
- Considers the size of the institution's contract in relation to the size of the service provider;
- Reviews the service provider's level of technological expenditures to ensure on-going support; and
- Assesses the impact of economic, political, or environmental risk on the service provider's financial stability.

3. Evaluate whether the institution's due diligence considers the following:

- References from current users or user groups about a particular technology service provider's service and performance;
- The service provider's experience and ability in the industry;

- The service provider's experience and ability in dealing with situations similar to the institution's environment and operations;
- The cost for additional system and data conversions or interfaces presented by the various technology service providers;
- Shortcomings in the service provider's expertise that the institution would need to supplement in order to fully mitigate risks;
- The service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities;
- The service provider's ability to respond to service disruptions;
- Key service provider personnel that would be assigned to support the financial institution;
- The service provider's ability to comply with appropriate federal and state laws. In particular, ensure management has assessed the service providers' ability to comply with federal laws (including GLBA and BSA); and
- Country, state, or local risk.

4. Verify that the contract appropriately addresses:

- Scope of services;
- Performance standards;
- Pricing;
- Controls;
- Financial and control reporting;
- Right to audit;
- Ownership of data and programs;
- Confidentiality and security;
- Regulatory compliance;
- Indemnification;
- Limitation of liability;
- Dispute resolution;
- Contract duration;
- Restrictions on, or prior approval for, subcontractors;

- Termination and assignment, including timely return of data in a machine-readable format;
- Insurance coverage;
- Prevailing jurisdiction (where applicable);
- Choice of Law (foreign outsourcing arrangements);
- Regulatory access to data and information necessary for supervision; and
- Business Continuity Planning.

5. Review service level agreements to ensure they are adequate and measurable. Determine whether:

- Significant elements of the service are identified and based on the institution's requirements;
- Objective measurements for each significant element are defined;
- Reporting of measurements is required;
- Measurements specify what constitutes inadequate performance; and
- Inadequate performance is met with appropriate sanctions, such as reduction in contract fees or contract termination.

6. Evaluate the institution's periodic monitoring of the service provider relationship(s), including:

- Timeliness of review, given the risk from the relationship;
- Changes in the risk due to the function outsourced;
- Changing circumstances at the service provider, including financial and control environment changes;
- Conformance with the contract, including the service level agreement; and
- Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship.

Appendix B: Glossary

Access point: Methods of connection that include a user's home network, cellular network, NFC, Bluetooth, or public Wi-Fi connections, such as those provided by a municipality or business.

Application security: The use of software, hardware, and procedural methods to protect applications from external threats.

Application store: A type of digital distribution platform for computer software, often in a mobile context.

Biometric: The measuring and analysis of such physical attributes as facial features and voice or retinal scans. This technology can be used to define an individual's unique identity, often for security purposes.

CHIPS: A private-sector U.S.-dollar funds transfer system, clearing and settling cross-border and domestic payments.

Code analysis: Use of tools to analyze source code and/or compiled version of code in order to help find security flaws.

Cross-site scripting: A type of computer security vulnerability typically found in web applications that enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting (XSS) vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Anti-XSS features help protect applications from cross-site scripting attacks.

Data security: The process of safeguarding important information from unauthorized access, corruption, or loss.

Data transmission security: The transfer of confidential or proprietary information over a secure channel.

Debit card: A payment card issued as either a PIN-based debit (ATM) card or as a signature-based debit card from one of the bankcard associations. A payment card issued to a person for purchasing goods and services through an electronic transfer of funds from a demand deposit account rather than using cash, checks, or drafts at the point-of-sale.

Debit entry: An entry to the record of an account to represent the transfer or removal of funds from the account.

Deferred net settlement: See "National Settlement Service".

Depository: An institution that holds funds or marketable securities for safekeeping.

Depositories may be privately or publicly operated and allow securities transfers through book-entry and offer funds accounts permitting funds transfers as a means of payment.

Depository bank (Check 21): Also known as Bank of First Deposit (BOFD). The first bank to which a check is transferred even though it is also the paying bank or the payee. A check deposited in an account is deemed to be transferred to the financial institution holding the account into which the check is deposited, even though the check is physically received and endorsed first by another financial institution.

Device fingerprinting: Information collected about a remote computing device for the purpose of identification.

Direct debit: Electronic transfer, usually through ACH, out of an individual's checking (or savings) account to pay bills, such as mortgage payments, insurance premiums, and utility payments. Also referred to as "direct payment."

Direct deposit: Electronic deposits or credit, usually through ACH, to an individual's deposit account. Common uses of direct deposit include payroll payments, Social Security benefits, and income from investments such as CDs, annuities, and mutual funds.

Direct presentment: Depository banks can present checks directly to the paying institution. The paying institution may be the depository bank (no settlement is needed), or, if not, may settle on the books of the Federal Reserve, using the Federal Reserve's national settlement service.

Electronic Benefits Transfer (EBT): A type of EFT system involving the transfer of public entitlement payments, such as welfare or food stamps, through direct deposit or point-of-sale technology (see POS). The recipient can be given an identification card, similar to a benefit card, and a PIN allowing access to the benefits through an electronic network.

Electronic bill presentment and payment (EBPP): An electronic alternative to traditional bill payment, allowing a merchant or utility to present its customers with an electronic bill and the payer to pay the bill electronically. EBPP systems usually fall within two models: direct and consolidation-aggregation. In the direct model, the merchant or utility generates an electronic version of the consumer's billing information, and notifies the consumer of a pending bill, generally via e-mail. The consumer can initiate payment of the electronically presented bill using a variety of payment mechanisms, typically a credit card. In the consolidation-aggregation model, the consumer's bills are consolidated by a consolidator acting on behalf of merchants and utilities (or aggregated on behalf of the consumer), combining data from multiple bills and presenting a single source for the consumer to initiate payment. Some consolidators present bills at their own web sites, typically most support the aggregation of bills by consumer service providers such as Internet portals, financial institutions, and brokerage web sites.

Electronic check conversion: The process by which a check is used as a source of information for the check number, the customer's account number, and the number that identifies the financial institution. The information is used to make a one-time electronic payment from the customer's account -- an electronic fund transfer. The check itself is not the method of payment.

Electronic check presentment (ECP): Check truncation methodology in which the paper check's MICR line information is captured and stored electronically for presentment. The physical checks may or may not be presented after the electronic files are delivered, depending on the type of ECP service that is used.

Electronic commerce (E-Commerce): A broad term encompassing the remote procurement and payment by businesses or consumers of goods and services through electronic systems such as the Internet.

Electronic data capture (EDC): Process used for capturing and transferring the encoded information on the magnetic strip from a bankcard or debit card at the point-of-sale to the processor's database.

Electronic funds transfer (EFT): A generic term describing any transfer of funds between parties or depository institutions through electronic data systems.

Electronically-created payment orders: These are payment orders received by merchants from consumers, typically by telephone or the Internet. These payment orders are processed through the check processing system although they were not initiated as paper checks. These payment orders are not subject to check law and are not warranted by the Federal Reserve Banks.

Encryption: A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

Expedited Funds Availability Act (EFAA): See "Regulation CC".

Federal Reserve Banks: The Federal Reserve Banks provide a variety of financial services including retail and wholesale payments. The Federal Reserve Bank operates a nationwide system for clearing and settling checks drawn on depository institutions located in all regions of the United States.

Fedwire®: The Federal Reserve Bank's nationwide real time gross settlement electronic funds and securities transfer network. Fedwire® is a credit transfer system. Each funds transfer is settled individually against an institution's reserve or clearing account on the books of the Federal Reserve. The transaction is considered an irrevocable payment as it is processed.

Finality: Irrevocable and unconditional transfer of payment during settlement.

Financial EDI (FEDI): Financial electronic data interchange. An instrument for settling invoices by initiating payments, processing remittance data and automating reconciliation, through the exchange of electronic messages.

Firewall: A hardware or software link in a network that relays only data packets clearly intended and authorized to reach the other side.

Firmware: A software program or set of instructions programmed on a hardware device.

Float: Funds held by an institution during the check-clearing process before being made available to a depositor. Interest may be earned on these funds.

Geolocation: The identification of the real-world geographic location of an object, such as a radar source, mobile phone or Internet-connected computer terminal.

Image archive (Check 21): Database for storage and easy retrieval of check images.

Image capture (Check 21): The process of digitizing both sides of physical items and their assorted MICR information as they are processed at the Federal Reserve Bank. Also includes storage of the images for up to 60 days.

Image exchange (Check 21): Exchange of some or all of the digitized images of a check.

Indemnifying bank (Check 21): A financial institution that transfers, presents, or returns a substitute check or a paper or electronic representation of a substitute check for which it receives consideration. The financial institution shall indemnify the recipient and any subsequent recipient (including a collecting or returning financial institution, the depository financial institution, the drawer, the drawee, the payee, the depositor, and any endorser) for any loss incurred by any recipient of a substitute check if that loss occurred due to the receipt of a substitute check instead of the original.

Interbank checks: Checks that are not “on-us.” They are cleared and settled either by direct presentment, a clearinghouse association, a correspondent bank, or a Federal Reserve Bank.

Interchange: Exchange of transactions between financial institutions participating in a bank card network, based on a common set of rules. Card interchange allows a financial institution’s customers to use a bank credit card at any card honoring merchant and to gain access to multiple ATM systems from a single ATM.

Interchange (fees): Fees paid by one financial institution to another to cover handling costs and credit risk in a financial institution card transaction. Interchange fees generally flow toward the institution funding the transaction and assuming the risk. In a credit card transaction, the interchange fee is paid by the merchant acquirer accepting the merchant’s sales draft to the card-issuing institution, which, in turn, passes the fee to its merchants. In EFT/POS transactions, interchange flows in the opposite direction: the card-issuing institution (or customer) pays the fee to the terminal-owning institution. When a transaction is an off-line debit sale, the card-issuing institution collects an interchange fee from the merchant, rather than from the customer, unlike in an EFT/POS transaction, where the customer pays the interchange fee. Interchange revenue is derived from fees set by the card associations. Depending on the card association, fees can range from 1% to 3% of the value of the transaction. Interchange revenue is recognized as a card issuer’s second largest revenue line item.

Internet: A worldwide network of computer networks, governed by standards and protocols

developed by the Internet Engineering Task Force (IETF).

Jailbreaking: A method of removing the manufacturer's device controls or core operating system controls to provide a user with additional access to and control over the device's operating and file systems, including the ability to circumvent security controls.

Large value funds transfer system: A wholesale payment system used primarily by financial institutions in which large values of funds are transferred between parties. Fedwire® and CHIPS are the two large-value transfer systems in the United States.

Lockbox: Deposit mechanism used by commercial firms and businesses to facilitate their deposit transaction volume. Typically, commercial firms and businesses direct customers to send payments directly to a financial institution address or post office box controlled by the institution. Financial institution personnel record payments received and prepare deposit slips, and subsequent processing proceeds as with other deposit taking activities.

Merchant acquirer: Bankcard association members that initiate and maintain contractual agreements with merchants for the purpose of accepting and processing bankcard transactions.

Merchant processing: Activity for the acceptance and settlement of bankcard products and transactions from merchants through the payment system.

Mobile application: Downloadable software applications developed specifically for use on mobile devices. Mobile financial applications are developed by or for financial institutions to allow customers to perform account inquiries, retrieve information, or initiate financial transactions.

Mobile device: A portable computing and communications device with information-storage capability.

Mobile device security: Controls to protect unauthorized access to or activities through portable computing and communications devices.

Mobile financial services: The products and services that a financial institution provides to its customers through mobile devices.

Mobile P2P: Payments initiated on a mobile device using the recipient's mobile phone number, e-mail address, or other identifier.

Mobile payment: A transfer of value via a mobile device.

Mobile wallet: A front-end application that stores payment card information on the mobile device and allows payments to be made using a mobile device. The mobile wallet utilizes traditional retail payment channels such as ACH, EFT, and debit/credit card networks to process the payments.

Mobile-enabled Web sites: A Web site is designed to detect the type of device the customer is using (e.g., mobile device or desktop computer) and displays Web pages in the best format

for that device.

Multilateral netting settlement system: Multilateral netting is an arrangement among three or more parties to net their obligations. In these settlement systems transfers are irrevocable but are only final after the completion of end-of-day-settlement.

NACHA: The Electronic Payments Association (NACHA) - The national association that establishes the rules and procedures governing the exchange of ACH payments.

National Settlement Service (NSS): Also referred to as Deferred Net Settlement. The Federal Reserve Banks' multilateral settlement service. NSS is offered to depository institutions that settle for participants in clearinghouses, financial exchanges, and other clearing and settlement groups. Settlement agents acting on behalf of those depository institutions electronically submit settlement files to the Federal Reserve Banks. Files are processed on receipt, and entries are automatically posted to the depository institutions' Reserve Bank accounts. Entries are final when posted.

Near field communication (NFC): A wireless protocol that allows for exchange of payment credentials stored on the mobile device and other data at close range.

Net debit cap: The maximum dollar amount of uncollateralized daylight overdrafts that an institution is authorized to incur in its Federal Reserve account. The net debit cap is generally equal to an institution's capital times the cap multiple for its cap category.

Office of Foreign Asset Control (OFAC): The Office of Foreign Assets Control, United States Department of the Treasury, administers and enforces economic sanctions programs primarily against countries and groups of individuals such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

One-time password: A password that is valid for only one login session or transaction on a computer system or other digital device.

On-us checks: Checks that are deposited into the same institution on which they are drawn.

Originating depository financial institution (ODFI): A participating financial institution that originates entries at the request of and by agreement with its originators in accordance with the provisions of the NACHA rules.

OWASP: An online community dedicated to Web application security.

Paying bank: A paying bank is the institution where a check is payable and to which it is sent for payment.

Payment: A transfer of value.

Payment system: The mechanism, the rules, institutions, people, markets, and agreements that make the exchange of payments possible.

Payments System Risk Policy (PSR): The Federal Reserve's Payments System Risk (PSR) policy addressing the risks that payment systems present to the Federal Reserve Banks, the banking system, and to other sectors of the economy.

Payroll card account: A bank account that is established directly or indirectly by an employer on behalf of an employee to which an electronic funds transfers the employee's wages or compensation on a recurring basis. The payroll card, often branded by one of the credit/debit card associations, provides the employee access to the funds.

Person-to-person (P2P) payment: Online payments using electronic mail messages to invoke a transfer of value between the parties over existing proprietary networks as on-us transactions.

Point-of-sale (POS) network: A network of institutions, debit cardholders, and merchants that permit consumers to make direct payment electronically at the place of purchase. The funds are withdrawn from the account of the cardholder.

Presentment fee: A fee that an institution receiving a check may impose on the institution that presents the check for payment. No presentment fee may be charged for checks presented by 8 a.m. local time.

Private label card: See "Store Card".

QR code: A type of two-dimensional bar code or machine-readable optical label that contains information about the item to which it is attached.

Real time gross settlement (RTGS) System: A type of payments system operating in real time rather than batch processing mode. It provides immediate finality of transactions. Gross settlement refers to the settlement of each transfer individually rather than netting. Fedwire® is an example of a real time gross settlement system.

Receiver: An individual, corporation, or other entity that has authorized a company or an originator to initiate a credit or debit entry to a transaction account belonging to the receiver held at its RDFI.

Receiving depository financial institution (RDFI): Any financial institution qualified to receive debits or credits through its ACH operator in accordance with the ACH rules.

Reconverting bank (Check 21): The financial institution that creates a substitute check. With respect to a substitute check that was created by a person that is not a financial institution, the reconverting bank is the first financial institution that transfers, presents, or returns that substitute check or, in lieu thereof, the first paper or electronic representation of that substitute check. The reconverting bank warrants that (1) the substitute check is the legal equivalent of the original check; and (2) the original check cannot be presented again in any form so the customer pays the check only once.

Regulation CC: A regulation (12 CFR 229) promulgated by the Board of Governors of the Federal Reserve System regarding the availability of funds and the collection of checks. The regulation governs the availability of funds deposited in checking accounts and the collection

and return of checks.

Regulation E: A regulation (12 CFR 205) promulgated by the Board of Governors of the Federal Reserve System to ensure consumers a minimum level of protection in disputes arising from electronic fund transfers.

Regulation Z: Regulation Z, the Truth in Lending Act (TILA) (12 CFR 226) promulgated by the Board of Governors of the Federal Reserve System. The regulation prescribes uniform methods for computing the cost of credit, disclosing credit terms, and resolving errors on certain types of credit accounts.

Remittance cards: Payment cards that are typically used to facilitate cross-border movement of funds by individuals and for person-to-person transactions.

Remote deposit capture (RDC): A service that enables users at remote locations to scan digital images of checks and transmit the captured data to a financial institution or a merchant that is a customer of a financial institution.

Remotely created check (RCC): A check that is drawn on a customer account at a financial institution, is created by the payee, and does not bear a signature in the format agreed to by the paying financial institution and customer. RCCs are also known as “demand drafts,” “telechecks,” “preauthorized drafts,” “paper drafts,” or “digital checks.”

Reserve account: A non-interest-earning balance account institutions maintain with the Federal Reserve Bank or with a correspondent bank to satisfy the Federal Reserve’s reserve requirements. Reserve account balances play a central role in the exchange of funds between depository institutions.

Reserve requirements: The percentage of deposits that a depository institution may not lend out or invest and must hold either as vault cash or on deposit at a Federal Reserve Bank. Reserve requirements affect the potential of the banking system to create transaction deposits.

Retail payments: Payments, typically small, made in the goods and services market.

Return (ACH): Any ACH entry that has been returned to the ODFI by the RDFI or by the ACH operator because it cannot be processed. The reason for each return is included with the return in the form of a “return reason code.” (See the NACHA “Operating Rules and Guidelines” for a complete reason code listing.)

Rogue code: In programming, rogue code is another term for code that constitutes a virus.

Root user: The conventional name of the user who has all rights or permissions to all files and programs. Having such rights or permissions allow the root user to do many things an ordinary user cannot.

Routing number: Also referred to as the ABA number. A nine-digit number (eight digits and a check digit) that identifies a specific financial institution.

Secure coding techniques: The process of developing code (e.g., Web application) with security built in during the development process using technical controls to mitigate the occurrence of software vulnerabilities.

Settlement: The final step in the transfer of ownership involving the physical exchange of securities or payment. In a banking transaction, settlement is the process of recording the debit and credit positions of the parties involved in a transfer of funds. In a financial instrument transaction, settlement includes both the transfer of securities by the seller and the payment by the buyer. Settlements can be “gross” or “net.” Gross settlement means each transaction is settled individually. Net settlement means parties exchanging payments will offset mutual obligations to deliver identical items (e.g., dollars or EUROS), at a specified time, after which only one net amount of each item is exchanged.

Settlement date (ACH): The date on which an exchange of funds with respect to an entry is reflected on the books of the Federal Reserve Bank.

Short message service: A text messaging service component of phone, Web, or mobile communication systems. SMS uses standardized communications protocols to allow devices to exchange short text messages. Also known as text messaging.

Single-Entry (ACH): A one-time transfer of funds initiated by an originator in accordance with the receiver’s authorization for a single ACH credit or debit to the receiver’s consumer account.

Standard Entry Class (SEC) code: Three-character code in an ACH company/batch header record used to identify the payment type within an ACH batch.

Store card: A credit card issued by a financial institution for a specific merchant or vendor that does not carry a bankcard association logo. Store cards can only be used at the merchant or vendor whose name appears on the front of the card.

Stored-value card: A card-based payment system that assigns a value to the card. The card’s value can be stored on the card itself (i.e., on the magnetic stripe or in a computer chip) or in a network database. As the card is used for transactions, the transaction amounts are subtracted from the card’s balance. As the balance approaches zero, some cards can be “reloaded” through various methods and others are designed to be discarded. These cards are often used in closed systems for specific types of purchases.

Substitute check (Check 21): Also known as the Image Replacement Document (IRD). A paper reproduction of an original check that (1) contains an image of the front and back of the original check; (2) bears a MICR line that, except as provided under ANS X9.100-140, contains all the information appearing on the MICR line of the original check when it was issued and any additional information that was encoded on the original check’s MICR line before an image of the original check was captured; (3) conforms in paper stock, dimension, and otherwise with ANS X9.100-140; and (4) is suitable for automated processing in the same manner as the original check. The Federal Reserve Board of Governors can by rule or order determine different standards.

Third-party sender: A special subset of a technology service provider that is authorized to

transmit ACH files on behalf of an originator. Typically, the ODFI must rely upon warranties by the third-party sender regarding the originators' identity and credit worthiness, which places additional risks on the ODFI.

Third-party service provider (TPSP)(For ACH): A third party, other than the ODFI or RDFI, that performs any function on behalf of the ODFI or the RDFI related to ACH processing. These functions would include the creation and sending of ACH files or acting as a sending or receiving point on behalf of a participating depository financial institution.

Threat modeling: A structured approach that enables an institution to aggregate and quantify potential threats. In the context of application development, threat modeling can be used to capture, organize, and analyze all of the threat information of an application and its environment that affects application security. It is used to enable informed decision-making about application security and helps to produce and rank a list of security improvements.

Token: A small device with an embedded computer chip that can be used to store and transmit electronic information. A soft token is a software-based token.

Tokenization: The process of substituting a sensitive data element with a surrogate value, referred to as a token.

Truncating bank (Check 21): The financial institution that truncates the original check. If a person other than a financial institution truncates the original check, the truncating bank is the first financial institution that transfers, presents, or returns, in lieu of such original check, a substitute check or, by agreement with the recipient, information relating to the original check (including data taken from the MICR line of the original check or an electronic image of the original check), whether with or without the subsequent delivery of the original check.

Trusted platform module: An international standard for a secure crypto processor that is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.

USA Patriot Act: The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law Pub.L. 107-56), commonly known as the "Patriot Act", was enacted by Congress to deter and punish terrorist acts in the United States and around the world by enhancing the law enforcement investigatory tools of both domestic law enforcement and foreign intelligence agencies.

Virtual payment card: A controlled way of making payments by generating a unique credit card number to settle a specific transaction typically online. Also referred to as single-use credit cards.

WEB SEC code: An ACH debit entry initiated by an originator resulting from the receiver's authorization through the Internet to make a transfer of funds from a consumer account of the receiver.

White-hat hacking: The specialization of penetration testing and other testing methodologies to review the security of an institution's information systems by determining

flaws and vulnerabilities. Also called ethical hacking.

Whitelist: A list of trusted entities.

Wipe: Removal of data from a device.

Wireless payment technology: The use of different core technologies to exchange payment credentials and authorization between the mobile device and the payment recipient. Examples include: near field communication, image based, carrier-based, mobile P2P, etc.

Appendix C: Schematic of Retail Payments

Access Channels & Payments Method

Retail payments can be categorized within two broad groups according to the access channel and the payment method. The access channel is used at the beginning of the transaction process and provides the user interface (e.g., a plastic card with a magnetic strip). The payment method includes the remaining parts of the payments process governed by applicable laws, regulations, and contracts.

ACCESS CHANNELS AND PAYMENT METHODS

NONCASH PAYMENT METHODS*(transaction, clearing & settlement processes)*

<u>ACCESS CHANNELS</u> <i>(Front End)</i>	ESTABLISHED: Check Credit card ACH debit ACH credit ATM account debit Wire transfers Established C-B relationship	NEW: Prepaid Balance transfer (book entry) Bank line of credit (new relationship)
	ESTABLISHED: Plastic Card Paper Check Telephone	
	NEW COMBINATIONS OF ESTABLISHED COMPONENTS:	
	NEW: Internet Cell phone Check Image MICR Reader Biometric Reader RFID Personal Data	

(well known technologies initiate commonly known types of payments) Credit card payments Paper checks PPD ACH debit PPD ACH credit PIN debit Signature debit	General purpose prepaid cards Payroll cards Closed network and gift Cards
ACH debit card (e.g. Debitman) ACH TEL Micropayment Aggregator (e.g., BitPass, Peppercoin, Yaga, Check 21 Substitute Check)	
(new technologies or networks access established payment method) ACH POP ACH ARC ACH WEB Check image presentment (not IRD) Cell phone payment Highway toll booths Contactless card payments (debit or credit) Charge to phone bill Biometric authentication License ID	Proprietary balance transfer Secured proprietary balance transfer Proprietary balance transfer via cell phone Prepaid wallet Instant credit (e.g., Bill Me Later, e-Charge)

Figure 13

Payment methods that have the fewest changes from established methods are shown in the upper left quadrant above. The lower right quadrant includes emerging payment methods in terms of access channels and payment methods. The remaining two quadrants, upper right and lower left, are hybrids of new and established components. The left side of the matrix shows examples of access channels used to initiate payment

transactions, while the top of the matrix identifies general payment methods. The cells list a sample of the payment types that incorporate these various access and payment-method components. Retail payments may be effected using a variety of electronic networks in addition to the traditional cash and check processes. The electronic networks, which are discussed throughout this handbook, include the Automated Clearing House, card associations such as Visa, or MasterCard, and ATM networks.

Retail payment systems continue to evolve with advances in technology. These advances enable financial institutions to develop new products and services, to lower the barriers to business entry for smaller institutions, and to use "economies of scale."

Appendix D: Laws, Regulations, and Guidance

Laws

- 15 USC 1601: Truth in Lending Act (N/A)
- 12 USC 1861-1867(c): Bank Services Company Act (N/A)
- 12 USC 4001: Expedited Funds Availability Act (N/A)
- 12 USC 5001: Check Clearing for the 21st Century Act (N/A)
- 15 USC 1681m(e): Fair Credit Reporting Act (N/A)
- 15 USC 1693: Electronic Funds Transfer Act (N/A)
- 15 USC 6801 and 6805(b): Gramm-Leach-Bliley Act (N/A)
- 18 USC 1 (Pub. L. No. 107-56): USA Patriot Act (N/A)
- 31 USC 5311: Bank Secrecy Act (N/A)

Federal Financial Institutions Examination Council

- Authentication in an Internet Banking Environment (October 2005)
- Bank Secrecy Act/anti-Money Laundering InfoBase (N/A)
- Check 21 InfoBase (N/A)

Federal Reserve Board

- 12 CFR 210, Subparts A and B (Regulation J) (N/A)
- 12 CFR 205 (Regulation E) (N/A)
- 12 CFR 226, Truth in Lending (Regulation Z) (N/A)
- 12 CFR 229, Subparts A, B, and C (Regulation CC) (N/A)
- SR Letter 09-2: FFIEC Guidance Addressing Risk Management of Remote Deposit Capture Activities (January 14, 2009)
- Board of Governors of the Federal Reserve System Payments System Risk (PSR)

Policy (December 19, 2008)

- SR Letter 07-15: Release of Revised FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (August 24, 2007)
- SR Letter 05-19: Interagency Guidance on Authentication in an Internet Banking Environment (October 13, 2003)
- SR Letter 01-15: Safeguarding Customer Information (June 7, 2001)
- SR Letter 01-11: Identity Theft and Pretext Calling (April 26, 2001)
- SR Letter 00-17: FFIEC Guidance on the Risk Management of Outsourced Technology Services (November 30, 2000)
- SR Letter 00-04: Outsourcing of Information and Transaction Processing (February 29, 2000)
- SR Letter 93-64: Credit Card-related Merchant Activities (December 18, 1993)

Federal Deposit Insurance Corporation

- FIL 4-2009: Risk Management of Remote Deposit Capture (January 14, 2009)
- FIL 129-2008: New General Counsel's Opinion No. 8, Stored Value Cards and Other Nontraditional Access Mechanisms (November 13, 2008)
- FIL 127-2008: Guidance on Payment Processor Relationships (November 7, 2008)
- FIL 44-2008: Guidance on Managing Third-Party Risk (June 6, 2008)
- FIL 32-2007: Identity Theft - FDIC's Supervisory Policy on Identity Theft (April 11, 2007)
- Credit Card Activities Manual (March 2007)
- FFIEC Guidance Authentication in an Internet Banking Environment, FIL 103-2005 (October 2005)
- FIL 7-2005: Fair and Accurate Credit Transactions Act of 2003, Guidelines Requiring the Proper Disposal of Consumer Information (February 2, 2005)
- FIL 116-2004: Check Clearing for the 21st Century Act (October 27, 2004)
- FIL 39-2001: Identity Theft and Pretext Calling (May 9, 2001)
- FIL 79-98: Electronic Financial Services and Consumer Compliance (July 16, 1998)

National Credit Union Administration

- NCUA Letter to Credit Unions, 09-CU-01: Risk Management of Remote Deposit Capture (with Enclosure) (January 2009)
- NCUA Letter to Credit Unions, 07-CU-13: Supervisory Letter - Evaluation Third Party Relationships (December 2007)
- NCUA Corporate Credit Union Guidance Letter 07-04: Accounting for Future-Dated Automated Clearing House (ACH) Transactions (October 2007)
- NCUA Letter to Credit Unions 06-CU-14: Bank Secrecy ACT (BSA)/Anti-Money Laundering (AML) Manual Interagency Outreach (September 2006)
- NCUA Letter to Credit Unions 05-CU-18: Guidance on Authentication in Internet Banking Environment (November 2005)
- NCUA Letter to Credit Unions 05-CU-16: Bank Secrecy Act Compliance (October 2005)
- NCUA Regulatory Alert 05-RA-02: Suspicious Activity Reports on OFAC blocked transactions (January 2005)
- NCUA Regulatory Alert 04-RA-12: Check 21 Act (October 2004)
- NCUA Regulatory Alert 03-RA-07: Final Patriot Act Regulations on Customer (Member) Identification (May 2003)
- NCUA Letter to Credit Unions, 01-CU-09: Identity Theft and Pretext Calling (September 2001)
- NCUA Letter to Credit Unions, 01-CU-11: Electronic Data Security Overview (August 2001)
- NCUA Regulatory Alert 01-RA-08: Interim Final Rules Amending Regulations B, E, M, Z, and DD - Electronic Delivery of Required Disclosures (August 2001)
- NCUA Letter to Credit Unions, 00-CU-11: Risk Management of Outsourced Technology Services (with Enclosure) (December 2000)
- NCUA Regulatory Alert 99-RA-3: Pretext Phone Calling by Account Information Brokers (February 1999)

Office of the Comptroller of the Currency

- Office of the Comptroller of the Currency (OCC) Comptroller's Handbook: Depository Services (November 19, 2008)
- OCC Bulletin 2009-4: Remote Deposit Capture: Interagency Guidance (January 14, 2009)
- OCC Comptroller's Handbook: Truth in Lending (October 6, 2008)
- OCC Bulletin 2008-12: Payment Processors: Risk Management Guidance (April 24,

2008)

- OCC Bulletin 2006-39: Automated Clearing House Activities: Risk Management Guidance (September 1, 2006)
- OCC Bulletin 2006-06: Bank Secrecy Act/Anti-Money Laundering: Joint Statement on Sharing Suspicious Activity Reports with Controlling Companies (January 27, 2006)
- OCC Bulletin 2005-13: Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance (April 14, 2005)
- OCC Advisory Letter 2004-6: Payroll Card Systems (May 14, 2004)
- OCC Bulletin 2003-01: Credit Card Lending, Account Management and Loss Allowance Guidance (January 8, 2003)
- OCC Comptroller's Handbook: Merchant Processing (December 2001)
- OCC Bulletin 2001-47: Third Party Relationships, Risk Management Principles (November 1, 2001)
- OCC Bulletin 2001-6: Expanded Guidance for Subprime Lending Programs (January 31, 2001)
- OCC Advisory Letter 2000-10: Payday Lending (November 27, 2000)
- OCC Advisory Letter 2000-9: Third-Party Risk (August 29, 2000)
- OCC Advisory Letter 2000-6: Audit and Internal Controls (July 23, 2000)
- OCC Bulletin 2000-20: FFIEC Uniform Retail Credit Classification and Account Management Policy (June 22, 2000)
- OCC Bulletin 2000-16: Risk Modeling, Model Validation (May 30, 2000)
- OCC Bulletin 2000-3: FFIEC Consumer Credit Reporting Practices (February 16, 2000)
- OCC Bulletin 99-15: Subprime Lending: Risks and Rewards (April 5, 1999)
- OCC Bulletin 99-10: Interagency Guidance on Subprime Lending (March 5, 1999)
- OCC Bulletin 98-3: Technology Risk Management: Guide for Bankers and Examiners (February 4, 1998)
- OCC Bulletin 97-24: Credit Scoring Models, Examiner Guidance (May 20, 1997)
- OCC Advisory Letter 96-7: Credit Card Pre-Approved Solicitations (September 26, 1996)

Office of Thrift Supervision

- 12 CFR Part 570: Interagency Guidelines Establishing Standards for Safeguarding Customer Information, Appendix B (N/A)
- RB 37-37: Electronic Fund Transfer Act (May 5, 2009)
- CEO Letter 291: Risk Management of Remote Deposit Capture (January 14, 2009)
- CEO Letter 273: Compliance with Truth in Savings and Electronic Transfer Act Rules: Government Accountability Office Report 08-281 (April 25, 2008)
- CEO Letter 228: Interagency Guidance on Authentication in an Internet Banking Environment (October 13, 2005)
- CEO Letter 214: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (March 30, 2005)
- RB 37-10: Check 21 (February 18, 2008)
- Thrift Bulletin 82a: Third Party Arrangements (September 1, 2004)
- CEO Letter 90: FFIEC Information Technology Examination Handbook- Audit Booklet, Electronic Banking Booklet (July 23, 1998)
- CEO Letter 113: Internal Controls (July 14, 1999)
- Examination Handbook: Section 218, Credit Card Lending (N/A)
- Thrift Activities Handbook: Section 340, Internal Control (December 2003)
- Thrift Activities Handbook: Section 341, Technology Risk Controls (January 2002)
- Thrift Activities Handbook: Section 580, Payment Systems Risk (January 1994)
- Examination Handbook: Section 1330, Electronic Funds Transfer Act (N/A)
- Examination Handbook: Section 1335, Expedited Funds Availability Act (N/A)
- Examination Handbook: Section 1336, Check 21 (N/A)
- Check Clearing for the 21st Century Compliance InfoBase, OTS Press Release 04-43 (October 2004)

Appendix E: Mobile Financial Services

AppE.1 Introduction

Mobile financial services (MFS) are the products and services that a financial institution provides to its customers through mobile devices.¹ The mobile channel² provides an opportunity for financial institutions of all sizes to increase customer access to financial services and decrease costs. Although the risks from traditional delivery channels for financial services continue to apply to MFS, the risk management strategies may differ. As with other technology-related risks, management should identify, measure, mitigate, and monitor the risks involved and be familiar with technologies that enable MFS.

AppE.1.a Purpose and Scope

This appendix focuses on risks associated with MFS and emphasizes an enterprise-wide risk management approach to the effective management and mitigation of those risks. This appendix also discusses the technologies used in the mobile channel and may be helpful to the board and management for the integration of MFS into the institution's risk management program. The risks and controls addressed in this appendix, however, are not exhaustive. Additionally, this appendix contains a set of work program objectives to help the examiner determine the inherent risk and adequacy of controls at an institution or third party providing MFS.

AppE.1.b Background

MFS involve the use of a mobile device to conduct banking transactions and to initiate retail payments. Customers' mobile transactions often emulate those initiated on traditional desktop computers; however, MFS can provide more convenient transaction execution capabilities, such as the initiation or acceptance of mobile payments. MFS can pose elevated risks related to device security, authentication, data security, application security, data transmission security, compliance, and third-party management. Customers are often less likely to activate security controls, virus protection, or personal firewall functionality on their mobile devices, and MFS often involve the use of third-party service providers. This appendix addresses the following:

- MFS technologies.
- Risk identification.
- Risk measurement.
- Risk mitigation.
- Monitoring and reporting.

¹ A mobile device is a portable computing and communications device with information-storage capability.

² The mobile channel refers to providing banking and other financial services through mobile devices.

AppE.2 Mobile Financial Services Technologies

Financial institutions implement and offer MFS through technologies such as the following:

- Short message service (SMS)/text messaging.
- Mobile-enabled Web sites and browsers.
- Mobile applications.
- Wireless payment technologies.

AppE.2.a Short Message Service

SMS is a text messaging service component of phone, Web, or mobile communication systems. SMS uses standardized communications protocols to allow devices to exchange short text messages. Messages are typically limited to 160 characters and communicate either between mobile devices or between businesses and mobile devices (e.g., financial institutions requesting customer verification of transactions). Within the context of MFS, a customer uses SMS to provide financial transaction instructions to their financial institution. Financial institutions use SMS to provide information to customers, including account alerts or to communicate one-time passwords for Web site authentication.

AppE.2.b Mobile-Enabled Web Sites

A mobile device's browser allows customers to access a financial institution's Web site. Many financial institutions provide mobile-enabled Web sites, in addition to their regular Web site, which may improve the customer experience. The mobile-enabled Web site is designed to detect the type of device the customer is using (e.g., mobile device or desktop computer) and displays Web pages in the best format for that device.

AppE.2.c Mobile Applications

Mobile applications are downloadable software applications developed specifically for use on mobile devices. Mobile financial applications are developed by or for financial institutions to allow customers to perform account inquiries, retrieve information, or initiate financial transactions. This technology leverages features and functions unique to each type of mobile device and often provides a more user-friendly interface than is possible or available with either SMS or Web-based mobile banking.

AppE.2.d Wireless Payment Technologies

Customers may use mobile technologies to initiate wireless payments at point-of-sale (POS) terminals, make person-to-person (P2P) payments, or make other types of wireless payments, such as parking meter and mass transit access payments. Mobile wallets³ allow customers to make wireless payments with a virtual payment card, as opposed to a physical card. The

³ A mobile wallet is a front-end application that stores payment card information on the mobile device and allows payments to be made using a mobile device. The mobile wallet utilizes traditional retail payment channels such as ACH, EFT, and debit/credit card networks to process the payments.

exchange of payment credentials and authorization between the mobile device and the payment recipient can use different core technologies. Technologies that provide the ability to make wireless payments include the following:

- **Near field communication (NFC).** Wireless protocol that allows for exchange of payment credentials stored on the mobile device and other data at close range. For example, NFC is used to facilitate mobile payment systems developed by mobile phone manufacturers in conjunction with issuing financial institutions.
- **Image-based.** Coded images similar to bar codes used to initiate payments. Credentials may be encoded within an image or stored in the cloud. For example, specific retailers use quick response (QR) codes⁴ to identify customers in a closed-loop mobile payment⁵ system.
- **Carrier-based.** Payments billed directly to a customer's mobile carrier account. Merchants are paid directly by the mobile carrier, bypassing traditional payment networks. For example, a carrier-based payment may occur when mobile users donate money to charity through SMS messages.
- **Mobile P2P.** Payments initiated on a mobile device using the recipient's mobile phone number, e-mail address, or other identifier. Payment is through established retail payment technologies. For example, customers may download a P2P mobile application from their financial institution that allows them to send money to other users enrolled in the institution's system.

Although these technologies help facilitate financial institution-centric mobile payments, established retail payments channels (automated clearing house (ACH), credit/debit networks, electronic funds transfer (EFT), and intra-account transfers) remain the principal methods by which mobile payments are funded⁶ and settled in the U.S. marketplace. With traditional retail payments channels serving as the backbone of mobile payments, users typically are required to provide verifiable financial institution account information or a credit, debit, or prepaid card to establish and fund a mobile payments service. The traditional retail payments channels allow financial institution mobile payments providers to leverage existing banking relationships to verify identities, satisfy federal anti-money laundering requirements, and fund accounts.

AppE.3 Risk Identification

Management should identify the risks associated with the types of MFS being offered as part of the institution's strategic plan. Management should incorporate the identification of risks associated with mobile devices, products, services, and technologies into the financial institution's existing risk management process. The complexity and depth of the MFS risk identification varies depending on the functionality provided through the mobile channel and the

⁴ A QR code is a type of two-dimensional bar code or machine-readable optical label that contains information about the item to which it is attached.

⁵ Closed-loop payments allow consumers to pre-load funds into a spending account that is linked to the payment device that can be used for purchases only at a specific company. Open-loop payments allow consumers to tie a mobile wallet to a personal account (e.g., credit card), do not require a prepaid amount, and spending is not limited to one company.

⁶ Funding refers to adding a positive balance that customers use to make purchases.

type of data in transit and at rest.

The identification process should include risks at the institution and those associated with the use of mobile devices where the customer implements and manages the security settings. In providing customers with avenues for performing banking activities through mobile devices, an institution may transfer to the customer the ability to implement security settings. This transfer increases dependence on the customer to manage the controls over sensitive financial data. Additionally, there are numerous types of mobile devices that present different risks, and management should identify unique risks associated with specific devices. Before implementing mobile products and services, management should identify the associated risks, particularly in the areas of strategic, operational, and compliance risks.

AppE.3.a Strategic Risk

When financial institution management fails to incorporate its decisions regarding MFS into its strategic planning, the institution's level of strategic risk may increase. Management should identify the risks associated with the decision to offer MFS and determine what types of MFS best fit with the strategic vision, goals, and risk appetite of the institution.

AppE.3.b Operational Risk

MFS introduce unique operational risks. Management should identify the risks involved with transaction initiation, authentication and authorization, and the MFS technology itself. Some of the operational risks are associated with the mobile device and how the device communicates with the POS or other similar terminal.⁷ Additionally, the varying access points⁸ provide challenges with authentication and security.

MFS provide the opportunity to leverage tools and techniques not available in traditional banking payment products. The prevalence of mobile devices, common operating systems, and downloadable applications make these devices a target for malware and viruses. Without implementing additional controls, basic device access controls such as personal identification numbers (PIN) may not be adequate to protect data that is stored on a mobile device because these controls could be circumvented by someone who has unrestricted physical access to the device. Additionally, a fraudster can compromise mobile application-based financial services by developing rogue, corrupted, or malicious applications (or adding rogue code to applications) that a customer downloads to his or her mobile device. Therefore, management should consider the implications of operational risks when evaluating and implementing such technologies.

⁷ Traditional payment risks associated with the underlying payment transaction are covered by existing risk management guidance contained in earlier sections of this booklet.

⁸ Access points include a user's home network, cellular network, NFC, Bluetooth, or public Wi-Fi connections, such as those provided by a municipality or business.

AppE.3.b(i) SMS Technology Risk

SMS technology presents a number of security-related risks. SMS messages typically are transmitted unencrypted over widely used telecommunications networks. The messages are also vulnerable to spoofing,⁹ which allows an unauthorized user to send an SMS message pretending to be from a different mobile number to mislead a customer into providing sensitive information to the unauthorized user. Similarly, fraudulent SMS messages may mislead customers into revealing financial institution account information or information used to access financial institution systems.

AppE.3.b(ii) Mobile-Enabled Web Site Risk

Mobile-enabled Web sites rely on existing Internet security protocols, which make the sites subject to many of the same vulnerabilities¹⁰ that can compromise computer-based banking. Additionally, mobile devices can be limited by their hardware and operating systems, which can result in a reduced level of security. Mobile Web browsers are common starting points for malicious attacks, and malicious messages can come from many other sources.¹¹ Whereas desktop browsers have anti-phishing¹² and anti-cross-site scripting (anti-XSS) capabilities¹³ to filter out the malicious code from Web sites, mobile-enabled browsers do not always have such features. The lack of anti-phishing and anti-XSS modules can increase the possibility of loss of sensitive information when using a mobile device.

As is the case with any Web-based application, attacks involving unvalidated “redirects and forwards”¹⁴ can be used to maliciously craft a URL¹⁵ to bypass the application’s access control check and then provide the attacker access to privileged functions that normally would not be accessible to them. The attacks also can lead to malware download and installation. By modifying a URL and redirecting the browser to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.

Users often find it difficult to recognize a phishing message or a forged Web site, or determine

⁹ SMS spoofing is the manipulation of address information to impersonate a user.

¹⁰ Vulnerabilities include malware attacks, eavesdropping, and spoofing.

¹¹ Besides e-mail and instant messages, sources can also include SMS, social messengers, hypertext markup language (HTML) links, and QR codes.

¹² Anti-phishing software are programs, either integrated with or built in to the Web browser, that display the real domain name of the site that a user is visiting to help prevent fraudulent sites from posing as legitimate sites.

¹³ Anti-XSS functionality is a defense mechanism to XSS, which is a vulnerability found in Web applications that enables attackers to inject client-side script into Web pages prompting a Web page to display unvalidated user input. Attackers may use this vulnerability to bypass access controls.

¹⁴ Unvalidated Web site redirects are possible when a Web application accepts untrusted input that could cause the application to redirect the request to a malicious URL. A user may be redirected and not realize it.

¹⁵ URL is an acronym for uniform resource locator and is a reference (an address) to a resource on the Internet.

whether a site is safe. Additionally, mobile browsers displayed on small screens may not effectively display the same visual security cues more easily seen on full-scale browsers on large screens.

AppE.3.b(iii) Mobile Application Risk

Applications can be downloaded onto mobile devices from a number of application stores. Although device manufacturer-authorized application stores perform due diligence, applications may still contain vulnerabilities that cause risks to the user and the financial institution. On some mobile devices, it is possible to download an application from application stores not authorized by the manufacturer, which poses a greater risk of users being exposed to malicious code because the applications may not be adequately reviewed by the store. Distribution of malware through applications is a material risk to the institution and its customers because of malware's ability to compromise sensitive data and monitor communications.

Another risk to the institution and its customers occurs with the end user's ability to access root user¹⁶ privileges in the operating system of the device. The process to gain access is known as "rooting." Another method of removing the manufacturer's device controls or core operating system controls is "jailbreaking." Jailbreaking provides the user with additional access to and control over the device's operating and file systems, including the ability to circumvent security controls. For certain mobile devices, rooting and jailbreaking allow the user to download applications from untrusted sources, which may introduce malware onto the device.

Many applications store usernames, passwords, and e-mail addresses in clear text. Because users often have the same usernames and passwords across systems, it is possible to use the information obtained from a poorly designed mobile application to compromise user accounts on other systems. Mobile applications collect personal information (e.g., name, account number, and other personal details) and track user activity (e.g., purchases and location). These data are valuable to attackers and can result in compromised user privacy. Without properly securing the mobile application, unauthorized users can gain access to the back-end databases containing confidential information.

The mobile ecosystem is the collection of carriers, networks, platforms, operating systems, developers, and application stores that enable mobile devices to function and interact with other devices. Vulnerabilities may exist in any area of this decentralized mobile ecosystem and, therefore, result in a multi-entity patch management process among mobile device operating system developers, device manufacturers, wireless carriers, and other application developers. As a result of the decentralized ecosystem of some devices, a known vulnerability may remain unremediated while the various parties review, update, and ensure compatibility with their applications and the security mitigation. Additionally, integrating MFS application functionality with other applications and services on the customer's device may introduce vulnerabilities because MFS applications are not built in or native to the device.

AppE.3.b(iv) Mobile Payments Risk

¹⁶ The root user is the conventional name of the user who has all rights or permissions to all files and programs. Having such rights or permissions allow the root user to do many things an ordinary user cannot.

The portability of mobile devices can lead to the devices being misplaced or stolen, which may allow unauthorized access to the mobile wallet or user credentials. Such access can result in unauthorized payments and funds transfers and fraudulent purchases.

Because mobile payments at the POS may use NFC, communications between the device and the POS terminal can be intercepted, while the device is in the user's possession. Even if these communications are encrypted, which they are not by default, there remains a potential for unauthorized access to transaction information, which could be used to perpetrate financial fraud.

Vulnerabilities create the potential to take advantage of weak security controls in the payment provisioning or enrollment functions of the NFC payment system process to commit fraud. Malicious actors using stolen identity information (e.g., from credit reports, tax records, health care records, and employee records) may establish fake accounts on NFC-enabled mobile devices to make unauthorized transactions.¹⁷

AppE.3.c Compliance Risk

Financial institution management should identify the compliance risks as it determines which MFS to offer and continue to monitor these risks as the technology for MFS evolves. Consumer laws, regulations, and supervisory guidance that apply to a given financial product or payment method generally apply regardless of the technology used to provide the products and services.

One of the challenges in providing MFS is that a significant portion of the innovation in the industry is driven by entities outside of the traditional financial services sector. These entities may be unfamiliar with regulatory requirements and supervisory expectations that apply to regulated financial institutions and their service providers. Management should understand how the institution's risk profile changes when it uses any third party, but particularly a third-party service provider that is unfamiliar with the regulation and supervision of the financial services sector, to design applications.

AppE.4 Risk Measurement

¹⁷ Refer to U.S. Secret Service and PCI Security Standards Council, "Joint Advisory Bulletin: Mobile Payment System Vulnerability," September 2015.

¹⁸ Personalization is providing a tailored user experience based on user preferences through MFS.

The identification of risks should be followed by a measurement of the level and types of risks involved in offering MFS. Management should measure potential risks across all applicable risk categories. This assessment may help management determine the likelihood and impact of the risks affecting the institution. The results should be prioritized to determine which controls may be appropriate for the services provided by the institution. This process should be ongoing and updated whenever management implements a change to the strategy or MFS.

AppE.5 Risk Mitigation

Effective enterprise-wide risk management helps management determine whether controls are effective and goals are compatible with the financial institution's risk appetite and strategic plan. When offering MFS, management should mitigate identified risks by implementing effective controls across the institution. As is the case with any new product offering, management should develop and implement policies and procedures to comply with applicable laws and regulations and require appropriate internal controls for security and confidentiality of the MFS transactions. As part of the institution's audit of retail payments systems, audit coverage should include MFS.

Unlike many financial services that allow institutions to control much of the interaction, MFS typically require the coordinated and secure exchange of information among several unrelated entities. Depending on the type of MFS offered, institutions may find that the effective management of risks involves interaction with application developers, mobile network operators, device manufacturers, specialized security firms, and other nonfinancial third-party service providers. Additionally, financial institution management should provide security awareness materials to the institution's customers, which may include prudent security practices for the device (e.g., use of mobile anti-malware, PIN protection) so that customers understand their roles in securing the device and the need for such security.

AppE.5.a Strategic Risk Mitigation

Financial institution management should incorporate decisions on providing MFS into its strategic planning process. Various elements should be part of any mobile strategy, including the products and services to be offered, types of transactions allowed, limits over transaction amounts, mobile architecture design, supported mobile devices, customer needs, and use of third parties.

AppE.5.b Operational Risk Mitigation

Financial institution management should develop a layered approach to mitigate operational risks from MFS. This may include implementing security techniques at the server and database level; using transaction monitoring and geolocation techniques to identify anomalous MFS transactions; implementing and refining fraud prevention, detection, and response programs that facilitate rapid notification of potentially fraudulent transactions; applying additional controls (e.g., stronger authentication, encryption) to prevent unauthorized access to sensitive customer information stored on the device; and educating customers and employees to identify social engineering attempts that could lead to fraud.

The following are general operational controls that an institution should consider when implementing MFS.

- **Enrollment.** Financial institution management should have appropriate controls and communication of policy and procedures to verify a customer's identity when enrolling customers in mobile payment systems used at the point of sale (e.g., allowing a customer with a physical payment card the ability to enroll that card into the customer's mobile wallet).
- **Authentication and authorization.** A financial institution should have a process for authenticating users of MFS to protect customers against fraudulent transactions or malicious activities. Depending on the technology used and associated level of risk, financial institutions may consider biometric (e.g., voice, fingerprint, facial recognition) or out-of-band¹⁹ authentication processes. The financial institution should not use mobile payment applications that rely on less secure (e.g., single factor) methods of authentication.²⁰
- **Application development and distribution.** The application development life cycle should include a thorough design and architecture review using threat-modeling²¹ techniques to reduce potential risks and meet the financial institution's security objectives. Additionally, application developers should develop applications using secure coding techniques,²² and applications should be rigorously tested for vulnerabilities (e.g., detailed code analysis and white-hat hacking²³) at least annually. Institutions should distribute applications and updates securely and in a timely fashion. Management should consider designing anti-malware capabilities into mobile applications. Applications should not retain sensitive customer information on the device, such as user IDs and passwords, and the application should securely wipe any sensitive customer information from memory when the customer exits the application. If a third party developed the application, the third-party developer should incorporate these control requirements into its development process.
- **Application security.** Management should ensure that the institution's MFS contain log-on credentials in addition to those used to access the device. Management should employ multi-

¹⁹ Out-of-band refers to activity outside of the primary means of interfacing with the customer. For example, if a user is performing activity online, he or she may be authenticated through a one-time password sent via text message.

²⁰ Resources that provide detailed information about authentication for financial institutions include: FFIEC Authentication Guidance (http://www.ffiec.gov/pdf/authentication_guidance.pdf), Frequently Asked Questions (https://www.ffiec.gov/pdf/authentication_faq.pdf), and Authentication Supplement ([https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20\(FFIEC%20Formatted\).pdf](https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formatted).pdf)).

²¹ Threat modeling is a structured approach that enables an institution to aggregate and quantify potential threats. In the context of application development, threat modeling can be used to capture, organize, and analyze all of the threat information of an application and its environment that affects application security. It is used to enable informed decision-making about application security and helps to produce and rank a list of security improvements.

²² Secure coding is the process of developing code (e.g., Web application) with security built in during the development process using technical controls to mitigate the occurrence of software vulnerabilities.

²³ White-hat hacking, also called ethical hacking, refers to the specialization of penetration testing and other testing methodologies to review the security of an institution's information systems by determining flaws and vulnerabilities.

factor authentication or layered security controls depending on the types and volumes of transactions. The system should require re-authentication whenever the device or MFS is unused for a designated period and each time the user launches the application.

- **Contracts.** The institution should use well-constructed contracts, developed with legal counsel, to mitigate its risks from third parties. Contracts should be appropriate for the institution's specific mobile strategy and should clearly identify each party's roles and responsibilities. Financial institution management may need to establish contracts with the institution's customers and third parties that cover types of data collected and circumstances related to data sharing.
- **Customer awareness.** Financial institution management should make reasonable efforts to educate customers about the need to maintain the physical and logical security²⁴ of mobile devices and suggest that users regularly install operating system and firmware updates. Management should make clear that customers should download applications only from reputable sources, and the institution's Web site should have a link to the source of any institution-approved applications. Institutions should have customer security awareness materials available to help customers understand the risks involved in using MFS, including the use of unsecured "public" wireless networks. Financial institutions should suggest that customers consider running anti-malware software on their mobile devices, if possible.
- **Logging and monitoring.** Management should have logging and monitoring capabilities on all MFS to track customer activity and security changes and identify anomalous behavior and transactions.

AppE.5.b(i) SMS Technology Risk Mitigation

Financial institution management should employ compensating controls (e.g., redacting customer account numbers when sent via SMS) to mitigate the inability to encrypt SMS messages. Additionally, management should limit the access or functionality available to the customer through SMS banking. When the transaction risk is more significant, management should consider other risk mitigation methods, including pre-registration and the use of security tokens. PINs also could be employed, but are often easier to break and harder to remember. To strengthen the security of PIN usage, management can implement specific requirements (e.g., requiring them to be regularly changed). An institution should update its customer awareness materials to include information on avoiding phishing messages by SMS.

AppE.5.b(ii) Mobile-Enabled Web Site Risk Mitigation

Financial institution management should consider several controls to mitigate risks associated with mobile-enabled Web sites, including the following:

- Provide specific training and security awareness materials for users and customers accessing the institution's sites to teach them how to identify compromised sites.
- Require Web site developers to follow a secure development life cycle to increase the security of the Web sites designed for the financial institution.

²⁴ Prudent security practices may include information on the use of the device's password function, general safeguards, and any additional logical security controls (e.g., available security applications).

- Require developers to build a secure Web site especially for mobile devices and encourage them to follow the guidelines provided from the Open Web Application Security Project (OWASP)²⁵ Top 10 for Web application and OWASP Top 10 for mobile.
- Make available a baseline set of controls, and educate customers on the use of those controls to protect their device and information (e.g., device passwords with complexity, application passwords, and an auto-wipe feature after excessive password failures).
- Determine whether mobile browsers have available safeguards implemented, such as anti-XSS modules or additional monitoring of browsers for those that are no longer supported, and deny access to devices with mobile browsers not meeting minimum standards.
- Determine whether mobile-enabled Web sites are designed with the following mitigating controls to help minimize the potential for exploitation of “redirect and forward” vulnerabilities:
 - Avoid using redirects and forwards.
 - Explicitly hard code the URL to prevent manipulation by an attacker.
 - Apply additional validation or control checks to verify the user trying to access the URL, validate the URL, check the appropriateness of the URL request, and prevent a malicious user from redirecting site users to a phishing, malicious, or nonaffiliated site.
 - Create a whitelist²⁶ of trusted URLs.
 - Force all redirects to go through a page that notifies a user that he or she is leaving the page and require user confirmation.
 - Perform frequent vulnerability scans.

AppE.5.b(iii) Mobile Application Risk Mitigation

Management should consider the use of a variety of security mechanisms for mobile applications and should evaluate, prioritize, and implement appropriate mitigating controls, including the following:

- Employing tools, such as policy enforcement and device fingerprinting, to determine whether a customer’s mobile device will be allowed to access the institution’s MFS by validating device characteristics (e.g., level of security controls, operating system type, operating system version, whether the mobile device is rooted or jailbroken, and patch status).
- Providing security awareness training to end users to help them recognize legitimate applications and provide a list of reputable sites to download institution-approved applications.
- Performing security testing at all post-design phases of the system development life cycle for all applications. Establishing a process to deactivate older application versions that no longer meet minimum security requirements or prompt the end user to upgrade to an acceptable version.
- Providing basic customer education relative to security to mitigate the risks associated with rooted or jailbroken devices.

²⁵ OWASP is an online community dedicated to Web application security.

²⁶ A whitelist is a list of trusted entities. With respect to URL redirects, an institution can create a whitelist of allowable URLs.

- Designing applications to ensure that critical information, such as passwords and credit card numbers, does not reside directly on a device. If critical information resides directly on a device, it should be stored securely (e.g., within an encrypted data section or within encrypted storage in the file system).
- Establishing processes when implementing mobile applications to collect only necessary information and appropriately secure that information and any related analytics reporting available within or external to the mobile application.
- Designing applications to mitigate the risk of unpatched devices or those that are no longer supported by the manufacturer.
- Securing back-end servers containing the MFS application and customer data to prevent unauthorized users from accessing data. If a third party manages the application and back-end server, validate that the third party implements appropriate security measures.
- Developing applications in a “sandbox,”²⁷ which creates a more secure area within the device from which to process transactions.
- Maintaining awareness of vulnerabilities through online forums, vendor sites, and U.S. Computer Emergency Readiness Team (US-CERT) or Financial Services-Information Sharing and Analysis Center (FS-ISAC) alerts. The vulnerabilities may affect unpatched and unsupported operating system versions. Take a risk-based approach when offering MFS to customers using unpatched and unsupported operating system versions and recommend to customers that they upgrade to more secure software, operating systems, and devices when appropriate.
- Periodically testing the functionality of MFS applications with other integrated mobile applications and services.

AppE.5.b(iv) Mobile Payments Risk Mitigation

Mitigating controls in mobile payments should include discussions between the financial institution and its mobile payments provider to identify and minimize potential risk factors. Financial institution management should work with mobile-payments platform developers to encourage the use of the following:

- Traffic filtering to help prevent or minimize denial-of-service attacks.²⁸
- Trusted platform modules.²⁹
- Secure telecommunications protocols (e.g., secure sockets layer/transport layer security [SSL/TLS]).

²⁷ A sandbox is a restricted, controlled execution environment that prevents potentially malicious software, such as malicious mobile code, from accessing any system resources except those for which the software is authorized.

²⁸ The goal of a denial-of-service attack is to restrict the availability of services or systems. If the institution can effectively filter traffic to disallow unknown or potentially malicious traffic, this can support the institution’s larger denial-of-service planning.

²⁹ The trusted platform module is an international standard for a secure crypto processor that is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.

- Tokenization³⁰ to limit the transmission of account information.
- Encryption to minimize the opportunity for the interception of traffic.
- Anti-malware software.
- Authentication controls of both the user and application.
- Encryption of personal information stored on the mobile device.

AppE.5.c Compliance Risk Mitigation

Institution management and system designers should consult with compliance staff to minimize compliance risks when developing and implementing MFS. Financial institution management should reassess its current mobile service offerings regularly and, in conjunction with appropriate compliance and legal staff, examine applicable laws and regulations, including those for consumer protection, to determine which may apply to their specific mobile financial service offerings. The compliance officer should take the following steps:

- Determine whether applicable disclosure requirements are fully accessible on the mobile device.
- Review the institution's existing compliance management system and ability to make appropriate modifications to policies and procedures to address the products, services, and operating features of the MFS technology.
- Monitor for any legal and regulatory changes that may be applicable to MFS on an ongoing basis.
- Train institution staff regarding compliance implications of MFS.

AppE.6 Monitoring and Reporting

Financial institution management should have appropriate performance monitoring systems for assessing whether the product or service is meeting operational expectations. Such systems should do the following:

- Include limits on the level of acceptable risk exposure that management and the board are willing to assume.
- Identify specific objectives and performance criteria, including quantitative benchmarks for evaluating success of the product or service.
- Periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner.

³⁰ In the context of data security, tokenization is the process of substituting a sensitive data element with a surrogate value, referred to as a token.

- Modify the business plan, when appropriate, based on the performance of the product or service. Such changes may include exiting the activity should actual results fail to achieve projections.

A variety of reports can facilitate management oversight of MFS activities. Management should structure the report content to meet the needs of the various levels of management. Reports should address point-in-time as well as trend activity for both individual customers and mobile channel activities to compare actual trends with the mobile strategy. Reports for new services should emphasize the volume of activity from the onset and report on changes in usage or volume over time. Management should develop reports to document the various demographic and industry sectors served and monitor changes in these areas to determine whether the MFS offered are meeting the institution's strategy or should be refined.

AppE.7 Mobile Financial Services Work Program

Objective 1: *Management effectively responds to issues raised or problems related to MFS.*

1. Review examination documents and financial institution reports for outstanding issues or problems related to MFS. Consider the following:
 - a. Pre-examination planning memos.
 - b. Prior regulatory reports of examination.
 - c. Prior examination work papers.
 - d. Internal and external audit reports, including SSAE 16³¹ reports.
 - e. Financial institution's overall risk assessment and strategic plan.
2. Review management's response to audit recommendations on MFS, if any, noted since the prior examination. Consider the following:
 - a. Adequacy and timing of corrective action.
 - b. Resolution of root causes rather than just specific audit deficiencies.
 - c. Existence of any outstanding issues.
 - d. Monitoring systems used to track the implementation of recommendations on an ongoing basis.

Objective 2: *Financial institution management incorporates (or plans to incorporate) its plan for implementing MFS into its strategic planning process.*

1. Determine whether financial institution management has an MFS strategy to identify the types of MFS that management plans to offer.

³¹ Statement on Standards for Attestation Engagements (SSAE) No. 16 is a type of audit report of controls at a service organization.

2. Describe the MFS that the financial institution offers. Determine whether the institution offers or implements MFS through one or more of the following technologies:
 - a. SMS.
 - b. Mobile-enabled Web sites or browsers.
 - c. Mobile applications.
 - d. Technologies that enable mobile payments.

Objective 3: *Financial institution management identifies the risks associated with offering MFS.*

1. After the MFS strategy is complete, determine whether the institution developed an effective risk assessment process for the MFS offerings. Verify whether management incorporates the results of the risk assessment into a process to periodically review and update the strategy.
2. Review whether the risk identification process includes risks associated with MFS, particularly in the areas of strategic, operational, and regulatory risks.
3. With respect to strategic risk, determine whether management identified the risks associated with the decision to offer MFS and whether that is consistent with the strategic vision, goals, and risk appetite of the institution.
4. Determine whether management considered and identified operational risks associated with MFS, including risks involved with the following:
 - a. Transaction initiation and completion.
 - b. Authentication and authorization.
 - c. Technology used for MFS.
 - d. Mobile devices.
 - e. Method of communication between the device and the terminal accepting payment.
 - f. Authentication and security of access points.
 - g. Fraud tools and techniques.
 - h. Current and emerging threats to mobile applications, weaknesses in mobile application security, and prevalence of mobile devices, common operating systems, and downloadable applications.
5. Determine whether management also considered the implications of operational risks specific to technologies used to implement MFS. Specifically, review whether management appropriately identified the differing risks related to the following technologies:
 - a. **SMS:** Include the lack of security through unencrypted text messages; SMS spoofing; and fraudulent text messages (phishing).
 - b. **Mobile-enabled Web sites:** Include vulnerabilities with Internet banking (hardware, operating system, and security limitations); malicious messages through Web-based attack vectors; limitations on anti-phishing and anti-XSS capabilities; malicious attacks

- through unvalidated redirects and forwards; user constraints on recognizing phished or forged sites; and limitations on visual security cues.
- c. **Mobile application:** Include application vulnerabilities (e.g., unpatched and outdated applications); malware; ability to jailbreak or root devices; use of unapproved application stores; weak storage controls over confidential information on devices; and inappropriate access to back-end databases.
 - d. **Mobile payments:** Include loss or theft of mobile devices leading to unauthorized payments, funds transfers, and credit card purchases; interception of NFC communications; and weak security controls in the payment provisioning process.
6. With respect to compliance risk, determine whether management identified the applicable risks related to MFS. Review whether management understands that the consumer laws, regulations, and supervisory guidance that apply to a given financial product or payment method generally apply regardless of the technology used. Additionally, determine whether management identified risks associated with the use of nontraditional third-party service providers often found in the innovation and development sphere of MFS.

Objective 4: Financial institution management appropriately and effectively measures risks associated with MFS and determines the likelihood and impact of those risks.

1. Determine whether management effectively measures risks and determines the likelihood and impact of those risks.
2. Determine whether management effectively prioritizes measured risks.
3. Determine the effectiveness of the frequency of the measurement process.

Objective 5: Financial institution management effectively identifies and implements controls to mitigate identified and prioritized risks associated with the MFS offering.

1. Determine whether management incorporates mobile risks into the overall risk management process.
2. Determine whether management implements policies and procedures for the MFS offering.
3. Determine whether management puts in place appropriate internal controls to ensure security and confidentiality of MFS.

4. Determine whether management implements controls to mitigate all applicable categories of risks related to MFS, including strategic, operational, and compliance risk.
 - a. **Strategic risk mitigation:** Review whether management incorporates its decisions to provide MFS into its strategic planning process.
 - b. **Operational risk mitigation:** Review whether management controls include the following: risk management; transaction monitoring and geolocation tools; fraud prevention, detection, and response programs; additional controls (e.g., stronger authentication³² and encryption); authentication and authorization processes (e.g., processes to enroll customers and devices in the mobile channel); application development and distribution controls (e.g., process for approving and submitting mobile application code to distribution partners); application security controls (including strategy to deactivate older application versions); contracts and agreements; customer awareness processes; and logging and monitoring processes. Specifically, review the controls that management has in place over the technologies employed for MFS, including the following:
 - SMS technology.
 - Mobile-enabled Web sites.
 - Mobile application.
 - Mobile payments.
 - c. **Compliance risk mitigation:** Review whether management consults with compliance staff, reassessing current mobile service offerings regularly and examining for compliance with applicable laws and regulations.
5. Determine whether management has appropriate and independent testing of controls for effectiveness.

Objective 6: *Financial institution management maintains effective oversight of MFS activities. Management maintains appropriate reporting for various levels of management to support that oversight.*

1. Review the monitoring process to determine whether the institution has appropriate performance monitoring systems to allow management to assess whether the product or service is meeting operational expectations. Determine whether the systems include the following features:
 - a. Limits on the level of acceptable risk exposure that management and the board are willing to assume.
 - b. Specific objectives and performance criteria to evaluate success of the product or service.

³² A review should include the financial institution's consideration of expectations set forth in appropriate supervisory guidance (e.g., authentication guidance in footnote 20 of this appendix).

- c. Ability to produce reports that periodically compare actual results with projections and qualitative benchmarks that provide trend information.
 - d. Ability to produce reports that provide data, which would trigger changes in the business plan, as appropriate.
- 2. Determine whether the institution's reporting process describes the following:
 - a. MFS activities.
 - b. Information to meet the needs of the various levels of management.
 - c. Trends, volumes, and changes in activity over time.
 - d. Statistics on demographics and locations served to evaluate whether the institution is meeting its strategy.

Objective 7: Discuss corrective action and communicate findings.

- 1. Review preliminary conclusions with the examiner-in-charge (EIC) regarding the following:
 - a. Violations of laws and regulations.
 - b. Significant issues warranting inclusion as matters requiring attention or recommendations in the report of examination.
 - c. Proposed URSIT³³ management component rating and the potential impact of the conclusion on composite or other component information technology ratings.
 - d. Potential impact of the conclusions on the institution's risk assessment.
- 2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.
- 3. Document conclusions in a memorandum to the EIC that provides report-ready comments for all relevant sections of the report of examination and guidance to future examiners.
- 4. Organize work papers to ensure clear support for significant findings by examination objective.

³³ Uniform Rating System for Information Technology.



Federal Financial Institutions Examination Council

FFIEC

Supervision of Technology
Service Providers

TSP

OCTOBER 2012

**IT EXAMINATION
HANDBOOK**

Table of Contents

Introduction	1
Supervisory Policy	2
Examination Responsibility	2
A. Insured Financial Institution	2
B. Insured Financial Institution as TSP	2
C. Holding Company and Non-Bank Subsidiary of the Holding Company	2
D. Bank Service Company as TSP	3
E. Independent TSPs, Including Those in the Multi-Regional Data Processing Servicers Program	3
Supervisory Programs	4
MDPS Program	4
Regional TSP Program	4
Supervision of Foreign-Based TSP Program	5
Shared Application Software Review Program	5
Roles and Responsibilities	5
Agency-In-Charge	6
Central Point of Contact	6
Examiner-In-Charge of Site or Activity	6
Risk-Based Supervision	6
Risk-Based-Examination Priority Ranking	7
Uniform Rating System for Information Technology	7
Frequency of Examinations	8
Risks Associated With TSPs	8
Risk Management	9
Audit and Internal Controls	9
Report of Examination	10
ROE Distribution	10
Customer List	10

Introduction

The Board of Governors of the Federal Reserve System (FRS), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (each individually, Agency, and collectively, Agencies) have statutory authority to supervise third-party servicers that enter into contractual arrangements with their regulated financial institutions.^[1]

The "Supervision of Technology Service Providers" booklet (TSP Booklet), of the FFIEC^[2] Information Technology Examination Handbook (IT Handbook), addresses this authority and rescinds the previous version dated March 2003. The TSP booklet outlines the Agencies' risk-based supervisory program and includes the examination ratings used for regulated financial institutions and their Technology Service Providers (TSP).^[3]

A financial institution's use of a TSP to provide needed products and services does not diminish the responsibility of the institution's board of directors and management to ensure that the activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations, just as if the institution were to perform the activities in-house.

While the examinations of TSPs generally focus on the underlying information technology (IT) risk, the risk assessment process also considers all business lines in which TSPs engage to ensure that all covered services are effectively included. The Agencies expect financial institutions to have a comprehensive, enterprise risk management process in place that addresses vendor management for their relationships with TSPs. The risk management process should include risk assessments and robust due diligence for the selection of TSPs, contract development, and ongoing monitoring of all TSPs' performance.^[4]

The Agencies conduct IT-related examinations of financial institutions and their TSPs based on the guidelines contained in the IT Handbook. The handbook is composed of the following individual booklets that address governance of risks expected of financial institutions and their TSPs as well as detailed examination procedures:

- Audit
- Business Continuity Planning
- Development and Acquisition
- Electronic Banking
- Information Security
- Management
- Operations
- Outsourcing Technology Services
- Retail Payment Systems

- Supervision of Technology Service Providers
- Wholesale Payment Systems

Management of financial institutions and TSPs should be aware of the guidance described in the IT Handbook.

Supervisory Policy

Supervisory policy provides for interagency examinations of TSPs that service insured financial institutions supervised by more than one federal financial institution regulator. The policy is expected to eliminate the need for separate examinations of TSPs by more than one regulator and to result in more efficient use of examiner resources and with less burden to the supervised TSP. Notwithstanding this policy, no federal or state regulatory agency is precluded from conducting an independent examination of any TSP that is servicing an insured financial institution for which the agency is responsible.

Federal and/or state banking agencies participating on interagency TSP examinations are precluded from levying any examination-associated fees against the examined service provider.

Examination Responsibility

Examination responsibility is determined based on the class/type of servicer as well as the class/type of insured financial institution(s) being serviced.

A. Insured Financial Institution

Technology service centers operated by an insured financial institution or its subsidiary are examined by the Agency responsible for the supervision of the financial institution.

B. Insured Financial Institution as TSP

Services provided by an insured financial institution, or by its subsidiary, to one class ^[5] or more of insured financial institutions are examined by the Agency responsible for supervising the servicing institution. The primary regulatory Agency seeks input from other interested Agencies and performs an IT examination of the entity's operations as they relate to the technology services it provides. The Agency generates a report with supporting information regarding the adequacy of its institution's servicing operations and provides the report to the primary federal regulators of the serviced institution(s). Application of the Risk-Based-Examination Priority Ranking Program (RB-EPRP) to the servicing institution is left to the discretion of its regulatory Agency.

C. Holding Company and Non-Bank Subsidiary of the Holding Company

Services provided by a financial institution holding company, or by its non-bank subsidiary, to one class or more of insured financial institution are examined by the Agency responsible for supervising the servicing entity. The primary regulatory Agency seeks input from other interested Agencies and performs an IT examination of the entity's operations as they relate to the technology services it provides. The Agency generates a report with supporting information regarding the adequacy of the entity's operations and provides the report to the primary federal regulators of the serviced institution(s). Application of the RB-EPRP to the servicing entity is left to the discretion of its regulatory Agency.

D. Bank Service Company as TSP

Responsibility for the examination of bank service companies ^[6] is based first on the type/class of entity(s) holding controlling ownership ^[7] in the servicer. Specifically:

- If there is one or more controlling owner, primary examination responsibility falls to the Agency(s) supervising the controlling owner(s).
- Where there is only one controlling owner, or where one controlling owner has claim to materially greater ownership interests relative to the others, the Agency supervising that owner has the discretion to retain primary examination responsibility with regard to any interagency examination work.
- Where controlling ownership is equally distributed, the primary examination responsibilities are rotated as agreed by the interested Agencies.

In all instances, regardless of the number of controlling owners, the Agencies supervising the serviced financial institutions have an interest in participating on interagency examinations.

E. Independent TSPs, Including Those in the Multi-Regional Data Processing Servicers Program

Responsibility for the examination of independent TSPs is based on the class of insured financial institution being serviced. If more than one class of insured institution is serviced, the examination is conducted jointly, and on a rotated basis, as agreed to among the federal financial institution regulators responsible for the classes of serviced institutions.

Examination of companies in the Multi-Regional Data Processing Servicers (MDPS) program is administered by the Agencies. The Agencies determine which TSPs are subject to examination under the MDPS program. Generally, Agency-In-Charge (AIC) responsibilities for an MDPS company are rotated among the Agencies responsible for the class of serviced, insured financial institutions after two consecutive examination cycles, ^[8] with exceptions subject to the Agencies' review and approval. As indicated in section C on page 3, if an independent MDPS company, through acquisition, becomes a

financial holding company, a bank holding company, a thrift holding company, or a non-financial institution subsidiary or affiliate thereof, the Agency supervising the holding company serves as the AIC unless such Agency chooses to rotate the responsibilities.

Examinations of independent TSPs that are not part of the MDPS program are administered by the Agencies' regional/district management under the guidelines in this booklet.

Supervisory Programs

The Agencies coordinate the interagency programs for the supervision of TSPs through the FFIEC. The programs establish responsibilities and requirements for the collaborative efforts of the Agencies to ensure effective supervision while making efficient use of examiner resources and reducing burden on the TSPs.

MDPS Program

The Agencies are responsible for the administration, coordination, oversight, and implementation of the supervisory program for the largest, systemically important TSPs: the MDPS program. The program represents a cooperative arrangement among the Agencies for the achievement of shared and consistent supervisory goals and objectives.

As a general rule, a TSP is considered for the MDPS program when the TSP processes:

- mission-critical applications ^[9] for a large number of financial institutions that are regulated by more than one Agency, thereby posing a high degree of systemic risk; or
- from a number of data centers located in different geographic regions.

The companies in the MDPS program can pose a significant risk to the banking system if one or more have operational or financial problems or fail. Because these companies provide services to banks, savings associations, and credit unions, the supervisory program allows for effective use of Agencies' resources, reduced burden to the MDPS, shared knowledge of the company's operations, development of a joint supervisory strategy, and generation of a single Report of Examination (ROE) for the company and its client-regulated financial institutions.

Regional TSP Program

The Agencies' district or regional offices are responsible for the administration, coordination, oversight, and implementation of the supervision of TSPs that are local and smaller in size or complexity. Although these TSPs are not part of the MDPS program, they are supervised in a similar manner and under the guidelines of the Supervisory

Policy previously discussed.

Supervision of Foreign-Based TSP Program

Advances in technology enable financial institutions to provide customers with an array of products, services, and delivery channels. One result of these changes is that financial institutions are entering into contractual obligations with, and outsourcing banking activities to, foreign-based TSPs (FBTSP). Outsourcing or subcontracting (by domestic TSPs) to FBTSPs raises country risk, in addition to other risks presented by the use of domestic TSPs. Country risk is the exposure to social, economic, and political conditions in a foreign country that could adversely affect the ability of a FBTSP to meet its contractual obligations.

The Agencies' supervisory approach to cross-border outsourcing emphasizes the responsibility of the serviced financial institution to conduct adequate due diligence, manage risks appropriately, comply with applicable U.S. and foreign laws and regulations, and ensure access to critical information with respect to the services being provided by the FBTSP. If circumstances warrant, the Agencies arrange, through the appropriate foreign regulatory agencies, to obtain information related to the services provided to U.S. regulated financial institutions. If significant risks and concerns warrant on-site supervision of the FBTSP, the Agencies secure approval of their representatives at the Task Force on Supervision (TFOS) ^[10] before conducting the examination. For these examinations, the Agencies use the same interagency process defined in this TSP booklet and described throughout the IT Handbook.

Shared Application Software Review Program

The Agencies established the Shared Application Software Review (SASR) program to effectively employ interagency resources in uniform reviews of software packages or systems. Shared application software packages include stand-alone software and integrated (turnkey system) packages. Generally, these are purchased software that involves mission-critical, core, or high-risk applications widely used at financial institutions.

The SASR program is not limited, however, to the review of shared application packages. The Agencies also use SASRs to support interagency safety and soundness initiatives when focusing on higher-risk applications in larger financial institutions. A SASR can evaluate financial institutions' software packages for use in wire transfer, capital markets, derivatives development/record keeping, securities transfer, asset management, Bank Secrecy Act and anti-money laundering, consumer compliance, or other lines of business.

An internal, confidential SASR report is developed strictly for regulatory purposes. The report is not provided to the company that developed the software application or to the user financial institutions. The information in the SASR report is intended to augment and expedite the Agencies' supervisory process by identifying potential systemic risks and presenting information, suggestions, and instructions to aid in completing the examinations of financial institutions that use the various applications and software products covered by this program.

Roles and Responsibilities

Agency-In-Charge

Based on an annual schedule approved by either the Agencies or the Agencies' district/regional offices, the Agencies select an AIC for each examined TSP.

Central Point of Contact

Each Agency assigns a qualified IT examiner to serve as its Central Point of Contact (CPC) for each company in the MDPS program, and where appropriate, for regional TSPs. ^[11] The selected CPCs form the CPC team, which serves as the primary group for all interagency examination-related activities, including developing supervisory strategies, performing examination activities, and pursuing the resolution of any significant findings. The CPC for the AIC is designated as the Lead CPC.

For TSPs that do not have designated CPC teams, the examiners assigned by the AICs are responsible for the supervision and oversight of the TSPs. These examiners carry out their responsibilities in collaboration with examiners from participating Agencies.

Examiner-In-Charge of Site or Activity

Some examinations of sites or specific supervisory activities of a TSP may have an examiner, who is not a member of the CPC team, assigned as Examiner-In-Charge (EIC). In these situations, the EIC conducts the assignment under the direction of the CPC team and is responsible to the Lead CPC for the administration and overall performance of the supervisory activity. The EIC keeps the CPC team informed of examination progress and findings.

Risk-Based Supervision

The Agencies' IT examination process is based on the concept of ongoing, risk-based supervision. This includes the identification and selection of TSPs warranting interagency supervision and the development of a risk-based supervisory strategy for each of these entities. This approach provides for examination coverage of selected TSPs, including core application processors, electronic funds transfer switches, Internet banking providers, item processors, managed security servicers, and data storage servicers. ^[12]

The examinations of TSPs focus on the following underlying risk issues that affect the client financial institutions or the institutions' customers:

- Management of technology. The planning and oversight of technology resources and

services, ensuring they support the strategic goals and objectives of the TSP and its serviced financial institutions.

- Integrity of data. The accuracy and reliability of automated information processes and associated management information systems.
- Confidentiality of information. The protection of information from intentional or inadvertent disclosure to unauthorized individuals.
- Availability of services. The resilience of the TSP, including effective disaster recovery, business continuity plans, and adherence to service-level agreements.
- Compliance. TSPs are expected to provide services to client financial institutions to help them comply with applicable laws, rules, regulations, and policies.
- Financial stability. The maintenance of sufficient capital and liquidity to support ongoing operations and the ability to generate profit to ensure future viability. Financial difficulties at the TSP can negatively affect the safe and sound operations of serviced financial institutions through deteriorating quality of service, reliability of service, or adequacy of controls.

Risk-Based-Examination Priority Ranking

The Agencies use the Risk-Based-Examination Priority Ranking Program (RB-EBR) in determining the overall level of risk a TSP presents to its client financial institutions. The Agencies also use the RB-EPRP to prioritize and establish the frequency of TSP examinations. The RB-EPRP ranks TSPs based on the risk their business lines, controls, and risk management processes present to their client financial institutions.

Uniform Rating System for Information Technology

The Agencies use the Uniform Rating System for Information Technology (URSIT) to uniformly assess and rate IT-related risks of financial institutions and their TSPs. The primary purpose of this rating system is to evaluate the examined institution's overall risk exposure and risk management performance and determine the degree of supervisory attention necessary to ensure that weaknesses are addressed and risks are properly managed. The assigned rating determines the degree of supervisory attention necessary.

The URSIT is based on a risk evaluation of four critical components: Audit, Management, Development and Acquisition, and Support and Delivery. The ratings assigned to these

individual components are used to quantify the overall effectiveness of the institution's IT risk management practices and condition. Examiners evaluate the functions identified within each component to assess the institution's ability to identify, measure, monitor, and control IT risks. The overall performance of IT within a financial institution or TSP is reflected by a composite rating. Please refer to Appendix A for additional information on composite and component URSIT ratings.

Frequency of Examinations

All TSPs that the Agencies supervise receive an examination sufficient in scope to assign or update the URSIT during each examination cycle. The number and frequency of supervisory activities conducted during the examination cycle varies depending on the risk profile of the TSP as established by the RB-EPRP and the URSIT. TSPs with a higher risk ranking are subject to more frequent and extensive examinations. The examination cycles, based on the assigned URSIT and Examination Priority Ranking (EPR), are as follows:

- "A" ranking: 24-month examination cycle
- "B" ranking: 36-month examination cycle
- "C" ranking: 48-month examination cycle

As part of the supervision of a TSP, examiners can conduct interim supervisory reviews or unscheduled site or service examinations for areas of evolving supervisory interest or concern. The number and frequency of interim supervisory reviews conducted during an examination cycle are based on the level of risk identified by the CPC team. All examined TSPs must receive at least one interim supervisory review during each examination cycle.

Examinations are conducted jointly according to schedules agreed upon by the participating Agencies. When joint examinations cannot be scheduled, one or more Agencies may be designated to perform the examination on behalf of all interested Agencies. If, however, the TSP's overall condition is determined to be less than satisfactory, the Agencies make a special effort to ensure subsequent examinations are conducted on a joint basis until the TSP's overall condition is satisfactory.

Risks Associated With TSPs

Operational risk is the primary risk associated with TSP processing. Operational risk may arise from inadequate or failed internal processes or systems, the misconduct or errors of people, and adverse external events. Operational risk also may affect other risks, such as credit, interest rate, liquidity, price, compliance, or strategic.

- Strategic risk. Inaccurate information from TSPs can cause the management of serviced financial institutions to make poor strategic decisions.
- Compliance (legal) risk. Inaccurate or untimely data related to consumer compliance disclosures or unauthorized disclosure of confidential customer information could expose financial institutions to civil money penalties or litigation. For example, TSPs often agree to keep disclosures or calculations in compliance with banking regulations, and their failure to track regulatory changes could increase compliance risk for their serviced financial institutions.
- Credit, interest rate, liquidity, and price (market) risks. Processing errors related to investment income or repayment assumptions could increase these risks of serviced financial institutions.

The quantity of operational risk at a TSP is the level or volume of risk that exists. The quality of operational risk management is an assessment of how well risks are identified, measured, controlled, and monitored.

Risk Management

The Agencies recognize that management practices, particularly as they relate to risk management, vary considerably among financial institutions and TSPs, depending on their size and sophistication, the nature and complexity of their business activities, and their risk profile. Accordingly, the Agencies also recognize that for less complex information systems environments, detailed or highly formalized systems and controls may not be required.

Financial institutions should oversee their TSPs and perform due diligence in selecting their third-party servicers, including a review of the risk management systems used by the TSPs. Such reviews should include measures taken by the TSPs to protect information about financial institutions' customers. Financial institutions also should monitor their TSPs to confirm the TSPs implement adequate security measures. As part of their monitoring activities, financial institutions should review such information as TSP service-level reports, audits, third-party reviews, internal control testing results, and other equivalent evaluations of their TSPs.

If a TSP has weak risk management controls requiring corrective action, the TSP's serviced institutions may also have to take remedial actions because the institutions have the ultimate responsibility to properly manage their risks. Management of TSPs and financial institutions should monitor changes in laws, regulations, and guidance that affects the services provided to financial institutions.

Audit and Internal Controls

Well-planned, properly structured audit programs are essential to strong risk management and effective internal control systems. Effective internal and external audit programs are also a critical defense against fraud and provide vital information to the board of directors about the effectiveness of internal controls systems. The Agencies encourage the use of well-supported risk-based auditing. Through this process, the board, management, and auditors can focus their resources on areas of greatest risk.

TSPs with effective risk-based auditing programs typically require less examination work by the Agencies. Additional guidance on what examiners review in information systems, audit, and internal control functions can be found in the "Audit" and "Management" booklets of the IT Handbook.

Report of Examination

The Agencies have a uniform Report of Examination (ROE) format for IT examinations of financial institutions and their TSPs. The ROE includes an "Open Section," which contains all significant findings and conclusions, and a "Confidential Section," which includes information solely for the Agencies' internal use.

ROE Distribution

The ROE is generally distributed to three primary groups: the Agencies, the supervised TSP, and the serviced financial institutions. ^[13]

All ROEs of a TSP, including those of stand-alone, subsidiary data centers, are directed to the board of directors, a committee thereof, or senior management of the TSP. The ROE is accompanied by a letter to the board, which includes the assigned URSIT and a reminder to recipients of the confidential nature of the letter and ROE.

The Agencies distribute to serviced financial institutions, either automatically or upon request, the Open section of a TSP ROE. Reports are automatically distributed when the TSP receives a composite URSIT rating of 4 or 5. A serviced financial institution can request a copy of the ROE from the institution's primary regulator and must demonstrate that it had a valid and current contract with the TSP as of the date of the examination.

The ROE is the joint property of the Agencies and is provided to the TSP and its client regulated financial institutions for their internal, confidential use. Under no circumstances shall any recipient of the ROE disclose or make public the ROE or any portion thereof. Unauthorized disclosure of any of the contents of the ROE is subject to the penalties in 18 USC 641.

Customer List

As part of the supervisory process, the Lead CPC obtains from the TSPs a list of

regulated financial institutions with which the servicer has entered into a contractual arrangement. The customer list, which is to be provided upon request (generally, during examinations, or, at a minimum, once each examination cycle), must be accurate, complete, and in a specified format that identifies the services being provided to each client financial institution.

The customer lists allow the Agencies to identify and validate regulated financial institutions that are entitled to copies of the ROEs produced on the TSPs. Additionally, the customer lists give the Agencies information to determine the scope of regulated financial institutions that may be affected by the operations of a TSP.

Endnotes

[1]	12 USC 1464(d)(7), 1867(c)(1). The Consumer Financial Protection Bureau (CFPB) has authority as described in 12 USC 5514(e), 5515(d), and 5516(e). See CFPB Bulletin 2012-03 (Apr. 13, 2012), available at http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf . The National Credit Union Administration (NCUA) does not have independent regulatory authority over TSPs. The Agencies coordinate the interagency programs to supervise third-party servicers through the Federal Financial Institutions Examination Council (FFIEC).
[2]	The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. The FFIEC members include the FRS, the FDIC, the NCUA, the OCC, the State Liaison Committee (SLC), and the CFPB.
[3]	The term TSP generally includes independent third parties, joint venture/limited liability corporations, and bank and credit union service corporations that provide processing services to financial institutions supervised by the FFIEC member Agencies.
[4]	Additional information on appropriate due diligence and oversight of outsourced technology services and third-party relationships can be found in the FFIEC Information Technology Examination Handbook, (IT Handbook), "Outsourcing Technology Services" booklet.
[5]	For example, national banks, state member banks, state non-member banks.
[6]	As defined in 12 U.S.C. 1861(b)(2).
[7]	12 U.S.C. 1861(b)(8).
[8]	The examination cycle is based on the assigned Examination Priority Ranking derived through the RB-EPRP. Examination cycles are 24, 36, or 48 months.
[9]	An application or system is mission-critical if it is vital to the successful continuance of a core business activity. An application also may be mission-critical if it interfaces with a designated mission-critical system. Products of software vendors also may be mission-critical.
[10]	The FFIEC TFOS coordinates and oversees matters relating to safety and soundness supervision and examination of depository institutions. It provides a forum for the member agencies that supervise banks, thrifts, and credit unions to promote quality, consistency, and effectiveness in examination and supervisory practices and to reduce unnecessary regulatory burden on those institutions. The TFOS has one standing subcommittee, the Information Technology (IT) Subcommittee.
[11]	Agencies that do not have sufficient regulatory interest in a TSP may choose not to have a designated CPC.

[12] This list is representative of some types of service providers that may be examined and is not intended to be all-inclusive.

[13] The Agencies also provide CFPB with access to service provider examination reports in accordance with the provisions of section 1022(c)(6)(B)(i) of the Dodd- Frank Wall Street Reform and Consumer Protection Act. See 12 USC 5512(c)(6) (B)(i)

Appendix A: URSIT

Introduction

Use of Composite Ratings

Each TSP examined for IT is assigned a summary or composite rating based on the overall results of the evaluation. The IT composite rating and each component rating are based on a scale of 1 through 5 in ascending order of supervisory concern, with 1 representing the highest rating and least degree of concern; and 5, the lowest rating and highest degree of concern.

The first step in developing an IT composite rating for an organization is the assignment of a performance rating to the individual Audit, Management, Development and Acquisition, and Support and Delivery (AMDS) components. The evaluation of each of these components, their interrelationships, and relative importance is the basis for the composite rating. A direct relationship exists between the composite rating and the individual AMDS component performance ratings. However, the composite rating is not an arithmetic average of the individual components. An arithmetic approach does not reflect the actual condition of IT when using a risk-focused approach. A poor rating in one component may heavily influence the overall composite rating for an institution.

A principal purpose of the composite rating is to identify those financial institutions and TSPs that pose an inordinate amount of information technology risk and merit special supervisory attention. Thus, individual risk exposures that more explicitly affect the viability of the organization or its customers should be given more weight in the composite rating.

The AIC of the TSP examination should notify other FFIEC Agencies' supervisory offices prior to issuing URSIT composite ratings of 3, 4, or 5 or engaging in informal or formal enforcement actions.

Use of Component Ratings

Each performance or component rating also ranges from 1 through 5, with 1 representing the highest or best, and 5, the lowest rating or worst. Each functional area of activity (audit, management, development and acquisition, and support and delivery) must be evaluated to determine its individual performance rating.

Composite Ratings Definitions

Composite - 1

Financial institutions and service providers rated composite 1 exhibit strong performance in every respect and generally have components rated 1 or 2. Weaknesses in IT are minor in nature and are easily corrected during the normal course of business. Risk management processes provide a comprehensive program to identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are well defined and fully integrated throughout the organization. This allows management to quickly adapt to changing market, business, and technology needs of the entity. Management identifies weaknesses promptly and takes appropriate corrective action to resolve audit and regulatory concerns. The financial condition of the service provider is strong and overall performance shows no cause for supervisory concern.

Composite - 2

Financial institutions and service providers rated composite 2 exhibit safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes, or system development. Generally, senior management corrects weaknesses in the normal course of business. Risk management processes adequately identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are defined but may require clarification, better coordination, or improved communication throughout the organization. As a result, management anticipates, but responds less quickly, to changes in market, business, and technological needs of the entity. Management normally identifies weaknesses and takes appropriate corrective action. However, greater reliance is placed on audit and regulatory intervention to identify and resolve concerns. The financial condition of the service provider is acceptable and while internal control weaknesses may exist, there are no significant supervisory concerns. As a result, supervisory action is informal and limited.

Composite - 3

Financial institutions and service providers rated composite 3 exhibits some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe. If weaknesses persist, further deterioration in the condition and performance of the institution or service provider is likely. Risk management processes may not effectively identify risks and may not be appropriate for the size, complexity, or risk profile of the entity. Strategic plans are vaguely defined and may not provide adequate direction for IT initiatives. As a result, management often has difficulty responding to changes in business, market, and technological needs of the entity. Self-assessment practices are weak and are generally reactive to audit and regulatory exceptions. Repeat concerns may exist indicating that management may lack the ability or willingness to resolve concerns. The financial condition of the service provider may be weak and/or negative trends may be evident. While financial or operational failure is unlikely, increased supervision is necessary. Formal or informal supervisory action may be necessary to secure corrective action.

Composite - 4

Financial institutions and service providers rated composite 4 operate in an unsafe and unsound environment that may impair the future viability of the entity. Operating weaknesses are indicative of serious managerial deficiencies. Risk management processes inadequately identify and monitor risk, and practices are not appropriate given the size, complexity, and risk profile of the entity. Strategic plans are poorly defined and not coordinated or communicated throughout the organization. As a result, management and the board are not committed to, or may be incapable of ensuring, that technological needs are met. Management does not perform self-assessments and demonstrates an inability or unwillingness to correct audit and regulatory concerns. The financial condition of the service provider is severely impaired or deteriorating. Failure of the financial institution or service provider may be likely unless IT problems are remedied. Close supervisory attention is necessary and, in most cases, formal enforcement action is warranted.

Composite - 5

Financial institutions and service providers rated composite 5 exhibit critically deficient operating performances and are in need of immediate remedial action. Operational problems and serious weaknesses may exist throughout the organization. Risk management processes are severely deficient and provide management little or no perception of risk relative to the size, complexity, and risk profile of the entity. Strategic plans do not exist or are ineffective, and management and the board provide little or no direction for IT initiatives. As a result, management is unaware of, or inattentive to, technological needs of the entity. Management is unwilling or incapable of correcting audit and regulatory concerns. The financial condition of the service provider is poor and failure is highly probable due to poor operating performance or financial instability. Ongoing supervisory attention is necessary.

Component Ratings Definitions

Each performance or component rating also ranges from 1 through 5, with 1 representing the highest and 5 the lowest rating. Each functional area of activity (audit, management, development and acquisition, and support and delivery) must be evaluated to determine its individual performance rating.

Each performance or component rating is described as follows:

Component 1-Strong performance: Performance that is significantly higher than average.

Component 2- Satisfactory performance: Performance that is average or slightly above and that provides adequately for the safe and sound operation of the data center.

Component 3-Less than satisfactory: Performance that exhibits some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe.

Component 4-Deficient: Performance that is in an unsafe and unsound environment that may impair the future viability of the entity.

Component 5-Critically deficient: Performance that is critically deficient and in need of immediate remedial attention. The financial condition of the service provider is poor and failure is highly probable due to poor operating performance or financial instability.

Component Rating Areas of Coverage

Audit

Financial institutions and service providers are expected to provide independent assessments of their exposure to risks and the quality of internal controls associated with the acquisition, implementation, and use of information technology. Audit practices should address the IT risk exposures throughout the institution and its service provider(s) in the areas of user and data center operations, client/server architecture, local and wide-area networks, telecommunications, information security, electronic data interchange, systems development, and contingency planning. This rating should reflect the adequacy of the organization's overall IT audit program, including the internal and external audit's abilities to detect and report significant risks to management and the board of directors on a timely basis. It should also reflect the internal and external auditor's capability to promote a safe, sound and effective operation.

The performance of audit is rated based upon an assessment of factors, such as:

- The level of independence maintained by audit and the quality of the oversight and support provided by the board of directors and management;
- The adequacy of audit's risk analysis methodology used to prioritize the allocation of audit resources and to formulate the audit schedule;
- The scope, frequency, accuracy, and timeliness of internal and external audit reports;
- The extent of audit participation in application development, acquisition, and testing, to ensure the effectiveness of internal controls and audit trails;
- The adequacy of the overall audit plan in providing appropriate coverage of IT risks;
- The auditor's adherence to codes of ethics and professional audit standards;
- The qualifications of the auditor, staff succession, and continued development through training;
- The existence of timely and formal follow-up and reporting on management's resolution of identified problems or weaknesses; and
- The quality and effectiveness of internal and external audit activity as it relates to IT controls.

Ratings

- A rating of 1 indicates strong audit performance. Audit independently identifies and reports weaknesses and risks to the board of directors or its audit committee in a thorough and timely manner. Outstanding audit issues are monitored until resolved. Risk analysis ensures that audit plans address all significant IT operations, procurement, and development activities with appropriate scope and frequency. Audit work is performed in accordance with professional auditing standards and report content is timely, constructive, accurate, and complete. Because audit is strong, examiners may place substantial reliance on audit results.
- A rating of 2 indicates satisfactory audit performance. Audit independently identifies and reports weaknesses and risks to the board of directors or audit committee, but reports may be less timely. Significant outstanding audit issues are monitored until resolved. Risk analysis ensures that audit plans address all significant IT operations, procurement, and development activities; however, minor concerns may be noted with the scope or frequency. Audit work is performed in accordance with professional auditing standards; however, minor or infrequent problems may arise with the timeliness, completeness, and accuracy of reports. Because audit is satisfactory, examiners may rely on audit results but because minor concerns exist, examiners may need to expand verification procedures in certain situations.
- A rating of 3 indicates less than satisfactory audit performance. Audit identifies and reports weaknesses and risks; however, independence may be compromised and reports presented to the board or audit committee may be less than satisfactory in content and timeliness. Outstanding audit issues may not be adequately monitored. Risk analysis is less than satisfactory. As a result, the audit plan may not provide sufficient audit scope or frequency for IT operations, procurement, and development activities. Audit work is generally performed in accordance with professional auditing standards; however, occasional problems may be noted with the timeliness, completeness, or accuracy of reports. Because audit is less than satisfactory, examiners must use caution if they rely on the audit results.
- A rating of 4 indicates deficient audit performance. Audit may identify weaknesses and risks but it may not independently report to the board or audit committee and report content may be inadequate. Outstanding audit issues may not be adequately monitored and resolved. Risk analysis is deficient. As a result, the audit plan does not provide adequate audit scope or frequency for IT operations, procurement, and development activities. Audit work is often inconsistent with professional auditing standards and the timeliness, accuracy, and completeness of reports is unacceptable. Because audit is deficient, examiners cannot rely on audit results.
- A rating of 5 indicates critically deficient audit performance. If an audit function exists, it lacks sufficient independence and, as a result, does not identify and report

weaknesses or risks to the board or audit committee. Outstanding audit issues are not tracked and no follow-up is performed to monitor their resolution. Risk analysis is critically deficient. As a result, the audit plan is ineffective and provides inappropriate audit scope and frequency for IT operations, procurement, and development activities. Audit work is not performed in accordance with professional auditing standards and major deficiencies are noted regarding the timeliness, accuracy, and completeness of audit reports. Because audit is critically deficient, examiners cannot rely on audit results.

Management

This rating reflects the abilities of the board and management as they apply to all aspects of IT acquisition, development, and operations. Management practices may need to address some or all of the following IT-related risks: strategic planning, quality assurance, project management, risk assessment, infrastructure and architecture, end-user computing, contract administration of third-party service providers, organization and human resources, and regulatory and legal compliance. Generally, directors need not be actively involved in day-to-day operations; however, they must provide clear guidance regarding acceptable risk exposure levels and ensure that appropriate policies, procedures, and practices have been established. Sound management practices are demonstrated through active oversight by the board of directors and management, competent personnel, sound IT plans, adequate policies and standards, an effective control environment, and risk monitoring. This rating should reflect the ability of the board and management as it applies to all aspects of IT operations. The performance of management and the quality of risk management are rated based upon an assessment of factors such as:

- The level and quality of oversight and support of the IT activities by the board of directors and management;
- The ability of management to plan for and initiate new activities or products in response to information needs and to address risks that may arise from changing business conditions;
- The ability of management to provide information reports necessary for informed planning and decision making in an effective and efficient manner;
- The adequacy of, and conformance with, internal policies and controls addressing the IT operations and risks of significant business activities;
- The effectiveness of risk monitoring systems;
- The timeliness of corrective action for reported and known problems;
- The level of awareness of and compliance with laws and regulations;
- The level of planning for management succession;
- The ability of management to monitor the services delivered and to measure the organization's progress toward identified goals in an effective and efficient manner;

- The adequacy of contracts and management's ability to monitor relationships with third-party servicers;
- The adequacy of strategic planning and risk management practices to identify, measure, monitor, and control risks, including management's ability to perform self-assessments; and
- The ability of management to identify, measure, monitor, and control risks and to address emerging information technology needs and solutions.
- In addition to the above, factors such as the following are included in the assessment of management at servicer providers:
- The financial condition and ongoing viability of the entity;
- The impact of external and internal trends and other factors on the ability of the entity to support continued servicing of client financial institutions; and
- The propriety of contractual terms and plans.

Ratings

- A rating of 1 indicates strong performance by management and the board. Effective risk management practices are in place to guide IT activities, and risks are consistently and effectively identified, measured, controlled, and monitored. Management immediately resolves audit and regulatory concerns to ensure sound operations. Written technology plans, policies and procedures, and standards are thorough and properly reflect the complexity of the IT environment. They have been formally adopted, communicated, and enforced throughout the organization. IT systems provide accurate, timely reports to management. These reports serve as the basis of major decisions and as an effective performance-monitoring tool. Outsourcing arrangements are based on comprehensive planning; routine management supervision sustains an appropriate level of control over vendor contracts, performance, and services provided. Management and the board have demonstrated the ability to promptly and successfully address existing IT problems and potential risks.
- A rating of 2 indicates satisfactory performance by management and the board. Adequate risk management practices are in place and guide IT activities. Significant IT risks are identified, measured, monitored, and controlled; however, risk management processes may be less structured or inconsistently applied and modest weaknesses exist. Management routinely resolves audit and regulatory concerns to ensure effective and sound operations; however, corrective actions may not always be implemented in a timely manner. Technology plans, policies, procedures, and standards are adequate and are formally adopted. However, minor weaknesses may exist in management's ability to communicate and enforce them throughout the organization. IT systems provide quality reports to management that serve as a

basis for major decisions and a tool for performance planning and monitoring. Isolated or temporary problems with timeliness, accuracy, or consistency of reports may exist. Outsourcing arrangements are adequately planned and controlled by management, and provide for a general understanding of vendor contracts, performance standards, and services provided. Management and the board have demonstrated the ability to address existing IT problems and risks successfully.

- A rating of 3 indicates less than satisfactory performance by management and the board. Risk management practices may be weak and offer limited guidance for IT activities. Most IT risks are generally identified; however, processes to measure and monitor risk may be flawed. As a result, management's ability to control risk is less than satisfactory. Regulatory and audit concerns may be addressed, but time frames are often excessive and the corrective action taken may be inappropriate. Management may be unwilling or incapable of addressing deficiencies. Technology plans, policies, procedures, and standards exist, but may be incomplete. They may not be formally adopted, effectively communicated, or enforced throughout the organization. IT systems provide requested reports to management, but periodic problems with accuracy, consistency, and timeliness lessen the reliability and usefulness of reports and may adversely affect decision making and performance monitoring. Outsourcing arrangements may be entered into without thorough planning. Management may provide only cursory supervision that limits its understanding of vendor contracts, performance standards, and services provided. Management and the board may not be capable of addressing existing IT problems and risks, as evidenced by untimely corrective actions for outstanding IT problems.
- A rating of 4 indicates deficient performance by management and the board. Risk management practices are inadequate and do not provide sufficient guidance for IT activities. Critical IT risks are not properly identified, and processes to measure and monitor risks are not properly identified, and processes to measure and monitor risks are deficient. As a result, management may not be aware of and is unable to control risks. Management may be unwilling or incapable of addressing audit and regulatory deficiencies in an effective and timely manner. Technology plans, policies and procedures, and standards are inadequate, have not been formally adopted or effectively communicated throughout the organization, and management does not effectively enforce them. IT systems do not routinely provide management with accurate, consistent, and reliable reports, thus contributing to ineffective performance monitoring or flawed decision-making. Outstanding arrangements may be entered into without planning or analysis, and management may provide little or no supervision of vendor contracts, performance standards, or services provided. Management and the board are unable to address existing IT problems and risks, as evidenced by ineffective actions and longstanding IT weaknesses. Strengthening of management and its processes is necessary. The financial condition of the service provider may threaten its viability.
- A rating of 5 indicates critically deficient performance by management and the board. Risk management practices are severely flawed and provide inadequate guidance for IT activities. Critical IT risks are not identified, and processes to measure and monitor risks do not exist, or are not effective. Management's inability to control risk may threaten the continued viability of the institution or service provider.

Management is unable or unwilling to correct audit and regulatory identified deficiencies and immediate action by the board is required to preserve the viability of the institution or service provider. If they exist, technology plans, policies, procedures, and standards are critically deficient. Because of systemic problems, IT systems do not produce management reports that are accurate, timely, or relevant. Outsourcing arrangements may have been entered into without management planning or analysis, resulting in significant losses to the financial institution or ineffective vendor services. The financial condition of the service provider presents an imminent threat to its viability.

Development and Acquisition

This rating reflects an organization's ability to identify, acquire, install, and maintain appropriate information technology solutions. Management practices may need to address all or parts of the business process for implementing any kind of change to the hardware or software used. These business processes include an institution's or service provider's purchase of hardware or software, development and programming performed by the institution or service provider, purchase of services from independent vendors or affiliated data centers, or a combination of these activities. The business process is defined as all phases taken to implement a change including researching alternatives available, choosing an appropriate option for the organization as a whole, converting to the new system, or integrating the new system with existing systems. This rating reflects the adequacy of the institution's systems development methodology and related risk technology. This rating also reflects the board's and management's ability to enhance and replace information technology prudently in a controlled environment. The performance of systems development and acquisition and related risk management practice is rated based upon an assessment of factors such as:

- The level and quality of oversight and support of systems development and acquisition activities by senior management and the board of directors;
- The adequacy of the organizational and management structures to establish accountability and responsibility for IT systems and technology initiatives;
- The volume, nature, and extent of risk exposure to the financial institution in the area of systems development and acquisition;
- The adequacy of the institution's system development life cycle (SDLC) and programming standards;
- The quality of project management programs and practices which are followed by developers, operators, executive management/owners, independent vendors or affiliated servicers, and end users;
- The independence of the quality assurance function and the adequacy of controls over program changes;
- The quality and thoroughness of system documentation;

- The integrity and security of the network, system, and application software;
- The development of information technology solutions that meet the needs of end users; and
- The extent of end user involvement in the system development process.
- In addition to the above, factors such as the following are included in the assessment of development and acquisition at service providers:
 - The quality of software releases and documentation; and
 - The adequacy of training provided to clients.

Ratings

- A rating of 1 indicates strong systems development, acquisition, implementation, and change management performance. Management and the board routinely demonstrate successfully the ability to identify and implement appropriate IT solutions while effectively managing risk. Project management techniques and the SDLC are fully effective and supported by written policies, procedures, and project controls that consistently result in timely and efficient project completion. An independent quality assurance function provides strong controls over testing and program change management. Technology solutions consistently meet end-user needs. No significant weaknesses or problems exist.
- A rating of 2 indicates satisfactory systems development, acquisition, implementation, and change management performance. Management and the board frequently demonstrate the ability to identify and implement appropriate IT solutions while managing risk. Project management and the SDLC are generally effective; however, weaknesses may exist that result in minor project delays or cost overruns. An independent quality assurance function provides adequate supervision of testing and program change management, but minor weaknesses may exist. Technology solutions meet end-user needs. However, minor enhancements may be necessary to meet original user expectations. Weaknesses may exist; however, they are not significant and they are easily corrected in the normal course of business.
- A rating of 3 indicates less than satisfactory systems development, acquisition, implementation, and change management performance. Management and the board may often be unsuccessful in identifying and implementing appropriate IT solutions; therefore, unwarranted risk exposure may exist. Project management techniques and the SDLC are weak and may result in frequent project delays, backlogs or significant cost overruns. The quality assurance function may not be independent of the programming function, which may adversely impact the integrity of testing, and program change management. Technology solutions generally meet end-user

needs, but often require an inordinate level of change after implementation. Because of weaknesses, significant problems may arise that could result in disruption to operations or significant losses.

- A rating of 4 indicates deficient systems development, acquisition, implementation, and change management performance. Management and the board may be unable to identify and implement appropriate IT solutions and do not effectively manage risk. Project management techniques and the SDLC are ineffective and may result in severe project delays and cost overruns. The quality assurance function is not fully effective and may not provide independent or comprehensive review of testing controls or program change management. Technology solutions may not meet the critical needs of the organization. Problems and significant risks exist that require immediate action by the board and management to preserve the soundness of the institution.
- A rating of 5 indicates critically deficient systems development, acquisition, implementation, and change-management performance. Management and the board appear to be incapable of identifying and implementing appropriate information technology solutions. If they exist, project management techniques and the SDLC are critically deficient and provide little or no direction for development of systems or technology projects. The quality assurance function is severely deficient or not present and unidentified problems in testing and program change management have caused significant IT risks. Technology solutions do not meet the needs of the organization. Serious problems and significant risks exist that raise concern for the financial institution or service provider's ongoing viability.

Support and Delivery

This rating reflects an organization's ability to provide technology services in a secure environment. It reflects not only the condition of IT operations but also factors such as reliability, security, and integrity, which may affect the quality of the information delivery system. The factors include customer support and training, and the ability to manage problems and incidents, operations, system performance, capacity planning, and facility and data management. Risk management practices should promote effective, safe, and sound IT operations that ensure the continuity of operations and the reliability and availability of data. The scope of this component rating includes operational risks throughout the organization and service providers.

The rating of IT support and delivery is based on a review and assessment of requirements such as:

- The ability to provide a level of service that meets the requirements of the business;
- The adequacy of security policies, procedures, and practices in all units and at all levels of the financial institution and service providers;

- The adequacy of data controls over preparation, input, processing, and output;
- The adequacy of corporate contingency planning and business resumption for data centers, networks, service providers and business units;
- The quality of processes or programs that monitor capacity and performance;
- The adequacy of controls and the ability to monitor controls at service providers;
- The quality of assistance provided to users, including the ability to handle problems;
- The adequacy of operating policies, procedures, and manuals;
- The quality of physical and logical security, including the privacy of data;
- The adequacy of firewall architectures and the security of connections with public networks.
- In addition to the above, factors such as the following are included in the assessment of support and delivery at service providers:
 - The adequacy of customer service provided to clients; and
 - The ability of the entity to provide and maintain service level performance that meets the requirements of the client.

Ratings

- A rating of 1 indicates strong IT support and delivery performance. The organization provides technology services that are reliable and consistent. Service levels adhere to well-defined service-level agreements and routinely meet or exceed business requirements. A comprehensive corporate contingency and business resumption plan is in place. Annual contingency plan testing and updating is performed; and, critical systems and applications are recovered within acceptable time frames. A formal written data security policy and awareness program is communicated and enforced throughout the organization. The logical and physical security for all IT platforms is closely monitored, and security incidents and weaknesses are identified and quickly corrected. Relationships with third-party service providers are closely monitored. IT operations are highly reliable, and risk exposure is successfully identified and controlled.
- A rating of 2 indicates satisfactory IT support and delivery performance. The organization provides technology services that are generally reliable and consistent; however, minor discrepancies in service levels may occur. Service performance adheres to service agreements and meets business requirements. A corporate contingency and business resumption plan is in place, but minor enhancements may be necessary. Annual plan testing and updating is performed and minor problems may occur when recovering systems or applications. A written data security policy is

in place but may require improvement to ensure its adequacy. The policy is generally enforced and communicated throughout the organization, e.g., through a security awareness program. The logical and physical security for critical IT platforms is satisfactory. Systems are monitored, and security incidents and weaknesses are identified and resolved within reasonable time frames. Relationships with third-party service providers are monitored. Critical IT operations are reliable and risk exposure is reasonably identified and controlled.

- A rating of 3 indicates that the performance of IT support and delivery is less than satisfactory and needs improvement. The organization provides technology services that may not be reliable or consistent. As a result, service levels periodically do not adhere to service-level agreements or meet business requirements. A corporate contingency and business resumption plan is in place but may not be considered comprehensive. The plan is periodically tested; however, the recovery of critical systems and applications is frequently unsuccessful. A data security policy exists; however, it may not be strictly enforced or communicated throughout the organization. The logical and physical security for critical IT platforms is less than satisfactory. Systems are monitored; however, security incidents and weaknesses may not be resolved in a timely manner. Relationships with third-party service providers may not be adequately monitored. IT operations are not acceptable and unwarranted risk exposures exist. If not corrected, weaknesses could cause performance degradation or disruption to operations.
- A rating of 4 indicates deficient IT support and delivery performance. The organization provides technology services that are unreliable and inconsistent. Service-level agreements are poorly defined and service performance usually fails to meet business requirements. A corporate contingency and business resumption plan may exist, but its content is critically deficient. If contingency testing is performed, management is typically unable to recover critical systems and applications. A data security policy may not exist. As a result, serious supervisory concerns over security and the integrity of data exist. The logical and physical security for critical IT platforms is deficient. Systems may be monitored, but security incidents and weaknesses are not successfully identified or resolved. Relationships with third-party service providers are not monitored. IT operations are not reliable and significant risk exposure exists. Degradation in performance is evident and frequent disruption in operations has occurred.
- A rating of 5 indicates critically deficient IT support and delivery performance. The organization provides technology services that are not reliable or consistent. Service-level agreements do not exist and service performance does not meet business requirements. A corporate contingency and business resumption plan does not exist. Contingency testing is not performed and management has not demonstrated the ability to recover critical systems and applications. A data security policy does not exist, and a serious threat to the organization's security and data integrity exists. The logical and physical security for critical IT platforms is inadequate, and management does not monitor systems for security incidents and weaknesses. Relationships with third-party service providers are not monitored, and the viability of a service provider may be in jeopardy. IT operations are severely deficient, and the seriousness of weaknesses could cause failure of the financial institution or service provider if not

addressed.



Federal Financial Institutions Examination Council

FFIEC

Wholesale Payment
Systems

JULY 2004

WPS

**IT EXAMINATION
HANDBOOK**

TABLE OF CONTENTS

INTRODUCTION	1
INTERBANK PAYMENT AND MESSAGING SYSTEMS.....	3
Fedwire and Clearing House Interbank Payments System (CHIPS)	3
Fedwire Funds Service	4
CHIPS.....	5
Other Clearinghouse, Settlement, and Messaging Systems.....	7
National Settlement Service (NSS).....	7
Society for Worldwide Interbank Financial Telecommunication (SWIFT)....	8
Telex-based Messaging Systems	8
Continuous Linked Settlement (CLS) Bank	9
SECURITIES SETTLEMENT SYSTEMS	11
U.S. Government Securities	11
Fixed Income Clearing Corporation (FICC).....	12
Fedwire Securities Service.....	13
Corporate and Municipal Securities	14
National Securities Clearing Corporation (NSCC).....	14
Depository Trust Company (DTC)	15
INTRABANK PAYMENT AND MESSAGING SYSTEMS	16
Internally Developed and Off-The-Shelf Funds Transfer Systems.....	16
Payment Messaging Systems.....	17
In-house Terminals	18
Non-automated Payment Order Origination.....	18
Funds Transfer Operations (Wire Room)	18
Computer and Network Operations Supporting Funds Transfer	20
WHOLESALE PAYMENT SYSTEMS RISK MANAGEMENT	21
Payments System Risk (PSR) Policy	22
Strategic Risk.....	23
Credit Risk	23
Customer Daylight Overdrafts	24

Settlement Risk.....	25
Liquidity Risk.....	26
Legal (Compliance) Risk.....	27
Operational (Transaction) Risk	30
Internal and Operational Controls	31
Audit.....	32
Information Security	33
Business Continuity Planning (BCP).....	33
Vendor and Third-Party Management.....	33
APPENDIX A: EXAMINATION PROCEDURES.....	A-1
APPENDIX B: GLOSSARY	B-1
APPENDIX C: LAWS, REGULATIONS AND GUIDANCE.....	C-1
Regulations	C-1
APPENDIX D: LEGAL FRAMEWORK FOR INTERBANK PAYMENT SYSTEMS.....	D-1
APPENDIX E: FEDERAL RESERVE BOARD PAYMENT SYSTEM RISK POLICY: DAYLIGHT OVERDRAFTS	E-1
APPENDIX F: PAYMENT SYSTEM RESILIENCY.....	F-1

INTRODUCTION

This Wholesale Payment Systems Booklet (Booklet) is one of several that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook (IT Handbook). It provides guidance to examiners and financial institution management regarding the risks and risk-management practices when originating and transmitting large-value payments. It replaces and rescinds Chapter 18 of the 1996 Information Systems Examination Handbook.

This booklet is organized into the following four sections describing the various aspects of wholesale payment systems, followed by examination procedures, a glossary, a discussion of the legal framework for interbank payment systems, a discussion of the Federal Reserve Board's Payments System Risk (PSR) Policy, and a discussion of the "Interagency Paper on Sound Practices to Strengthen the Resiliency of the U.S. Financial System." Management action summaries are included in each of the four sections providing a snapshot of the risks and risk management practices described in the text.

- *Interbank Payment and Messaging Systems* – The first section includes a discussion of interbank funds transfer and messaging systems, and interbank clearing and settlement systems. This section concludes with a discussion of Internet-based wholesale payment systems.
- *Intrabank Payment and Messaging Systems* – The second section provides an overview of the funds transfer and messaging systems employed by typical financial institutions.
- *Securities Settlement Systems* – The third section provides an overview of the major securities markets and securities settlement systems. Securities settlement generates a large volume of wholesale payments typically processed by financial institutions. The information presented in this section describes these settlement processes. While securities settlement generally involves both the delivery of a security and the corresponding payment, this section focuses on the wholesale payments generated by these transactions, and does not cover the complete range of activities associated with securities processing, including the transfer and delivery of securities, custodial arrangements, and related trading activities.¹
- *Wholesale Payment Systems Risk Management* – The fourth section describes the risks associated with wholesale payment systems, using various risk categories, including strategic, credit, liquidity, legal/compliance, and operational/transaction risk. This

¹ For further information on these topics, refer to the Committee on Payment and Settlement Systems (CPSS) "Recommendation for Central Counterparties," at www.bis.org.

section also describes the risk management measures management should establish to mitigate the risks described.

The booklet references a number of other *IT Handbook booklets*, including the “Information Security Booklet,” “Business Continuity Planning Booklet,” “Outsourcing Technology Services Booklet,” and the “FedLine Booklet.”² In addition to describing the information technology risks and controls, the booklet also describes certain credit and liquidity risks that may be present when conducting wholesale payment services. A full review of a financial institution’s wholesale payment system environment may require the use of examiners with experience in credit, liquidity, and compliance issues and additional agency-specific examination procedures.

Examiners should use the examination procedures (detailed in Appendix A) for reviewing risks in wholesale payment systems. These procedures address services and products of varied complexity, and examiners should adjust the procedures for the scope of the examination and the size and risk profile of the institution. Examiners may use the procedures independently or in combination with procedures from other IT Handbook booklets and agency specific handbooks and guidance.

For financial institutions whose primary method for originating, transmitting, and receiving large-value payment orders is the use of the FedLine Funds Transfer (FT) application, examiners should use the “FedLine Booklet” to assess the wholesale payment systems and funds transfer environment. In addition, examiners should also review the “Legal Framework” and “PSR” discussions in Appendices D and E, respectively, if an expanded evaluation of the funds transfer operation is necessary.

² FedLine® is a registered trademark of the Federal Reserve Banks.

INTERBANK PAYMENT AND MESSAGING SYSTEMS

FEDWIRE AND CLEARING HOUSE INTERBANK PAYMENTS SYSTEM (CHIPS)

In the United States, payment and securities settlement systems consist of numerous financial intermediaries, financial services firms, and non-bank businesses that create, distribute, and process large-value payments. The bulk of the dollar value of these payments are processed electronically and are generally used to purchase, sell, or finance securities transactions; disburse or repay loans; settle real estate transactions; and make large-value, time-critical payments, such as payments for the settlement of interbank purchases and sales of federal funds, settlement of foreign exchange transactions, or other financial market transactions.

There are two primary networks for interbank, or large-value, domestic, funds transfer payment orders. The first, Fedwire® Funds Service, is operated by the Federal Reserve Banks, and is an important participant in providing interbank payment services as well as safekeeping and transfer services for U.S. government and agency securities, and mortgage-backed securities. In addition, Fedwire³ Funds Service and the Federal Reserve's National Settlement Service (NSS) are critical components used in other payment systems' settlement processes. The Clearing House Interbank Payments Company L.L.C. (CHIP Co.) operates the second, the Clearing House Interbank Payments System (CHIPS).⁴

Processing large-value funds transfers involves two key elements: clearing and settlement. Clearing is the transfer and confirmation of information between the payer (sending financial institution) and payee (receiving financial institution). Settlement is the actual transfer of funds between the payer's financial institution and the payee's financial institution. Settlement discharges the obligation of the payer financial institution to the payee financial institution with respect to the payment order. Final settlement is irrevocable and unconditional. The finality of the payment is determined by that system's rules and applicable law.

In general, payment messages may be credit transfers or debit transfers. Most large-value funds transfer systems are credit transfer systems in which both payment messages and funds move from the payer financial institution to the payee financial institution. An

³ Fedwire® is a registered service mark of the Federal Reserve Banks. See <http://www.frb services.org/> for further information on Fedwire Funds and Securities Service, and NSS.

⁴ CHIPS is a private multilateral settlement system operated by CHIP Co., a subsidiary of The Clearing House (formerly known as the New York Clearing House Association).

institution initiates a funds transfer by transmitting a payment order (a message that requests the transfer of funds to the payee). Payment order processing follows the predefined rules and operating procedures of the large-value payment system used. Typically, large-value payment system operating procedures include identification, reconciliation, and confirmation procedures necessary to process the payment orders. In some systems, financial institutions may contract with one or more third parties to help perform clearing and settlement activities on behalf of the institution.

The legal framework governing payment activity and the regulatory structure for financial institutions that provide payment services is complex.⁵ There are rules for large-value payments that are distinct from retail payments. Large-value funds transfer systems differ from retail electronic funds transfer (EFT) systems, which generally handle a large volume of low value payments including automated clearinghouse (ACH) and debit and credit card transactions at the point of sale.

FEDWIRE FUNDS SERVICE

Fedwire Funds Service is a real-time gross settlement system (RTGS) enabling participants to transmit and receive payment orders between each other and on behalf of their customers. Real-time gross settlement means that the clearing and settlement of each transaction occurs continuously during the processing day. Payment to the receiving participant (payee) over Fedwire Funds Service is final and irrevocable when the Federal Reserve Bank either credits the amount of the payment order to the receiving participant's Federal Reserve Bank reserve account or sends notice to the receiving participant, whichever is earlier.

Fedwire Funds Service participants must maintain an account with a Federal Reserve Bank. Because of this requirement, non-financial organizations are not permitted direct access to Fedwire Funds Service, although these entities may use these services indirectly as customers of deposit-taking financial institutions.⁶ Certain payment and securities settlement systems, such as CHIPS and CLS, also rely upon Fedwire Funds Service to allow participants or their correspondents to provide necessary funding.⁷

⁵See Appendix D for a discussion of the general legal framework for interbank payment systems.

⁶ Subject to the Federal Reserve Bank's and the Federal Reserve Board's risk reduction policies, where applicable, entities authorized by law, regulation, policy, or agreement to be participants include depository institutions, agencies and branches of foreign banks, member banks of the Federal Reserve System, the Treasury and any entity specifically authorized by federal statute to use the Reserve Banks as fiscal agents or depositories, entities designated by the Secretary of the Treasury, foreign central banks, foreign monetary authorities, foreign governments, and certain international organizations; and any other entities authorized by a Federal Reserve Bank to use Fedwire Funds or Security Services. See Appendix E for a discussion of the Federal Reserve Board's PSR Policy.

⁷ CHIPS and CLS also use Fedwire Funds Service for settlement services by establishing zero-balance settlement accounts to settle clearinghouse participant obligations. The Federal Reserve Bank requires participants in a net debit position to make a Fedwire Funds Service funds transfer payment to the settlement account. It then pays participants in a net credit position by means of a Fedwire Funds Service funds transfer from that settlement account. Once the Federal Reserve Bank processes these funds transfers, they are final and irrevocable.

Financial institutions sending a Fedwire Funds Service payment order irrevocably authorize their Federal Reserve Bank to debit (charge) their Federal Reserve account for the transfer amount and to give credit in the same amount to the payee. Only the originating financial institution can have funds removed from its Federal Reserve account using the Fedwire Funds Service. Depository institutions that maintain a reserve or clearing account with a Federal Reserve Bank may use Fedwire Funds Service to send payments to, or receive payments from, other account holders directly. Once the Federal Reserve Bank credits the receiving institution's account, it will not reverse the transaction at the request of the originating institution.

Financial institutions may access the Fedwire Funds Service via high-speed direct computer interface (CI), FedLine, or with off-line telephone connectivity with a Federal Reserve Bank. Financial institutions may also access certain Fedwire Funds Service inquiry information via FedLine for the Web.⁸ On-line participants, using either a CI or FedLine PC connection to Fedwire Funds Service, require no manual processing by the Federal Reserve Banks. Off-line participants provide funds transfer instructions to one of two Federal Reserve Bank customer support sites by telephone, and after authenticating the participant, the Federal Reserve Bank enters the transfer instruction into the Fedwire Funds Service system for execution. The manual processing required for off-line requests makes them more costly and suitable only for institutions processing a small number of funds transfer payment orders.

The Federal Reserve Bank's FedLine for the Web currently offers access to low-risk Federal Reserve Bank financial services. FedLine Advantage, which should begin a graduated rollout by year-end 2004, will allow depository institutions access to additional Federal Reserve financial services, including the Fedwire Funds Services and the Fedwire Securities Service, via a secure Internet Protocol (IP) gateway to Federal Reserve Bank financial services. Residing on a secure Web server, FedLine Advantage will be accessible to customer financial institutions with authenticated credentials using digital certificates.

CHIPS

CHIPS is a privately operated, real-time, multilateral, payments system typically used for large dollar payments. CHIPS is owned by financial institutions, and any banking organization with a regulated U.S. presence may become an owner and participate in the network. The payments transferred over CHIPS are often related to international interbank transactions, including the dollar payments resulting from foreign currency transactions (such as spot and currency swap contracts) and Euro placements and returns. Payment orders are also sent over CHIPS for the purpose of adjusting correspondent balances and making payments associated with commercial transactions, bank loans, and securities transactions.

⁸ By year-end 2004, customers should be able to initiate Fedwire Funds Service and Fedwire Securities Service transactions through the web via FedLine Advantage.

Since January 2001, CHIPS has been a real-time final settlement system that continuously matches, nets and settles payment orders. This system provides real-time finality for all payment orders released by CHIPS from the CHIPS queue. To achieve real-time finality, payment orders are settled on the books of CHIPS against participants' positive positions, simultaneously offset by incoming payment orders, or both. This process is dependant on up to two rounds of required prefunding.

To facilitate this prefunding, CHIP Co. members jointly maintain a pre-funded balance account (CHIPS account) on the books of the Federal Reserve Bank of New York. Under the real-time finality arrangement, each CHIPS participant has a pre-established opening position (or initial prefunding) requirement, which, once funded via a Fedwire Funds Service funds transfer to the CHIPS account, is used to settle payment orders throughout the day.⁹ A participant cannot send or receive CHIPS payment orders until it transfers its opening position requirement to the CHIPS account. Opening position requirements can be transferred into the CHIPS account any time after the opening of CHIPS and Fedwire Funds Service at 9:00 p.m. Eastern Time. However, all participants must transfer their requirement no later than 9:00 a.m. Eastern Time.

During the operating day, participants submit payment orders to a centralized queue maintained by CHIPS. Participants may remove payment orders from the queue at any time prior to the daily cutoff time for the system (5:00 p.m. Eastern Time). When an opportunity for settlement involving one, two or more payment orders is found, the system releases the relevant payment orders from the central queue and simultaneously marks the CHIPS records to reflect the associated debits and credits to the relevant participant's positions. Debits and credits to the current position are reflected only in CHIPS records and are not recorded on the books of the Federal Reserve Bank of New York. Under New York law and CHIPS Rules, payments orders are finally settled at the time of release from the central CHIPS queue.

This process, however, typically will be unable to settle all queued messages. Soon after 5:00 p.m. Eastern Time, CHIPS tallies any unreleased payment orders remaining in the queue on a multilateral net basis. The resulting net position for each participant is provisionally combined with that participant's current position (which is always zero or positive) to calculate the participant's final net position; if that position is negative, it is the participant's "final position requirement."

Each participant with a final position requirement must transfer, via Fedwire Funds Service, this second round of prefunding to the CHIPS account. These requirements, when delivered, are credited to participants' balances. Once all of the Fedwire Funds Service funds transfers have been received, CHIPS is able to release and settle all remaining payment orders. After completion of this process, CHIPS transfers to those participants who have any balances remaining the full amount of those positions,

⁹ CHIP Co., using a formula based on the latest transaction history of each participant, establishes the amount of a participant's opening position requirement.

reducing the amount of funds in the CHIPS account to zero by the end of the day. In the event that less than all final position requirements are received, CHIPS settles as many payments as possible, subject to the positive balance requirement, and deletes any remaining messages from the queue. Participants with deleted messages are informed of which messages were not settled, and may choose, but are in no way required, to settle such messages over Fedwire Funds Service.

OTHER CLEARINGHOUSE, SETTLEMENT, AND MESSAGING SYSTEMS

NATIONAL SETTLEMENT SERVICE (NSS)

NSS is a multilateral settlement service owned and operated by the Federal Reserve Banks. It allows participants in private clearing arrangements to settle their net obligations with same-day finality using participant's reserve or clearing account balances maintained at the Federal Reserve Banks. NSS participants include local check clearinghouse associations, automated clearinghouse (ACH) networks, credit card processors, and automated teller machine (ATM) networks.

To use NSS, a settlement agent transmits a settlement file electronically to a Federal Reserve Bank. The file contains a listing of the participants, the settlers (either the participant itself or the participant's correspondent), and the dollar amount of the debit or credit to be posted to the settler's account. If validity checks are satisfied, the Federal Reserve Bank accepts the file for processing and sends an acknowledgment to the agent. The Federal Reserve Bank accepts NSS files for processing and settlement between 8:30 a.m. and 5:30 p.m. Eastern Time. If an institution submits files earlier than 8:30 a.m. Eastern Time, they enter a queue for processing beginning at 8:30 a.m. Eastern Time. The NSS checks each debit balance on the settlement file against the account balance and intraday credit available to the settlers. The system may reject debit balances if a settler does not have a sufficient balance or sufficient intraday credit to cover the debit. Once it has posted all debit entries on the settlement file, NSS posts the credit balances. All transactions are final and irrevocable once the NSS posts them. The settlement for a file is complete when all credits have been posted. The NSS then sends an acknowledgment message to the settlement agent.

NSS offers payment finality similar to that of the Fedwire Funds Service and provides an automated mechanism for submitting settlement files to the Federal Reserve Banks. NSS improves operational efficiency and reduces settlement risk to participants by providing settlement finality on settlement day. It also enables the Federal Reserve Banks to manage and limit risk by incorporating risk controls similar to those used in the Fedwire Funds Service. NSS can settle transactions across Federal Reserve Districts or within a single Federal Reserve District.

SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION (SWIFT)

International funds transfer operates differently from domestic large-value funds transfer. While the SWIFT operates as a messaging system, transmitting instructions to move funds, the domestic systems discussed above accomplish the actual funds movement.

SWIFT is an industry-owned cooperative, which supplies secure, standardized messaging services and interface software to 7,500 financial institutions in 199 countries. The SWIFT community includes a variety of financial services firms, including banks, broker/dealers, and investment managers, as well as their market infrastructures in payments, securities, treasury, and trade. The SWIFT core application is the FIN (Financial Transaction) application, which provides a store and forward financial messaging service accessed over X.25 network connections.¹⁰ The system now uses bilateral key security and provides message validation to ensure messages are formatted according to SWIFT standards.

SWIFT messages may be used to transmit payment instructions for both domestic and international financial transactions. Financial institutions generating a high volume of funds transfer activity typically establish direct SWIFT connectivity with their internal, intrabank funds transfer system. The SWIFT network controls the integrity of the messages once properly entered at the point of origination. Thus there is no requirement for the receiver to re-verify payment orders. As a result, payment instructions pass through the system without human intervention unless programmed conditions (e.g., overdraft limit excesses) or error messages occur.

In 2002, SWIFT began migrating its core FIN application from an X.25 network to SWIFTNet, an IP-based network using the Secure Internet Protocol Network (SIPN). The introduction of IP-based technologies, that uses both bilateral keys and public keys, will allow SWIFT to expand its services. Payment-related business solutions currently being developed include cash reporting, bulk payments processing, and securities reporting. To promote the use of SWIFTNet and XML (Extensible Markup Language) based cash reporting tools among major cash clearing institutions and their correspondents, a working group has been set up to design the industry solution, including query/response standards and a rule book. In bulk payments, SWIFT developed a new XML-based message standard that was introduced in 2002.

TELEX-BASED MESSAGING SYSTEMS

Several private telecommunications companies offer worldwide or interconnected services that provide a printed record of each transmitted message. Financial institutions that do not have access to SWIFT use Telex-based proprietary systems. Financial institutions access Telex-based systems via a dial-up or a dedicated line with dedicated

¹⁰ X.25 is the software that SWIFT provides to its users for access capability to SWIFT's core FIN application.

printers. Some systems are computer monitored 24 hours a day, seven days a week and are fully redundant with automatic switch over and recovery capability.

Telex systems do not include built-in security features. Financial institutions that use Telex must exchange security codes. Typically, senders number messages sent to another institution to provide better audit controls. The sending institution is responsible for incorporating a test key in all instructions to a receiver to execute a payment order. The receiver is responsible for safekeeping the unique test code keys of each sender and decoding each test message. This function should be clearly separated from the Telex operating area and funds payment function. Presently, only a few institutions employ fully automated interface of Telex with their funds payment systems.

CONTINUOUS LINKED SETTLEMENT (CLS) BANK

CLS Bank is a private sector special purpose bank that uses the CLS system to settle payments associated with a foreign exchange (FX) transaction simultaneously.

CLS is designed to eliminate the risk occurring when each leg of certain FX transactions is settled separately, i.e., the payment is made and the corresponding payment is not received. CLS Bank settles payment instructions in the following currencies: Australian Dollar, Canadian Dollar, Danish Krone, Euro, Japanese Yen, Norwegian Krone, Singapore Dollar, Swedish Krona, Swiss Franc, GB Pound, and U.S. Dollar, and is expected to add more currencies over time.

Customers may join CLS Bank as either a Settlement Member or User Member. Settlement members have accounts with CLS Bank and must sponsor User members that do not have such accounts. Any Settlement member or User member may submit payment instructions for settlement processing, but the sponsoring Settlement member must authorize each instruction a User member submits. Non-members may settle their FX payments through private arrangements with members who will submit the settlement processing instructions to the service. Such members are responsible to CLS Bank as principals with respect to such payment instructions.

Payment instructions are settled under the CLS Bank rules when it debits and credits the relevant Settlement members' accounts for the amounts involved. This final settlement will only occur within the context of several risk management tests.¹¹ If any of these tests are not satisfied, no debits or credits will be made, and the pair of Settlement Eligible Instructions will remain on the settlement processing queue and be retested each time the queue is cycled through. The risk management tests will continue to be applied to all Settlement Eligible Instructions on the settlement processing queue until the

¹¹ The risk management tests are: (1) any Short Position in respect to each currency would not exceed the relevant Settlement Member's Short Position Limit (adjusted based on the committed liquidity facilities available to CLS Bank for that day); (2) the Aggregate Short Position in the Settlement Member's Account, calculated as an equivalent U.S. dollar value, would not exceed the Aggregate Short Position Limit which is set for that Settlement Member; and (3) the sum of the Settlement Member's Long Positions and Short Positions (the "Account Balance"), adjusted by applicable Haircuts (the "Adjusted Account Balance"), would not be negative.

applicable currency closing time has passed or all Settlement Eligible Instructions on the settlement processing queue have been settled. CLS Bank does not (i) guarantee the settlement of every payment instruction that is submitted for settlement or (ii) become a counterparty to any FX transaction referenced in a payment instruction that is submitted for settlement. In the event that a member is unable to provide its expected pay-in, other CLS members may be obligated to provide revised pay-in requirements.

SECURITIES SETTLEMENT SYSTEMS

The major securities markets in the United States include the government securities market, the corporate equities and bond market, the market for money market instruments, and the municipal bond market. The instruments traded in these markets are generally traded through organized exchanges or through the over-the-counter dealer markets. Major categories of financial instruments commonly traded include U.S. Treasury securities, government agency securities, securities issued by federal government-sponsored enterprises, corporate equities and bonds, money market instruments such as commercial paper, and municipal (state and local) government securities. Participants in these markets include securities issuers; intermediaries such as brokers and dealers; and investors such as insurance companies, investment companies, non-financial corporations and individuals.

The mechanisms for clearing and settling securities transactions vary by market and type of instrument, and generally involve two types of specialized financial intermediaries: clearing corporations and securities depositories. Clearing corporations provide trade confirmation and comparison services, and multilateral netting of trade obligations; while, securities depositories transfer securities ownership on a gross or net basis against payment via book-entry transfers.

Depository institutions play several important roles in securities clearing and settlement. Not only do depository institutions participate in clearing and settlement arrangements for themselves, they also act as custodians, issuing and paying agents, and settling banks for their customers. In addition depository institutions provide credit to clearing corporations, securities depositories, and clearing participants for routine and contingency purposes.

U.S. GOVERNMENT SECURITIES

The U.S. government securities market encompasses all primary and secondary market transactions in securities issued by the U.S. Treasury, certain federal government agencies, and federal government-sponsored enterprises.¹² Trading in government securities is conducted over the counter between brokers, dealers, and investors. In over-the-counter trading, participants trade with one another on a bilateral basis rather than on an organized exchange. Nearly all U.S. government securities are issued and transferred through a book-entry system operated by the Federal Reserve.

¹² Government-sponsored enterprises (GSEs) are publicly-traded corporations created by Congress to address public policy concerns about the ability of members of certain groups to borrow sufficient funds at affordable rates. GSEs do not receive federal funds and rely primarily on debt financing for their day-to-day operations. GSE securities are not government securities; however, market participants rate and price GSE securities similar to U.S. government-issued securities.

In the primary market, U.S. Treasury securities are issued through regularly scheduled auctions. The Federal Reserve Banks serve as conduits for the auctions, with the Federal Reserve Bank of New York coordinating much of the auction activity. Individuals, corporations and financial institutions may participate in the auctions. Participation in Treasury auctions, however, is typically concentrated among a small number of dealer firms, known as primary dealers.¹³

In the secondary market for government securities, trading activity takes place between primary dealers and non-primary dealers. Customers of these dealers are financial institutions, non-financial institutions and individuals. The majority of transactions between primary dealers and other large market participants are conducted through inter-dealer brokers that provide both anonymity and price information to market participants. Approximately 2,000 securities brokers and dealers are registered to operate in the U.S. government securities market.

FIXED INCOME CLEARING CORPORATION (FICC)

FICC¹⁴, composed of the Government Securities Division (GSD) and the Mortgage-Backed Securities Division (MBSD), compares and nets trades of U.S. Treasury securities, agency debt securities, and mortgage-backed securities. As the name implies, GSD clears and nets U.S. government securities and agency debt securities. MBSD provides automated post-trade comparison, netting, risk-management, and pool notification services to the mortgage-backed securities market. Securities eligible for MBSD clearing are mortgage-backed securities issued by the Government National Mortgage Association (GNMA), the Federal Home Loan Mortgage Corporation (FHLMC), and the Federal National Mortgage Association (FNMA).

FICC uses real time trade matching; trade details are compared and matched as soon as trade information is submitted. Successfully compared trades result in binding and enforceable obligations for settlement. Unmatched trades may be revised to achieve a trade match.

Successfully matched trades of eligible securities, for FICC netting service participants, are netted against offsetting net-receive or net-deliver obligation of the same security. Once the government securities net positions are determined GSD interposes itself between the original trading parties and becomes the legal counter-party to FICC members for settlement purposes. Therefore, GSD members' net settlement obligations are delivered to or received from GSD. MBSD, however, engages in multilateral position netting and does not stand in the middle of transactions. Final net settlement obligations

¹³ Primary dealers are designated trading counterparties for the Federal Reserve Bank of New York in its execution of market operations to carry out US monetary policy. Currently there are 23 designated primary dealers.

¹⁴ FICC is a subsidiary of the Depository Trust and Clearing Corporation, a holding company that also includes the National Securities Clearing Corporation and the Depository Trust Company. In January 2003, the Mortgage-Backed Securities Clearing Corporation merged with the Government Securities Clearing Corporation to form the FICC. For further information about the Government Securities Division and the Mortgage-Backed Securities Division, see www.ficc.com.

of GSD and MBSD participants are settled through the Fedwire Securities Service via participants' settlement bank.

FEDWIRE SECURITIES SERVICE

As fiscal agents of the United States, the Federal Reserve Banks act as the securities depository for all marketable U.S. Treasury securities, many federal agency securities, and certain mortgage-backed securities issued by GSEs.¹⁵ U.S. government securities are issued in book-entry form through the Federal Reserve's Fedwire Securities Service using either an auction process or dealer syndicate mechanisms. The Federal Reserve's Fedwire Securities Service provides for the safekeeping and transfer of these securities. The safekeeping function involves the records of securities balances, and the transfer and settlement function involves the transfer of securities between parties.

When book-entry securities transfers are processed using Fedwire Security Service, the institution sending the transfer receives immediate credit in its Federal Reserve (funds) account for the payment associated with the transfer, and its securities account is correspondingly debited. The Federal Reserve (funds) account of the institution receiving a book-entry securities transfer is debited for the payment amount, and its securities account is credited. There are more than 9,000 participants in the system and they are largely composed of depository institutions.

The Federal Reserve's Fedwire Securities Service is supported by a real-time, delivery-versus-payment (DVP) gross settlement system that provides for the immediate, final, and simultaneous transfer of securities against the settlement of funds. This system, known as the National Book-Entry System (NBES), provides for the safekeeping and transfer of U.S. Treasury, government agency, and GSE securities as well as securities issued by certain international organizations. The safekeeping function involves the electronic storage of securities records in custody accounts, and the transfer and settlement function involves the transfer of securities between parties.

Financial institutions may access the Fedwire Securities Service via high-speed direct CI, FedLine, or with off-line telephone connectivity with a Federal Reserve Bank. Financial institutions may also access certain Fedwire Securities Service inquiry information via FedLine for the Web. On-line participants, using either a mainframe or FedLine PC connection to Fedwire Securities Service, require no manual processing by the Federal Reserve Banks. Off-line participants provide funds transfer instructions to their Federal Reserve Bank by telephone, and once authenticated, the Federal Reserve Bank enters the transfer instruction into the Fedwire Securities Service system for execution. The manual processing required for off-line requests makes them more costly and suitable only for institutions processing a small number of funds transfer payment orders.

¹⁵ The Federal Reserve also acts as agent and depository for the securities of certain international organizations, such as the World Bank.

CORPORATE AND MUNICIPAL SECURITIES

Corporate equities and bonds, commercial paper, and municipal bonds are traded on various established exchanges and on over-the-counter markets. The primary securities exchanges in the United States are the New York Stock Exchange, the American Stock Exchange, and the primary over-the-counter dealer market is the National Association of Securities Dealers Automated Quotations (NASDAQ).

The commercial paper market warrants special mention as it is an important source of short term funding for financial corporations and municipal governments. Commercial paper is a money market instrument issued by prime-rated non-financial and financial companies with maturities ranging from one to 270 days. Commercial paper is issued through dealer placements or direct placements with investors. Although commercial paper is a negotiable instrument, secondary market trading is limited. Disruption in the issuance of commercial paper can cause significant liquidity and credit concerns for issuers, many of whom are depository institutions and other financial companies, and depository institutions that provide issuing and paying agent services to issuers.

NATIONAL SECURITIES CLEARING CORPORATION (NSCC)

NSCC, established in 1976, provides clearing and settlement services for corporate equities, corporate debt, municipal securities, mutual funds, annuities, and unit investment trusts. NSCC is a registered clearing corporation regulated by the Securities and Exchange Commission (SEC). With roughly 250 full-service participants, NSCC handles all aspects of the clearing and settlement of trades between brokers and dealers in securities traded on the over-the-counter markets, the New York Stock Exchange, the American Stock Exchange, and other regional exchanges.

Executed trades are typically reported to NSCC on trade date. Trades are either reported to NSCC by an established exchange as matched (irrevocable) trades or by brokers and dealers as unmatched trades. Trades submitted by brokers and dealers are compared and matched within NSCC's Continuous Net Settlement (CNS) system. Following the comparison process, NSCC becomes the legal central counterparty and guarantees completion of all securities trades following through CNS. CNS functions as an automated book-entry accounting system that centralizes the settlement of compared security transactions and maintains an orderly flow of securities and money balances.¹⁶

Similar to the FICC netting process, successfully matched trades of eligible securities are netted against offsetting net-receive or net-deliver obligation of the same security. Settlement of securities takes place at the Depository Trust Company and funds settlement occur over the Fedwire Funds Service through settlement banks.

¹⁶ Further information about NSCC's clearing processes can be found at www.nsccl.com.

DEPOSITORY TRUST COMPANY (DTC)

DTC is a New York limited purpose trust company, a member of the Federal Reserve System, and a clearing agency registered with the SEC. DTC, the central securities depository for corporate equities and bonds, municipal government securities, and money market instruments, provides safekeeping and transfer of these securities. DTC participants include securities brokers, dealers, institutional investors, and depository institutions acting on their own behalf as well as functioning as custodians, issuing and paying agents, and settling banks for their customers.

Like Fedwire Securities, the safekeeping function involves the electronic recordkeeping of securities balances for participants, and the transfer function involves the transfer of securities between parties. DTC transfers securities on a gross basis throughout the day, while settling funds obligations on a net basis at the end of the day. During the transfer process, DTC will limit its credit exposure through participants' net debit caps. Any net debit position incurred by participants must be fully collateralized. End of day funds settlement occur over the Fedwire Funds Service through participants' settlement banks.¹⁷

¹⁷ See www.dtc.org for more information on DTC.

INTRABANK PAYMENT AND MESSAGING SYSTEMS

Action Summary

Financial institutions require efficient systems for transferring funds internally, among themselves, and with their customers for large-dollar payments relating to financial market transactions and settling corporate and consumer payments.

Management and the board should:

- Establish dual controls and separation of duties for funds transfer systems;
- Monitor and log access to funds transfer systems, maintaining an audit trail of all sequential transactions; and
- Incorporate the funds transfer controls into the organization's information security program to ensure the integrity and confidentiality of customer information.

INTERNALLY DEVELOPED AND OFF-THE-SHELF FUNDS TRANSFER SYSTEMS

Financial institutions rely on internal funds transfer systems and networks to send payment instructions to their correspondents for the transfer of correspondent balances or to initiate Fedwire Funds Service or CHIPS payments. Large financial institutions have either developed their own funds transfer systems or relied on off-the-shelf funds transfer systems. In either case, the internal financial institution funds transfer systems interface with Fedwire Funds Service and CHIPS, supporting the interface and transaction format specifications for the transmission of payment orders. Off-the-shelf funds transfer systems typically support a variety of treasury, cash management, and straight-through-processing (STP) modules, which automate payment order processing.

The Federal Reserve Banks provide the Computer Interface Protocol Specifications (CIPS) that funds transfer and book-entry securities systems need to adopt in order to implement a CI connection successfully. The Federal Reserve provides a website with a list of vendors who have completed the Federal Reserve Banks' protocol certification process.¹⁸ The Federal Reserve Banks do not endorse any specific software vendor or

¹⁸ Refer to <http://www.frbsservices.org/Wholesale/ProtocolCertVendors.cfm> for a list of protocol certified vendors.

product. The Federal Reserve Banks make no warranties or representations with respect to any of the products offered by these vendors except that communication-level software correctly executes systems network architecture (SNA) commands as specified in the CIPS.

PAYMENT MESSAGING SYSTEMS

Financial institutions, corporations, and other organizations employ wholesale payment message systems to originate payment orders, either for their own benefit or for a third party. These systems are indispensable components of funds-transfer activities. Unlike payment systems, which transmit actual debit and credit entries, message systems process administrative messages and instructions to move funds. The actual movement of the funds is then accomplished by initiating the actual entries to debit the originating customer's account and credit the beneficiary's account at one or more financial institutions. If the beneficiary's account or the beneficiary institution's account is also with the originator's institution, the institution normally handles the transaction internally through a book transfer. If the beneficiary-related accounts are outside the originating customer's institution, the parties will complete the transfer by use of a payments system such as Fedwire Funds Service or CHIPS. The means of arranging payment orders range from manual methods (e.g., memos, letters, telephone, fax, or standing instruction) to electronic methods using telecommunications networks. These networks may include those operated by the private sector, such as SWIFT or Telex, or operated internally by or for the institution. The internal networks can be for inter-company purposes only or connected to customer sites.

Since the payment order is the institution's authorization to act on behalf of the customer, it is imperative that a system is in place to establish the authenticity and time of receipt of the order. These two elements are the primary components cited by the Uniform Commercial Code Article 4A (UCC4A) in establishing responsibility for the execution of a payment order. Even though the transfers initiated through systems such as SWIFT and Telex do not result in the immediate transfer of funds from the issuing institution, they do result in the issuing institution having an immediate liability, which is payable to the disbursing institution. Therefore, the physical and logical controls surrounding payments messaging systems should include:

- Physical controls limiting access to only those staff members assigned responsibility for managing the payment messaging system;
- Logical access controls restricting access on a need to know basis;
- Assigning access to payment messaging application and data based on functional job duties and requirements; and
- Identification and authentication controls used to authenticate access to payment messaging systems.

IN-HOUSE TERMINALS

Some financial institutions employ terminals, connected via telecommunications networks with customers and the institutions' operating departments, to execute funds payment orders. These systems may be dial-up or dedicated lines and are often fully interfaced to the institution's funds payments system. The primary security method is the use of unique passwords for each user of the system. Since there is often no intervention by the funds payment operation, it is necessary to establish controls directly in the area employing the terminals. These controls should cover origination, data entry, and release, and should be the same as those associated with an independent funds payment function.

NON-AUTOMATED PAYMENT ORDER ORIGATION

While in-house terminals are the primary sources for payment order origination, less complex institutions still rely heavily on memos, letters, telephone, fax, or standing instructions. (Note: standing instructions are normally maintained in the automated funds transfer system as recurring transfers and should be subject to the same input/verification controls as wires when first entered into the system). It is imperative that an institution using these payment order methods has a viable security program, which includes:

- Maintaining signature lists for use with internally and externally generated memos, letters, or fax instructions. As noted in UCC4A Section 201, signature verification alone is not defined as a security procedure; however, institutions may use it with other security devices such as call backs or codes.
- Call back to authorized individuals for both internally and externally generated telephone instructions.
- Procedures covering standing instructions protecting against unauthorized change, periodic review to validate accuracy, and ensuring execution under the agreed terms.

FUNDS TRANSFER OPERATIONS (WIRE ROOM)

A financial institution's funds transfer operation (wire room) is responsible for originating, transmitting, and receiving payment orders. In less complex financial institutions, the wire room typically includes a FedLine PC. Less complex institutions may also have a core banking package that includes a funds transfer module, which generates payment orders in a Fedwire Funds Service format for uploading to the FedLine PC.¹⁹ Staff assigned responsibility for these activities are generally responsible for other duties and are not typically dedicated full-time to the wire room function. In most financial institutions, funds transfer payment order volume does not justify the costs associated with a full time staff, and the sending and receiving of payment orders may be

¹⁹ See the *IT Handbook's*, "FedLine Booklet."

a part-time responsibility for one or more people. For less complex financial institutions, a complete separation of duties may be difficult to achieve, and compensating controls, including rotation of duties and internal review procedures covering those payment orders requiring officer review, should be considered.

Financial institutions generating significant payment order volume usually have a separate funds transfer department with dedicated staff. Financial institutions generating a large volume of high value Fedwire Funds Service payment orders typically use dedicated funds transfer software (developed in-house or purchased) connected via computer interface to the Federal Reserve Bank's Fedwire Funds Service application. The software used for wire transfers automatically posts transactions to the demand deposit account and general ledger. The automated function provides an efficient means to process a large number of payment orders supporting a variety of business lines.

Payment orders can be received from several different sources including business areas within the financial institution, as well as from corporate and individual customers. Payment orders can be initiated by phone, fax, and online systems. Individuals wishing to wire funds typically do so at the teller window or contact their loan officer or account representative. Payment order verification is an important safeguard, and institutions should, at a minimum, keep accurate records of all payment order requests, including those initiated by telephone. Institutions should record all phone calls initiating payment orders for security and audit reasons. The institutions should maintain the tapes for at least a 30-day period.

After receiving a payment order, the wire room operator keys the payment order into FedLine (or the payment order is generated through the use of a third-party software product funds transfer module). Before sending a payment order to the Federal Reserve Bank, a second staff member should verify it for accuracy and authorization. Most FedLine PCs have two printers attached, one that prints copies of all outgoing payment order Fedwire Funds Service messages and another that prints incoming Fedwire Funds Service payment order messages. Institutions should maintain a record of all payment orders for record keeping purposes. The unbroken printout sheet helps ensure a complete record of all messages; however, institutions should also verify the sequence numbers of the messages to identify missing records due to communication problems. The sequence number provides an audit trail for all funds transfers on the Fedwire Funds Service system.

The institution should have appropriate procedures in place to verify all processed payment orders. These procedures usually include the use of code words, call backs, and corporate resolutions authorizing certain employees to send payment orders. Verification and security procedures are extremely important in light of the potential for fraud or errors.

A Fedwire Funds Service message is generated either by the application supporting the business line or by an authorized wire room employee who enters the message into an on-line terminal. Before transmitting the wire, it is sent to a second terminal for an

independent employee to verify for accuracy as well as proper authorization. Only after a second staff member reviews the payment order should a financial institution send it to the Federal Reserve Bank for processing.

This separation of duties is important to ensure security. The institution's internal funds transfer system should maintain data on each day's transfers, including wires sent and received, wires listed by amount, wires listed by sequence number, and wires listed by account holder. Most software systems maintain the work of several previous days, often the last 5 to 7 days, to allow on-line access to trace errors and problems. After the 5 to 7 days, the data is typically archived.

COMPUTER AND NETWORK OPERATIONS SUPPORTING FUNDS TRANSFER

Wholesale funds transfer systems are high risk. Therefore, management should configure hardware and software components to control access and support effective monitoring. Management should develop change management procedures to ensure the integrity of the hardware configurations and applications software. Operations personnel should have the appropriate procedures to manage critical payment systems software.

Applications should employ strong user authentication, support user entitlement (information access and function controls) administration, and provide audit trails in sufficient detail to support the analysis or investigation of specific transactions. Management should enable funds transfer activity logs and designate independent staff members to monitor operations, applications support, system administration, and security administrators' activities associated with the funds transfer system.

Telecommunications systems employed for EFT can range from a dial-up connection between the institution and payments system (e.g., FedLine) to terminal connections with institution staff and customers that transmit institution's funds transfer system payment orders directly to Fedwire Funds Service via CI connection. An institution's information security program should include access, authentication, and transmission controls surrounding wire room activities and all terminal connections. Access and authentication controls may consist of personal identification numbers, passwords, or other identifying keys such as account numbers, balances, or other financial data. Financial institutions should use encryption as a means of protecting data throughout the EFT system. Encrypting data during transmission allows institutions to scramble the contents of message/payment orders during transmission and limit the value of the information to an interloper even if a transmission is intercepted. Nevertheless, financial institutions should monitor or prevent access to funds transfer activity by data processing personnel who have access to communications equipment and can monitor and record data flowing in clear text from encryption devices.

WHOLESALE PAYMENT SYSTEMS RISK MANAGEMENT

Action Summary:

Financial institutions engaged in wholesale payment systems and related activities should establish appropriate risk management processes that identify, measure, and limit risks.

Financial institutions should tailor their risk management processes based on the nature and complexity of their wholesale payments business and their participation in wholesale payment, clearance, and settlement systems.

Management and the board of directors should manage and mitigate identified risks through effective and appropriate policies, procedures, and controls.

Wholesale payment systems risk management should include the identification, measurement, mitigation, and management of risks related to a financial institution's wholesale payments and securities settlement activities. These risks arise in the process of originating wholesale payment or securities settlement transactions and in the process for clearing and settling these transactions. Financial institutions should employ sound risk-management processes to identify and control these risks.

In identifying its potential risks, the financial institution should consider the risks it may be exposed to from the process of creating and transmitting payment orders or securities delivery instructions; from participating in wholesale payments and securities settlement systems directly, including any loss-sharing or liquidity provision procedures associated with these systems; from participating in such systems indirectly through a correspondent; and, for some institutions, from providing operational or other supporting services to a wholesale payments or securities settlement system, including any credit or liquidity facilities the institution provides to the system beyond those associated with participation in the system (either directly to the system operator or indirectly through the system's participants).

Sound risk management involves a combination of policies, processes, people, and reporting systems that address the credit, liquidity, operational, and legal risks borne by an institution as a result of its wholesale payments and securities settlement activities. For example, the institution should have credit policies and controls, such as limits on customers' daylight overdrafts. The appropriate staff should have a clear understanding of the normal, abnormal, and contingent liquidity demands that may arise from the

institutions participation in wholesale payment systems, and liquidity management and treasury procedures should take these demands into consideration.

Operational policies and controls should cover the critical and core systems that support an institution's wholesale payment activities and address areas such as business continuity planning, crisis management, physical and logical information security, and vendor management. Finally, an institution should use appropriate measures to identify and mitigate its legal risks, including risk arising from compliance with federal and state laws, customer agreements, counterparty agreements, relevant payments laws, rules and regulations, and wholesale payment system policies and procedures.

Management and the board of directors should also oversee the implementation of the risk management strategy, policies, and controls through appropriate governance arrangements, effective external and internal audits, and appropriate management information systems.

PAYMENTS SYSTEM RISK (PSR) POLICY

Given the role of payments and securities settlement systems as critical components of the nation's financial system, the Federal Reserve Board has developed a policy to foster the safety and efficiency of these systems.²⁰

One major component of the Federal Reserve's policy addresses the extent to which institutions with Federal Reserve accounts are allowed to have daylight overdrafts in that account. Additional information about this aspect of the PSR policy is provided in Appendix E. A daylight overdraft occurs when an institution's Federal Reserve account is in a negative position during the business day. Negative balances typically occur when there are insufficient funds in an institution's account to cover outgoing Fedwire funds transfers, incoming book-entry securities transfers, or other payment activity processed by a Federal Reserve Bank. The PSR policy applies a series of limits and incentives to control the Federal Reserve Banks' exposures to the credit risk associated with these daylight overdrafts. Limits on net debit positions are sufficiently flexible to reflect the overall financial condition and operational capacity of each institution using Federal Reserve Bank payment services.

Institutions with the highest net debit caps are subject to an annual self-assessment process that is outlined in the "Guide to the Federal Reserve's Payments System Risk Policy."²¹ In addition to an analysis of the institution's general creditworthiness,

²⁰ The regulatory agencies have also issued interagency and agency-specific policies on payments and payment system risk. The "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," for example, identifies sound practices focusing on minimizing the immediate systemic effects of a wide-scale disruption to critical financial markets. The sound practices discussed in this paper supplement the agencies' respective policies and other guidance on business continuity planning. See <http://www.federalreserve.gov/paymentsystems/psr/default.htm>.

²¹ <http://www.federalreserve.gov/paymentsystems/psr/guide.pdf>

institutions eligible for a self-assessed cap should manage and control their intraday funds positions, maintain credit policies and controls at the customer level, and employ operational controls and contingency plans. In particular, institutions with self assessed caps need to be able to monitor and control the intraday credit they extend to their customers. Such credit has the potential to result in Federal Reserve daylight overdrafts for the institution. The risks associated with customers' daylight overdrafts are discussed below.

Another major component of the PSR policy provides expectations for risk management in payments and securities settlement systems, and adopts international standards for systemically important systems.²² This portion of the policy is directed at system operators, but contains key information about the risks that such systems present to system participants, and in some cases, requires covered systems to provide participants with clear information about these risks. Moreover, examined institutions may have an important role in the governance of wholesale payments and securities settlement systems, as many private sector systems are owned by their participant financial institutions.

STRATEGIC RISK

Strategic risk relates to a financial institution's future business plans and strategies. It includes risks associated with plans for entering new business lines, expanding existing services through mergers and acquisitions, and enhancing the infrastructure (e.g., physical plant and equipment and information technology and networking).

To mitigate strategic risk, management should have a strategic planning process in place to address its wholesale payment system business goals and objectives, including the information technology and network components required to carry out its business plan.

CREDIT RISK

Credit risk is the risk that a counter party will not settle an obligation for full value when due. In relation to wholesale payments and securities settlement systems, credit risk can take several forms and have multiple sources. Two of the most important sources, customer daylight overdrafts and settlement risks (including settlement lags, principal risk, and loss-sharing provisions), are discussed below. These forms of credit risk, as

²² See <http://www.federalreserve.gov/paymentsystems/psr/default.htm> for details and further references.

well as other forms of credit risk, should be appropriately monitored and managed. Information technology is often critical to such controls.

CUSTOMER DAYLIGHT OVERDRAFTS

Financial institutions often permit their individual and corporate customers to incur intraday overdrafts by allowing customers to make payments without available balances. In most cases, overdrafts are eliminated with incoming funds transfers from other institutions (or outgoing securities transfers against payment) by the end of the business day.

Financial institutions engaging in this practice are extending credit to their customers. As such, they should monitor the credit position of individual customers; control the amount of intraday credit extended to each customer; and have guidelines to prevent exceeding approved intraday and overnight overdraft limits. These guidelines should include:

- Reviewing customer credit limits and the frequency and scope of internal credit reviews. In the absence of pre-authorized limits, institutions should have a process for management approval of daylight overdrafts. Authorization should be within the lending authority of approving officers.
- Reporting and approval procedures for payments exceeding established credit limits to ensure officers with sufficient lending authority make approvals.
- Reviewing intraday overdrafts incurred for compliance with established limits as well as approval and reporting requirements.
- Reviewing arrangements/agreements regarding collateralization of credit exposures.

To the extent that these guidelines give consideration to projected incoming payments, the financial institution should be aware of the risk that expected payments may not be received when expected. Moreover, as described below, institutions should also consider whether such payments have been or are expected to be made with finality.

Since daylight overdrafts constitute an extension of credit (no matter the period of time involved), financial institutions' credit policies should include provisions for approving and monitoring intraday credit lines to customers. Daylight overdrafts have the potential to become overnight overdrafts or overnight loans, and institutions should also have procedures to determine limits on overnight overdrafts. Both sets of procedures should be similar to loan portfolio credit analysis.

Credit policies and procedures should include:

- Analyzing worthiness of all borrowers with amounts outstanding in excess of the credit line.
- Reviewing reporting and approval procedures for overdrafts and settlement credits exceeding established limits.
- Assessing reporting and approval procedures for payments against uncollected funds.

Depending on the creditworthiness of the customer and the nature of the activity, a financial institution should consider requiring customers to advise the institution of anticipated incoming securities transfers. Financial institutions should also consider requiring the customer to pre-fund all such anticipated transfers, with the understanding that any transfers not pre-funded may be reversed. To further mitigate credit risk, management should consider requiring customers to collateralize intraday overdrafts. As mentioned above, the control of customers' daylight overdrafts is one of several elements of the Self-Assessment process set out in the Board's PSR policy (see Appendix E).

SETTLEMENT RISK

In addition to the explicit provision of credit via daylight overdrafts, financial institutions also need to control their exposure to settlement risks incurred through the institutions' participation in interbank payment and settlement systems. In general, settlement risk is the possibility that the completion or settlement of individual transactions or settlement at the interbank funds transfer or securities settlement level more broadly, will not take place as expected. In addition to credit risk, settlement risk often includes elements of liquidity risk.

One important source of settlement risk is any time lag between the origination of the payment or securities settlement instructions and final settlement, and discharge of those instructions. This time difference between the delivery of payment details and payment finality, or settlement lag, creates the possibility that sending institutions could fail during the lag or at least not be able to settle their obligations when due, typically at the end of the day. If the receiving bank credits the anticipated payment proceeds to the customer's account before the payment is final, the receiving bank may be exposed to credit risk from the sending bank until final settlement occurs. As long as final settlement has not occurred, any credits or additional payment activity undertaken on the basis of "unsettled" payment messages results in credit risk.²³ Financial institutions should analyze and control this credit risk as they would any other extension of credit.

Real-Time Gross Settlement systems, such as Fedwire Funds Service, are not subject to this risk as payments credited to a receiver's account are final at the time of receipt.

²³ For more information, see "Real-time Gross Settlement Systems," Committee on Payment and Securities Settlement Systems, 1997 at www.bis.org/publ/cpss22.pdf.

CHIPS payments were previously subject to this kind of risk. However, starting January 2001, CHIPS began sending payment details to the receiving bank only once a payment became final.²⁴ Securities settlements that occur at DTC may be subject to this kind of risk.

Another form of settlement risk is caused by a time-lag between the final settlement of two sides of a given trade or transaction (e.g., any difference in timing between the payment for and delivery of securities, or for foreign exchange transactions, the final delivery of one currency prior to the other). Such time lags can put the entire principle value of trades at risk. Several payments and securities settlement systems, including DTC and CLS Bank are designed to avoid this risk. Nonetheless, many foreign exchange transactions are not settled in CLS Bank, and may be subject to this type of settlement risk. Securities settlement systems in other countries in which U.S. institutions participate may also be subject to this form of risk.

Finally, many payments and securities settlement systems, especially those that rely on settlement lags, netting, or intraday credit, often implement various forms of risk controls that have important credit risk implications for system participants. In particular, systems often employ various types of loss-sharing and supplemental liquidity requirements in the event of settlement failures or disruptions. Participants in any payment or securities settlement system should understand the risks related to these settlement failure procedures and should be prepared to make any required supplemental payments of loss allocation assessments as described in the system rules. Financial institutions may also pre-arrange to serve as liquidity providers to payment or securities settlement systems in the event of a settlement disruption. These liquidity arrangements may involve committed lines of credit on either a secured or unsecured basis or foreign exchange swap facilities. Institutions should understand the nature of these special commitments and be well-prepared to act on them.

LIQUIDITY RISK

Liquidity risk involves the possibility that earnings or capital will be negatively affected by an institution's inability to meet its obligations when they come due. Liquidity risk is the risk that the financial institution cannot settle an obligation for full value when it is due (even if it may be able to settle at some unspecified time in the future). Liquidity problems can result in opportunity costs, defaults in other obligations, or costs associated with obtaining the funds from some other source for some period of time. In addition, operational failures may also negatively affect liquidity if payments do not settle within an expected time period. Until settlement is completed for the day, a financial institution may not be certain what funds it will receive and thus it may not know if its liquidity position is adequate. If an institution overestimates the funds it will receive, even in a system with real-time finality, then it may face a liquidity shortfall. If a shortfall occurs

²⁴ Receiving banks may, however, request certain details about payments queued for their receipt. Such information should not be treated as a final payment.

close to the end of the day, an institution could have significant difficulty in raising the liquidity it needs from an alternative source.

Systems that postpone a significant portion of their settlement activity (in dollar terms) toward the end of the day, such as CHIPS, may be particularly exposed to liquidity risk. These risks can also exist in RTGS systems such as Fedwire. As mentioned above, systems or markets that pose various forms of settlement risk also pose forms of liquidity risk. CLS Bank, while eliminating the bulk of principle risk through its payment-versus-payment design, retains significant liquidity risk, as funding is made on a net basis, and pay-in obligations may need to be adjusted in the event that a counterparty is unable to fund its obligations. Other systems, including securities settlement systems, may also be subject to liquidity risks.

To manage and control liquidity risk, it is important for financial institutions to understand the intraday flows associated with their customers' activity to gain an understanding of peak funding needs and typical variations. To smooth a customer's peak credit demands, a depository institution might consider imposing overdraft limits on all or some of its customers. Moreover, institutions must have a clear understanding of all of their proprietary payment and settlement activity in each of the payment and securities settlement systems in which they participate.

LEGAL (COMPLIANCE) RISK

Legal/compliance risk arises from an institution's failure to enact appropriate policies, procedures, or controls to ensure it conforms to laws, regulations, contractual arrangements, and other legally binding agreements and requirements. In particular, legal risks can result if a financial institution does not provide adequate attention to the operating circulars, procedures and rules of the payment and settlement systems in which it participates. Similarly, an institution's contractual relationships with customers, counterparties, and vendors must be sound and appropriate to the relevant legal framework(s) such as payment and bankruptcy frameworks. Contracts, among financial institutions, their customers, and counterparties are also important to allocate risk-sharing responsibilities applicable to payments. Finally, an institution must ensure it is in compliance with all applicable Federal and State laws and regulations governing payments activity, including the Bank Secrecy Act, the USA PATRIOT Act, and laws regarding economic sanctions. Appendix D provides details on the general legal framework for payments and securities settlement systems.

Office of Foreign Assets Control (OFAC)

The Office of Foreign Assets Control (OFAC), an agency of the U.S. Treasury, administers a series of laws imposing economic sanctions against targeted hostile foreign countries to further U.S. foreign policy and national security objectives. The U.S. government exercises economic sanctions through trade embargoes, blocked assets controls, travel bans, and other commercial and financial restrictions. The economic

sanctions programs of the U.S. government are powerful foreign policy tools. Their success requires active participation and support of every financial institution. The Secretary of the Treasury manages the sanctions for the U.S. The U.S. Government mandates that all financial institutions located in the U.S., overseas branches of U.S. financial institutions, and, in certain instances, overseas subsidiaries of U.S. financial institutions, comply with economic sanctions and embargo programs administered under regulations issued by OFAC. In general, the regulations:

- Block accounts and other assets of countries identified as being a threat to national security by the President of the United States (this always involves accounts and assets of the sanctioned countries' governments; it may also involve nationals of the sanctioned countries). In addition, OFAC also blocks the accounts of individuals on OFAC's Specially Designated Nationals (SDN) listing who may not be associated with a sanctioned country.
- Prohibit unlicensed trade and financial transactions with such countries. U.S. law requires that assets and accounts be blocked when such property is located in the U.S., is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. The definition of assets and property is very broad and covers direct, indirect, present, future, and contingent interests. Certain individuals and entities located around the world that are acting on behalf of sanctioned country governments have been identified by the U.S. Treasury and must be treated as if they are part of the sanctioned governments. U.S. banks must block funds transfers that are remitted:
 - By, or on behalf of a blocked individual or entity;
 - To, or through a blocked entity; or
 - In connection with a transaction in which a blocked individual or entity has an interest.

Financial institutions receiving instructions to make a payment that falls into one of these categories are required to execute the payment order and place the funds into a blocked account. Customers cannot cancel or amend a payment order after the U.S. bank has received it. Once assets or funds are blocked, they may be released only by specific authorization from the U.S. Treasury. If OFAC compliance issues are found during an examination, the examiner should follow up with the bank regulatory agency's compliance area to determine whether the financial institution needs to acquire subject matter expert support.²⁵

²⁵ For a complete discussion of legal requirements, consult 31 CFR Part 500 et seq.

Bank Secrecy Act (BSA)

Financial institutions should develop and provide for the continued administration of a program reasonably designed to ensure and monitor compliance with the record keeping and reporting requirements set forth in subchapter II of the Bank Secrecy Act.²⁶ The BSA requires a written compliance program that is approved by the board of directors. The board must note the approval in the board minutes. The compliance program must include, at a minimum:

- Provision for a system of internal controls to ensure ongoing compliance;
- Provision for independent testing for compliance to be conducted by institution personnel or by an outside party;
- Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance, and
- Provision for training for appropriate personnel.

USA PATRIOT Act

On October 26, 2001, the President signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. The USA PATRIOT Act contains strong measures to prevent, detect, and prosecute terrorism and international money laundering. The provisions of the USA PATRIOT Act that most affect financial institutions are those contained in Title III. Among other things, Title III amends the Bank Secrecy Act and provides the Treasury Department and federal agencies with enhanced authority to combat international money laundering and block terrorist access to the U.S. financial system.

The Act is far-reaching in scope, covering a broad range of financial activities and institutions. One such provision is section 312 – Due Diligence for Correspondent and Private Banking Accounts. Section 312 requires a U.S. financial institution that maintains a correspondent account or private banking account for a non-U.S. person to establish appropriate and, if necessary, enhanced due diligence procedures to detect and report instances of money laundering. Section 312 also describes specific enhanced due diligence standards for U.S. financial institutions that enter into correspondent banking relationships with foreign banks operating under offshore banking licenses or under banking licenses issued by countries that have been:

- Designated as non-cooperative with international anti-money laundering principles by an international body (such as the Financial Action Task Force) with the concurrence of the U.S. representative to that body, or

²⁶ Chapter 53 of title 31, United States Code, the Bank Secrecy Act, and the implementing regulations promulgated by the Department of Treasury at 31 CFR part 103.

- The subject of special measures imposed by the Secretary of the Treasury under section 311 of the USA PATRIOT Act.

In addition, section 312 describes minimum anti-money laundering due diligence standards for the maintenance of private banking accounts by U.S. financial institutions for non-U.S. persons. The Treasury Department (Treasury) is authorized to issue regulations implementing section 312. The Act provides that the provisions of section 312 became effective July 23, 2002, whether or not final regulations were in place. Because of the complexity of the issues raised by the proposed rule, Treasury did not promulgate a final rule by July 23, 2002, but rather issued an interim final rule that was effective immediately. The interim final rule requires that insured depository institutions, U.S. branches and agencies of foreign banks, and Edge and Agreement corporations comply with the statutory requirements of section 312.

The interim final rule also provides compliance guidance to financial institutions. This guidance, which is set forth in supplementary information and not as a regulation, indicates what Treasury would consider as “reasonable” due diligence policies and procedures pending the issuance of a final rule. According to Treasury’s guidance, these policies and procedures include (1) focusing on accounts that pose the highest risk of money laundering, (2) according priority to those accounts opened on or after July 23, 2002, and (3) complying with existing best practice standards for banks, such as those issued by the Wolfsberg Group in May 2002, the Clearing House in March 2002, and the Bank for International Settlements in October 2001. Treasury noted that it would be reasonable for an institution not to apply every best practice standard if it has a justifiable basis for not adopting a particular practice.

Until Treasury issues a final rule implementing section 312, examiners should make certain covered banking organizations are aware of the specific provisions of the law and have reasonable policies and procedures in place to assure and monitor compliance. Also, in accordance with existing practices concerning anti-money laundering related matters, examiners should ensure that a banking organization is in compliance with the terms of section 312.

OPERATIONAL (TRANSACTION) RISK

In the context of payment systems, operational risk is the risk of loss resulting from inadequate or failed internal processes, systems, and staff, or from external events. Operational risk includes various physical and information security risks. Institutions should address operational risk by adopting the appropriate internal and operating controls, information security policies and controls, operational resiliency policies and resources, and by comprehensively and effectively auditing these policies, controls, and

resources. Institutions should ensure all policies, controls, and resources are sufficient to meet all regulatory expectations.²⁷

INTERNAL AND OPERATIONAL CONTROLS

Management should consider implementing a variety of specific measures to mitigate or limit operational risks, such as authentication and encryption techniques to ensure the authenticity of the payer and payee as well as prevent unauthorized access to information in transit; and edit checks and automated balancing to verify the integrity of the information relative to the payment order and funds transfer transaction. Additional controls include the use of certified tamper resistant equipment, logical access controls to verify transactions, verification of account balances, and the logging of all transactions and attempts to make a transaction.

Additional internal control measures that management should employ to mitigate wholesale payment system risk include:

- Dual custody and separation of duties for critical payment transaction processing and accounting tasks;
- Payment data verification;
- Clear error processing and problem resolution procedures; and
- Confidential and tamper resistant mailing procedures for bankcards and other sensitive material.

The operational controls for funds transfer operations require clearly defined procedures establishing a control environment which provides for the authorization and authentication of transactions. Financial institutions should establish effective operational controls that identify and document:

- The original payment instructions from the corporate or individual customer to the financial institution and other pertinent information (e.g., account officer, branch manager, terminal entry identity, automated interface identification);
- Every transfer point of data for each step of the manual process (e.g., account officer, message receipt, authentication, data entry, and payment release); and
- Every transfer point of data for each step of an automated process (e.g., SWIFT and Telex, message preparation, data entry, and payment release).

Basic internal controls should be in effect to maintain overall integrity for any funds transfer operation. However, depending on the complexity and volume of operations, certain steps may not be applicable for some institutions. Recommended control objectives for a wholesale funds transfer system include:

²⁷ See Appendix F for a discussion of the “Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.”

- Verifying the accuracy and completeness of the outgoing instruction;
- Protecting original instructions from loss or alteration;
- Authenticating the identity and authority of the sender;
- Ensuring collected balances are available and held for the outgoing payments;
- Ensuring the original unaltered outgoing instruction is entered into the internal accounting system;
- Maintaining a physically secure environment; and
- Maintaining appropriate separation of duties for employees involved in the payment process.

Financial institutions should have funds transfer policies and procedures addressing both the processing of funds transfer messages and the related standards for creating and maintaining source documents. Policies and procedures should include documentation describing all interfaces between the funds transfer application and other back office and customer-related banking processes, and should address the controls relating to crediting, debiting, and reconciling customer and institution account balances. Policies and procedures should also document institution specific compliance requirements to address federal and state regulations including OFAC verification procedures.

AUDIT

A financial institution's internal auditors should conduct periodic independent reviews of the funds transfer operation, including all pertinent internal policies and procedures. An external audit can supplement or replace internal audit procedures. Financial institution audits should verify the effectiveness of the funds transfer control environment and identify funds transfer deficiencies for correction.

Examiners should perform an evaluation of the institution's audit function to determine whether audit activities related to funds transfer operations are comprehensive and effective. Examiners also should review the auditor's opinion of the adequacy of accounting records and internal controls for funds transfer operations. The review of audit procedures should focus on:

- The scope and frequency of the internal funds transfer audit program;
- The effectiveness of audit procedures in determining any control/operating problems disclosed since the previous examination and what corrective measures management has taken;
- Audit work papers to ensure they document adherence to prescribed audit procedures;
- IT audit coverage of new system enhancements and development projects; and
- External audit findings and recommendations.

INFORMATION SECURITY

A financial institution's information security program should include an effective risk assessment methodology that includes an evaluation of risks relating to performing high-risk activities such as funds transfer and other payment-related activities. Management should use risk assessments based on a periodic review of high-risk activities to develop effective standards for adequate separation of duties, physical security, and logical access controls based on the concept of "least possible privilege." Refer to the *IT Handbook's* Information Security Booklet for more detail.

Management should establish logical access controls on the funds transfer application that assign appropriate access levels to staff members working in the wire room or funds transfer operation. Inappropriate access levels provide the opportunity to create and transmit unauthorized funds transfer messages. The risk is greater without adequate separation of duties. Management should ensure no employees have access to more than one assigned user code unless the code is under dual control. Management should configure message verification rights to ensure adequate separation of duties between employees initiating and employees verifying and sending funds transfer messages.

BUSINESS CONTINUITY PLANNING (BCP)

Financial institutions should recognize their role in supporting systemic financial market processes (e.g., inter-bank payment systems and key market clearance and settlement activities) and understand that service disruptions at their institution may significantly affect the integrity of key financial markets. Critical markets include, but are not limited to, the markets for federal funds, foreign exchange, commercial paper, and government, corporate, and mortgage-backed securities. Firms that play significant roles in critical financial markets are those that participate in sufficient volume or value such that their failure to perform critical activities by the end of a business day could present systemic risk (see Appendix F).

In addition, financial institutions should coordinate BCP development and testing with all applicable third parties. All financial institutions, especially those that play a major role in critical financial markets, are expected to have sufficient business continuity plans, commensurate with their funds transfer activities. Financial institutions should also coordinate testing with other industry participants. Refer to *IT Handbook's* Business Continuity Planning Booklet for more detail.

VENDOR AND THIRD-PARTY MANAGEMENT

Some financial institutions rely on third party service providers and other financial institutions for wholesale payment system products and services either to enhance the services performed in-house or to offer wholesale payment services that are otherwise not cost effective.

Financial institutions should have adequate due diligence processes, appropriate contract provisions, and service provider monitoring procedures to ensure they conduct wholesale payment operations appropriately. Effective monitoring should include the review of select wholesale payment transactions to ensure they are accurate, reliable, and timely. The integrity and accuracy of wholesale payment transactions depend on the use of proper control procedures throughout all phases of processing, including outsourced functions.

Regardless of whether the financial institution's control procedures are manual or automated, internal controls should address the areas of transaction initiation, data entry, computer processing, and distribution of output reports. Financial institutions should also maintain effective control over service provider access to customer and financial institution information consistent with GLBA 501(b). Contractual provisions should define the terms of acceptable access and potential liabilities in the event of fraud or processing errors. Refer to *IT Handbook's* Outsourcing Technology Services Booklet for more detail.

APPENDIX A: EXAMINATION PROCEDURES

EXAMINATION OBJECTIVE: Examiners should use the Wholesale Payment Systems Examination Procedures to determine the adequacy of the financial institution's payment system risk policies and wholesale payment business processes, including personnel and internal control systems used to mitigate the risks associated with wholesale payment systems. Wholesale payment system services include Fedwire Funds Service funds transfer and book-entry securities; CHIPS; SWIFT; payment messaging systems; net settlement, clearing and settlement systems; internally developed and off-the-shelf funds transfer systems; and web-based payment systems. The examiner's assessment of risk and risk management practices relating to a financial institution's wholesale payment system service should help determine the extent of testing and which procedures to perform. The assessment should consider the effectiveness of formal policies and procedures as well as the financial institution's underlying internal control environment including information security, business continuity and disaster recovery, and management of wholesale payment services outsourced to third parties.

Financial institutions are exposed to numerous credit, liquidity, legal, and operational risks in provisioning wholesale payment system services to counter parties and performing related processing, clearance, and settlement functions in-house and with third parties. Depending on the financial risks, IT related operational (transactional) risks, compliance risks, and complexity of wholesale payment system activity, the examination may require an integrated team approach that includes the knowledge and skills of safety and soundness examiners and IT examiners.

Examiners may incorporate the Examination Procedures as part of either an IT or safety and soundness examination. The Examination Procedures can also be used in its entirety, or can be used in modular fashion, focusing on particular wholesale payment system products or business lines. Depending on the size and complexity of the financial institution or service provider, examiners may tailor the use of the examination procedures. In many cases, they can eliminate certain procedures and still arrive at a conclusion regarding the quality of risk management practices and performance. The examination procedures are structured as follows:

- Tier I objectives and procedures, which evaluate the effectiveness of the financial institution and service provider's wholesale payment systems, internal controls, and risk management processes that may be relied on for the purpose of identifying and managing risks.
- Tier II objectives and procedures, which provide additional validation as warranted by the risks to verify the effectiveness of the financial institution and service provider's wholesale payment systems function.

TIER I EXAMINATION OBJECTIVES AND PROCEDURES

Objective 1: Determine the scope and objectives of the examination of the wholesale payment systems function.

1. Review past reports for comments relating to wholesale payment systems.
Consider:
 - Regulatory reports of examination.
 - Internal and external audit reports.
 - Regulatory reports on and, audit, and information security reports from/on service providers.
 - Trade group, card association, interchange, and clearing house documentation relating to services provided by the financial institution.
 - Supervisory strategy documents, including risk assessments.
 - Examination work papers.
2. Review past reports for comments relating to the institution's internal control environment and technical infrastructure. Consider:
 - Internal controls including logical access controls, data center operations, and physical security controls.
 - Wholesale EFT network controls.
 - Inventory of computer hardware, software, and telecommunications protocols used to support wholesale EFT transaction processing.
3. During discussions with financial institution and service provider management:
 - Obtain a thorough description of the wholesale payment system activities performed, including transaction volumes, transaction dollar amounts, and scope of operations, including Fedwire Funds Service, CHIPS, SWIFT, and all wholesale payment messaging systems in use.
 - Review the financial institution's payment system risk policy and evaluate its compliance with net debit caps and other internally generated self-assessment factors.
 - Identify any wholesale payment system functions performed via outsourcing relationships and determine the financial institution's level of reliance on those services.
 - Identify any significant changes in wholesale payment system policies, personnel, products, and services since the last examination.

4. Review the financial institution's response to any wholesale payment systems issues raised at the last examination. Consider:
 - Adequacy and timing of corrective action.
 - Resolution of root causes rather than specific issues.
 - Existence of outstanding issues.

Objective 2: Determine the quality of oversight and support provided by the board of directors and management.

1. Determine the quality and effectiveness of the financial institution's wholesale payment systems management function. Consider:
 - Data center and network controls over backbone networks and connectivity to counter parties.
 - Departmental controls, including separation of duties and dual control procedures, for funds transfer, clearance, and settlement activities.
 - Compliance with the Federal Reserve's Payment System Risk policies and procedures.
 - Physical and logical security controls designed to ensure the authenticity, integrity, and confidentiality of wholesale payments transactions.
2. Assess management's ability to manage outsourcing relationships with service providers and software vendors contracted to provide wholesale payment system services. Evaluate the adequacy of terms and conditions, and whether they ensure each party's liabilities and responsibilities are clearly defined. Consider:
 - Adequacy of contract provisions including service level and performance agreements.
 - Compliance with applicable financial institution and third party (e.g. Federal Reserve, CHIPS, SWIFT) requirements.
 - Adequacy of contract provisions for personnel, equipment, and related services.
3. Evaluate the adequacy and effectiveness of financial institution and service provider contingency and business recovery plans. Consider:
 - Ability to recover transaction data and supporting books and records based on wholesale payment system business line requirements.
 - Ability to return to normal operations once the contingency condition is over.
 - Confidentiality and integrity of interbank and counter party data in transit and storage.
4. Evaluate wholesale payment system business line staff. Consider:

- Adequacy of staff resources.
 - Hiring practices.
 - Effective policies and procedures outlining department duties.
 - Adequacy of accounting and financial controls over wholesale payment processing, clearance, and settlement activity.
5. Review the disaster recovery plan for the funds transfer system (FTS) to ensure it is reasonable in relation to the volume of activity, all units of the FTS are provided for in the plan, and the plan is regularly tested.

Objective 3: Determine the quality of risk management and support for Payment System Risk policy compliance.

1. Review policies and procedures in place to monitor customer balances for outgoing payments to ensure payments are made against collected funds or established intraday or overnight overdraft limits and payments resulting in excesses of established uncollected or overdraft limits are properly authorized.
2. Review a sample of contracts authorizing the institution to make payments from customers' accounts to ensure they adequately set forth responsibilities of the institution and the customer, primarily regarding provisions of the Uniform Commercial Code Article 4A (UCC4A) related to authenticity and timing of transfer requests.

Objective 4: Determine the quality of risk management and support for internal audit and the effectiveness of the internal audit program for wholesale payment systems.

1. Review the audit program to ensure all functions of the FTS are covered. Consider:
 - Payment order origination (funds transfer requests).
 - Message testing.
 - Customer agreements.
 - Payment processing and accounting.
 - Personnel policies.
 - Physical and data security.
 - Contingency plans.
 - Credit evaluation and approval.
 - Incoming funds transfers.

- Federal Reserve's Payment Systems Risk Policy.
2. Review a sufficient sample of supporting audit work papers necessary to confirm that they support the execution of procedures established in step 1 above.
 3. Review all audit reports related to the FTS and determine the current status of any exceptions noted in the audit report.

CONCLUSIONS

1. Determine the need to proceed to Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.
2. From the procedures performed, including any Tier II procedures performed:
 - Document conclusions related to the quality and effectiveness of the retail payment systems function.
 - Determine and document to what extent, if any, the examiner may rely upon wholesale payment systems procedures performed by internal or external audit.
3. Review your preliminary conclusions with the EIC regarding:
 - Violations of law, rulings, regulations, and third party agreements.
 - Significant issues warranting inclusion as matters requiring board attention or recommendations in the report of examination.
 - Potential impact of your conclusions on URSIT composite and component ratings.
4. Document your conclusions in a memo to the EIC that provides report ready comments for all relevant sections of the FFIEC Report of Examination and guidance to future examiners.
5. Organize work papers to ensure clear support for significant findings and conclusions.

TIER II EXAMINATION OBJECTIVES AND PROCEDURES

Overall Objective: The Tier II examination procedures for Wholesale Payment Systems provide for additional verification procedures to evaluate the effectiveness of the financial institution's internal control processes over its wholesale payment systems, including Fedwire Funds Service funds transfer and book entry securities, CHIPS, SWIFT, payment messaging systems, net settlement, clearing and settlement systems, internally developed and off-the-shelf funds transfer systems, and web-based payment systems. These procedures are designed to assist in achieving examination objectives, and may be used in their entirety or selectively. Examiners should coordinate this coverage with other examiners involved in assessing the institution's information systems, operations, and information security effectiveness to ensure there is an adequate understanding of the control environment as it pertains to the bank's wholesale payment systems.

Objective 1: Determine if management and the board have enacted sufficient controls over funds transfer activity.

1. Determine if management and the board provide administrative direction for the funds transfer function. Ascertain whether:
 - The directors and senior management are informed regarding the nature and magnitude of risks with the institution's funds transfer activities.
 - Management is informed of new systems designs and available hardware for the wire transfer system.
 - The board of directors and/or senior management regularly review and approve any funds transfer limits, and if so, when the limits were last reviewed.
 - Senior management and the board monitor customers with large intraday or overnight overdrafts and analyze the overdrafts along with all other credit exposure to the customer.
2. Determine if the board and management have developed sufficient policies and procedures to ensure that the following are reviewed:
 - Transaction volumes.
 - Adequacy of personnel and equipment.
 - Customer creditworthiness.
 - Funds transfer risk.
3. Determine if the board and senior management develop and support adequate user access procedures and controls for funds transfer requests. Assess whether the institution:

- Maintains a current list of employees approved to initiate funds transfer requests.
 - Has developed and approved an organization plan that shows the structure of the funds management department and limits the number of employees who can initiate or authorize transfer requests.
 - Has a list of authorized employee signatures maintained in a secure environment.
 - Regularly reviews staff compliance with credit and personnel procedures, operating instructions, and internal controls.
 - Requires its senior management receive and review activity and quality control reports which disclose unusual or unauthorized activities and access attempts
4. Determine if management maintains authorization lists from its customers that use the funds transfer system. Verify:
 - Management advises customers to limit the number of authorized signers.
 - There are dual controls or other protections over customer signature records.
 - The authorization list also identifies authorized sources of requests (e.g., telephone, fax, memo, etc.).
 - The customer authorization establishes limits over the amount each signer is authorized to transfer.
 5. Determine if the institution has dual control procedures that prohibit persons who receive transfer requests from transmitting or accounting for those requests.

Objective 2: Determine the adequacy of the internal and external audit reviews of the funds transfer area.

1. Review the internal and external audit function to determine if the scope and frequency of audit review for the funds transfer area is adequate. Review:
 - Whether internal auditors have expertise or training in funds transfer operations and controls.
 - The frequency and scope of internal and external audit reviews of the funds transfer function.
 - Whether the internal and external audits provide substantive testing or quantitative measurements of the following areas:
 - Personnel policies.
 - Operating policies (including segregation of duty and dual controls).
 - Customer agreements.
 - Contingency plans.

- Physical security.
 - Logical security (user access, authentication, etc.).
 - Sample tests for message and recordkeeping accuracy.
 - Processing.
 - Balance verification and overdraft approval.
2. Obtain and review internal and external audit reports to ensure they provide an adequate appraisal of the funds transfer function to management.
 3. Review management's response to audit reports to ensure the institution takes prompt and appropriate corrective action. Ensure there is adequate tracking and resolution of outstanding exceptions.

Objective 3: Determine if there are adequate written documents outlining the funds transfer operating procedures.

1. Obtain the institution's written procedures for employees in the incoming, preparation, data entry, balance verification, transmission, accounting, reconciling and security functions of the funds transfer area. Determine if management reviews and approves the procedures periodically. Determine if the procedures address:
 - Control over test words, signature lists, and opening and closing messages.
 - Origination of funds transfer transactions and the modification and deletion of payment orders or messages.
 - Review of rejected payment orders or messages.
 - Verification of sequence numbers.
 - End of day accounting for all transfer requests and message traffic.
 - Controls over message or payment orders received too late to process in the same day.
 - Controls over payment orders with future value dates.
 - Supervisory review of all adjustments, reversals, reasons for reversals and open items.

Objective 4: Determine the adequacy of institution controls over funds transfer requests.

1. Determine if institution personnel use standard, sequentially numbered forms to initiate funds transfer requests.
2. Determine if the institution has an approved request authentication system.

3. Determine if the institution has adequate security procedures for requests received from customers via telex, on-line terminals, telephone, fax, or written instructions. Determine if management:
 - Developed policies and procedures to verify the authenticity of requests (e.g., call backs, customer authentication, signature verification).
 - Maintains a current record of authorized signers for customer accounts.
4. Determine if the institution records incoming and outgoing telephone transfer requests. Also determine if the institution notifies the customer that calls are recorded (e.g., through written contracts, audible signals).
5. Determine if the institution maintains sequence control internally for requests processed by the funds transfer function.
 - Review a sample of incoming and outgoing messages to determine if they are time stamped or sequentially numbered for control. If not, determine if the institution maintains an unbroken copy of all messages received via telex or other terminal printers during a business day.
 - Determine if the sequence records and unbroken copies are reviewed and controlled by an employee independent of the equipment operations.
6. Ascertain whether the financial institution records transfer requests in a log or another bank record prior to execution.
 - Review the logs to determine if supervisory personnel review the record of transfer requests daily.
 - Select a sample of the transfer request log entries and compare them to funds transfer requests for accuracy.
7. Determine if the institution has guidelines for the information to be obtained from a customer making a funds transfer request. The request should contain:
 - The account name and number.
 - A sequence number.
 - The amount to be transferred.
 - The person or source initiating the request.
 - The time and date.
 - Authentication of the source of the request.
 - Instructions for payment.
 - Bank personnel authorization for large dollar amounts.

Objective 5: Determine if there are adequate controls over the institution's use of test keys for authentication.

1. Determine if all message and transfer requests that require testing are authenticated with a test key. If so determine whether:
 - The institution maintains an up-to-date test key file.
 - An agreement between the bank and the customer stipulates that test key formulas incorporate a variable (e.g., sequence number).
 - There is a procedure in place for an employee (independent of testing the authenticity of transfer requests) to issue and cancel test keys.
 - Test codes are verified by an employee who does not receive the initial transfer request.
2. Obtain and review management's test key user access list to determine if:
 - There are dual controls or other protections over files containing test key formulas.
 - Only authorized personnel have access to the test key area or to terminals used for test key purposes.

Objective 6: Determine if agreements concerning funds transfer activities with customers, correspondent banks, and service providers are adequate and clearly define rights and responsibilities.

1. Obtain any material agreements or contracts concerning funds transfer services between the financial institution and correspondent banks, service providers and operators (e.g., Federal Reserve Bank and CHIPS). Review the agreements to determine if they:
 - Establish responsibilities and accountability among all parties.
 - Establish recovery time objectives in the event of failure.
 - Outline the other party's liability for actions of its employees.
2. Obtain a sample of customer agreements regarding funds transfer activity and review it for compliance with applicable sections of the Uniform Commercial Code. Consider if:
 - Agreements adequately describe security procedures as defined by UCC Article 4A Sections 201 and 202.
 - The bank obtains written waivers from its customers if they choose security procedures that are different from what is offered by the bank, as indicated in UCC Article 4A Section 202(c).

- Agreements with customers establish cut-off times for receipt and processing of payment orders and canceling or amending payment orders as noted in UCC Article 4A Section 106.

Objective 7: Review the institution's payment processing and accounting controls to determine the integrity of funds transfer data and the adequacy of the separation of duties.

1. Review the institution's reconciliation policies and procedures as they relate to the funds transfer department. Determine if:
 - The funds transfer department prepares a daily reconciliation of funds transfer activity (incoming and outgoing) by dollar amount and number of messages.
 - The funds transfer department performs end-of-day reconciliations for messages sent to and received from intermediaries (e.g., Federal Reserve Bank, servicers, correspondents, and clearing facilities).
 - The daily reconciliations account for all pre-numbered forms, including cancellations.
 - Supervisory personnel review the reconciliations of funds transfer and message requests on a daily basis.
 - The staff responsible for balancing and reconciling daily activity is independent of the receiving, processing, and sending functions.
 - The funds transfer department verifies that work sent to and received from other institution departments agree with its totals.
 - The institution accepts transfer requests after the close of business or with a future value date, and whether there are appropriate processing controls.
2. Determine if the institution's daily processing policies and procedures are adequate to ensure data integrity and independent review of funds transfer activity. Determine if:
 - Supervisory personnel and the originator initial all general ledger tickets or other supporting documents.
 - The institution reviews all transfer requests to determine that they have been properly processed.
 - Independent wire transfer personnel verify key fields before transmission.
 - Staff members independent of entering the messages release funds transfer messages.
 - Employees not involved in the receipt, preparation, or transmittal of funds review all reject and/or exception reports.

3. Determine if there is adequate oversight of the funds transfer department. Ensure:
 - An independent institution department (e.g., accounting or correspondent banking) reviews and reconciles the Federal Reserve Bank, correspondent bank, and clearing house statements used for funds transfer activities to determine if:
 - They agree with the funds transfer departments records.
 - They identify and resolve any *open* funds transfer items.
 - Open statement items, suspense accounts, receivables/payables, and inter-office accounts related to funds transfer activity are controlled outside of the funds transfer operations.
 - Management receives periodic reports on open statement items, suspense accounts, and inter-office accounts that include:
 - Aging of open items.
 - The status of significant items.
 - Resolution of prior significant items.
 - An officer reviews and approves corrections, overrides, open items, reversals, and other adjustments.
4. Determine if the institution has documented any operational or credit losses that it has incurred, the reason the losses occurred, and actions taken by management to prevent future loss occurrences.
5. Determine if the institution maintains adequate records as required by the Currency and Foreign Transactions Reporting Act of 1970 (also known as the Bank Secrecy Act) and the USA PATRIOT Act.

Objective 8: Determine the adequacy of the institution's personnel policies governing the funds transfer function.

1. Obtain and review the institution's personnel policies to assess the procedures and controls over hiring new employees. Determine if:
 - The bank conducts screening and background checks on personnel hired for sensitive positions in the funds transfer department.
 - The bank prohibits new employees from working in sensitive areas of the funds transfer operation without close supervision.
 - The institution limits or excludes temporary employees from working in sensitive areas without close supervision.

2. Assess management's personnel policies regarding current employees in the funds transfer department. Determine if:
 - Management obtains statements of indebtedness of employees in sensitive positions of the funds transfer function.
 - Employees are subject to unannounced rotation of responsibilities.
 - Relatives of employees in the funds transfer function are precluded from working in the institution's bookkeeping, audit, data processing, and/or funds transfer departments.
 - The institution enforces a policy that requires employees to take a minimum number of consecutive days as part of their annual vacation.
 - There are policies and procedures to reassign departing employees from sensitive areas of the funds transfer function and to remove user access profiles of terminated employees as soon as possible.

Objective 9: Determine if the institution has enacted sufficient physical and logical security to protect the data security of the funds transfer department.

1. Obtain, review, and test the policies and procedures regarding the physical security of the funds transfer department. Determine if:
 - Management restricts access to the funds transfer area to authorized personnel. Identify and assess the physical controls (e.g., locked doors, sign-in sheets, terminal locks, software locks, security guards) that prevent unauthorized physical access.
 - There is an up-to-date funds transfer area visitors log and whether visitors are required to sign in and be accompanied while in restricted areas.
 - There are adequate controls over the physical keys used to access key areas and key equipment within the funds transfer department.
2. Obtain and review policies and procedures regarding wire transfer password controls to determine if they are adequate. Consider whether:
 - Management requires operators to change their passwords at reasonable intervals.
 - Management controls access to master password files ensuring that no one has access to employee passwords.
 - Passwords are suppressed on all terminal displays.
 - Policy requires that passwords meet certain strength criteria so they are not easily guessed.
 - Management maintains required generic system account passwords under dual control.

- Terminated or transferred employees access is removed as soon as possible.
 - Access levels and who has passwords is periodically reviewed for appropriateness.
3. Review funds transfer system user access profiles to ensure that:
- User access levels correspond to job description.
 - Management appropriately limits user access to the funds transfer system and periodically reviews the access limits for accuracy.
 - There are adequate separation of duties and access controls between funds transfer personnel and other computer areas or programs.
4. Review the institution's access controls to determine if terminals in the funds transfer area are shut down or locked out when not in use or after business hours. Determine:
- The adequacy of time out controls.
 - The adequacy of time of day controls.
 - Whether supervisory approval is required for access during non-work hours.
5. Determine if the institution's training program adequately protects the integrity of funds transfer data. Ensure:
- The institution conducts training in a test environment that does not jeopardize the integrity of live data or memo files.
 - There are adequate controls to protect the confidentiality of data housed in the test environment.
 - There are procedures and controls to prevent the inadvertent release of test data into the production environment, thus transferring live funds over the system.

Objective 10: Review the adequacy of backup, contingency, and business continuity plans for the funds transfer function.

1. Obtain the institution's written contingency and business continuity plans for partial or complete failure of the systems and/or communication lines between the bank and correspondent bank, service provider, CHIPS, Federal Reserve Bank, and data centers. Consider if:
- The procedures, at a minimum, ensure recovery by the opening of the next day's processing depending on the criticality of this function to the institution.
 - The contingency plans are reviewed and tested regularly.
 - Management has distributed these plans to all funds transfer personnel.

- There are procedures to secure sensitive information and equipment before evacuation (if time permits) and security personnel adequately restrict further access to the affected areas.
 - The plan includes procedures for returning to normal operations after a contingency.
2. Review the institution's policies and procedures regarding back-up systems. Assess whether:
 - The institution maintains adequate back-up procedures and supplies for events such as equipment failures and line malfunctions.
 - Supervisory personnel approve the acquisition and use of back-up equipment

Objective 11: Determine if the institution adequately monitors intraday and overnight overdrafts. Ensure that management applies appropriate credit standards to customers that incur overdrafts.

1. Determine if management has developed procedures to approve customer use of daylight or overnight overdrafts including assigning appropriate approval authority to officers. Obtain and review a list of officers authorized to approve overdrafts and their approval authority, a current list of borrowers authorized to incur daylight and overnight overdrafts, and a sample of overdraft activity. Determine if:
 - Management has established limits for each customer allowed to incur intraday and overnight overdrafts.
 - The institution has assigned overdraft approval authority to officers with appropriate credit authority. Ensure that:
 - Payments that exceed the established limits are referred to an officer with appropriate credit authority for review and approval before release.
 - Payments made in anticipation of the receipt of covering funds are approved by an officer with appropriate authority.
 - Management assesses all of a customer's credit facilities and affiliated relationships in determining overdraft limits.
 - The institution routinely reviews and updates the institution and customer limits as well as officer approval authority.
2. Review the institution's policies and procedures regarding overdrafts to ensure it prohibits transfers of funds against accounts that do not have collected balances or preauthorized credit availability. Determine if:

- Supervisory personnel monitor funds transfer activities during the business day to ensure that payments in excess of approved limits are not executed without proper approval.
 - An intraday record is kept for each customer showing opening collected and uncollected balances, transfers in and out, and whether the collected balances are sufficient at the time payments are released.
 - The cause of any violations of overnight overdraft limits is identified and documented.
 - Intraday exposures are limited to amounts expected to be received the same day.
 - Adequate follow-up is made to obtain the covering funds in a timely manner.
3. If required as a participant of a net settlement system, determine whether management sets and approves bi-lateral credit limits on a formal credit analysis.
 4. If the institution is an Edge Act Corporation, determine whether intraday and overnight overdrafts comply with Regulation K.

Objective 12: Review and determine the adequacy of the institution's controls over incoming funds transfers.

1. Review policies and procedures regarding incoming funds transfers. Select a sample of incoming funds transfers and review them to determine if:
 - The institution maintains separation of duties over receipt of instructions, posting to a customer's account, and mailing customer credit advices.
 - OFAC verification is performed.
 - There are adequate audit trails maintained from receipt through posting the transfer to a customer's account.
 - Procedures ensure accuracy of accounting throughout the process.
 - Customer advices are issued in a timely manner.
 - Any funds transfer requests received via telex, telephone or fax are authenticated prior to processing.

Objective 13: Determine if the institution complies with the Federal Reserve Policy Statement on Payments System Risk.

1. Determine if the institution incurs overdrafts in its Federal Reserve account. If so, consider if:
 - The institution has reviewed and complied with the Payment System Risk program (i.e., the institution selected an appropriate net debit cap).

- The institution has elected a de minimis or self-assessed net debit cap and ensure that the examination evaluates the adequacy of records supporting the accuracy of the de minimis or self-assessed rating.

Objective 14: Review the institution's policies and procedures regarding the release of payment orders to assess the adequacy of controls.

1. Determine whether all incoming and outgoing payment orders and messages are received in the funds transfer area.
2. Obtain a sample of payment orders. Determine if the payment orders are:
 - Logged as they enter the funds transfer department.
 - Time stamped or sequentially numbered for control.
 - Reviewed for signature authenticity.
 - Reviewed for test verification, if applicable.
 - Reviewed to determine whether personnel who initiated each funds transfer have the authority to do so.
3. Determine if current lists of authorized signatures are maintained in the wire transfer area. Ensure the lists indicate the amount of funds that individuals are authorized to release.
4. Assess whether there are adequate dual controls over the review of payment orders and message requests. Determine whether an independent employee reviews the requests for the propriety of the transaction and for future dates, especially on multiple transaction requests.

Objective 15: Coordinate the review of wholesale payment systems with examiners in charge of reviewing other information technology risks.

1. In discussion with other examiners, ensure that management applies corporate-wide, information technology policies and procedures (i.e. development and acquisition, operational security, environmental controls, etc.) to the funds transfer department. If any discrepancies exist, determine their severity and document any corrective actions.

APPENDIX B: GLOSSARY

Aggregate Short Position	The sum of a Settlement Member's short positions, each such short position expressed in its base currency equivalent and adjusted by the applicable haircut.
Aggregate Short Position Limit	In respect of a Settlement Member, the maximum aggregate short position that such Settlement Member is permitted to incur at any time.
Authentication	The process of verifying the identity of an individual user, machine, software component, or any other entity.
Automated Clearing House (ACH)	An electronic clearing system in which a data processing center handles payment orders that are exchanged among financial institutions, primarily via telecommunications networks. ACH systems process large volumes of individual payments electronically. Typical ACH payments include salaries, consumer and corporate bill payments, interest and dividend payments, and Social Security payments.
Automated Teller Machine (ATM)	An Electronic Funds Transfer (EFT) terminal that allows customers using a pin-based debit (ATM) card to initiate transactions (e.g., deposits, withdrawals, account balance inquiries).
Bankcard	A general-purpose credit card, issued by a financial institution under agreement with the bankcard associations (Visa and MasterCard), which customers can use to purchase goods and services and to obtain cash against a line of credit established by the bankcard issuer.
Bilateral Key Security	A multi-level data encryption system, based on the exchange of Bilateral Keys, allowing users of SWIFT to create, send, and receive SWIFT messages. Bilateral Keys are unique authenticator keys possessed by only the two parties (either the provider or recipient of a message) involved and provide confirmation in both directions of the legitimacy of a message sent via SWIFT.
Check	A written order from one party (payer) to another (payee) requiring the payer's financial institution to pay a specified sum on demand to the payee or to a third party specified by the payee.
Clearance	The process of transmitting, reconciling, and in some cases, confirming payment orders or financial instrument transfer instructions prior to settlement.
Compared and Noncompared Transaction	See <i>Matching</i> .

Consumer	Usually refers to an individual engaged in non-commercial transactions.
Correspondent Bank	An institution, acting on behalf of other institutions, that can settle the checks they collect for other institutions (respondents) by using accounts on their books or by sending a wire funds transfers. Generally, a provider of banking and payment services to other financial institutions.
Credit Card	A card indicating the holder has been granted a line of credit. It enables the holder to make purchases or withdraw cash up to a prearranged ceiling. The credit granted can be settled in full by the end of a specified period or can be settled in part, with the balance taken as extended credit. Interest is charged based on the terms of the credit card agreement and the holder is sometimes charged an annual fee.
Currency Balance	As at the time calculated, the current amount (positive or negative) of a particular eligible currency included in an account, as indicated on the books and records of CLS Bank. A currency balance is not a separate account.
Daylight Overdraft	A daylight overdraft occurs at any point in the business day when the balance in an institution's account becomes negative. Daylight overdrafts can occur in accounts at Federal Reserve Banks as well as at private financial institutions. Daylight credit can also arise in the form of net debit positions of participants in private payment systems. A daylight overdraft occurs at a Federal Reserve Bank when there are insufficient funds in an institution's Federal Reserve Bank account to cover outgoing funds transfers or incoming book-entry securities transfers. An overdraft can also be the result of other payment activity processed by the Federal Reserve Bank, such as check or automated clearinghouse transactions.
Depository	An institution that holds funds or marketable securities for safekeeping. Depositories may be privately or publicly operated, allow securities transfers through book-entry, and offer funds accounts permitting funds transfers as a means of payment.
Electronic Funds Transfer (EFT)	A generic term describing any transfer of funds between parties or depository institutions via electronic data systems.

Electronic Funds Transfer Act (EFTA)	The Electronic Funds Transfer Act and Regulation E are designed to ensure adequate disclosure of basic terms, costs, and rights relating to electronic fund transfer (EFT) services provided to consumers. Institutions offering EFT services must disclose to consumers certain information, including: initial and updated EFT terms, transaction information, periodic statements of activity, the consumer's potential liability for unauthorized transfers, and error resolution rights and procedures. EFT services include automated teller machines, telephone bill payment, point-of-sale transfers in retail stores, fund transfers initiated through the Internet, and pre-authorized transfers to or from a consumer's account.
Encryption	A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.
Federal Reserve Banks	The Federal Reserve Banks provide a variety of financial services including retail and wholesale payments. The Federal Reserve Bank operates a nationwide system for clearing and settling checks drawn on depository institutions located in all regions of the United States.
Fedwire® Funds Service	The Federal Reserve Banks' high-speed electronic funds transfer system. As a real-time gross settlement system, the Fedwire® Funds Service processes and settles individual payments between participants immediately in central bank money. Once processed, these payments are final.
Fedwire® Securities Service	The Federal Reserve Banks' high-speed electronic payments system for maintaining securities accounts and for effecting securities transfers. The Fedwire® Securities Service provides a real-time, delivery-versus-payment (DVP), gross settlement system that allows for the immediate, simultaneous transfer of securities against payment. Once processed, securities transfers are final.
FIN (Financial Application)	The SWIFT application within which all SWIFT user-to-user messages are input and output.
Finality	Irrevocable and unconditional transfer of payment during settlement.
Haircut	With respect of an eligible currency, the percentage increase of a negative currency balance or reduction of a positive currency balance and is based on (a) the volatility of the historic foreign exchange movements in the applicable eligible currency determined by CLS Bank and (b) an add-on component.

Instruction	Means (i) any instruction submitted by a Member through the submission process directing CLS Bank to settle certain payment entitlements and obligations arising pursuant to an FX transaction eligible for settlement in CLS Bank and (ii) any instructions resulting from the split of Settlement Eligible Instructions.
Internet	A worldwide network of computer networks, governed by standards and protocols developed by the Internet Engineering Task Force (IETF).
Large Value Funds Transfer System	A wholesale payment system used primarily by financial institutions in which large values of funds are transferred between parties. Fedwire® and CHIPS are the two large-value transfer systems in the United States.
Long Position	In respect of a currency balance that is greater than zero, the amount by which such currency balance is greater than zero. A position that appreciates in value if market prices increase. When one buys a currency, their position is long.
Matched Instructions	Two Instructions in which the information set forth in a specific CLS Bank Rule is matched in accordance with the parameters and procedures set forth in the CLS Bank Rules
Matching	With respect to compared and non-compared transactions, the process of comparing the trade or settlement details provided by counterparties to ensure they agree with respect to the terms of the transaction. Also called comparison checking.
National Settlement Service (NSS)	The Federal Reserve Banks' multilateral settlement service. NSS is offered to depository institutions that settle for participants in clearinghouses, financial exchanges, and other clearing and settlement groups. Settlement agents acting on behalf of those depository institutions electronically submit settlement files to the Federal Reserve Banks. Files are processed on receipt, and entries are automatically posted to the depository institutions' Reserve Bank accounts. Entries are final when posted
Net debit cap	The maximum dollar amount of daylight overdrafts an institution is permitted to incur in its Federal Reserve account at any point in the day or on average over a two-week period. The net debit cap is generally equal to an institution's capital times the cap multiple for its cap category.

Office of Foreign Asset Control (OFAC)	The Office of Foreign Assets Control, United States Department of the Treasury, administers and enforces economic sanctions programs primarily against countries and groups of individuals such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.
Open Market Operations	The buying and selling of government securities in the open market in order to expand or contract the amount of money in the banking system.
Originating Depository Financial Institution (ODFI)	A participating financial institution that originates entries at the request of and by agreement with its originators in accordance with the provisions of the NACHA rules.
Originator	A person that has authorized an ODFI to transmit a credit or debit entry to the deposit account of a receiver at an RDFI.
Payment	A transfer of value.
Payment System	The mechanism, the rules, institutions, people, markets, and agreements that make the exchange of payments possible.
Payments System Risk Policy (PSR)	The Federal Reserve's Payments System Risk (PSR) policy addressing the risks that payment systems present to the Federal Reserve Banks, the banking system, and to other sectors of the economy.
Real-Time Gross Settlement (RTGS) System	A type of payments system operating in real-time rather than batch processing mode. It provides immediate finality of transactions. Gross settlement refers to the settlement of each transfer individually rather than netting. Fedwire® is an example of a real-time gross settlement system.
Receiver	An individual, corporation, or other entity that has authorized a company or an originator to initiate a credit or debit entry to a transaction account held at its RDFI.
Receiving depository financial institution (RDFI)	Any financial institution qualified to receive debits or credits through its ACH operator in accordance with the ACH rules.
Regulation E	A regulation (12 CFR 205) promulgated by the Board of Governors of the Federal Reserve System to ensure consumers a minimum level of protection in disputes arising from electronic fund transfers.

Reserve Account	A non-interest earning balance account institutions maintain with the Federal Reserve Bank or with a correspondent bank to satisfy the Federal Reserve's reserve requirements.
Retail Payments	Small-dollar payments made in the goods and services market.
Security Procedure Agreement	An agreement between a financial institution and a Federal Reserve Bank whereby the financial institution agrees to certain security procedures if it uses an encrypted communications line with access controls for the transmission or receipt of a payment order to or from a Federal Reserve Bank.
Settlement	The final step in the transfer of ownership involving the physical exchange of securities or payment. In a banking transaction, settlement is the process of recording the debit and credit positions of the parties involved in a transfer of funds. In a financial instrument transaction, settlement includes both the transfer of securities by the seller and the payment by the buyer. Settlements can be "gross" or "net." Gross settlement means each transaction is settled individually. Net settlement means parties exchanging payments will offset mutual obligations to deliver identical items (e.g., dollars or Euros), at a specified time, after which only one net amount of each item is exchanged.
Settlement Eligible Instructions	See Matched Instructions.
Short Position	In respect of a currency balance that is less than zero, the amount by which such currency balance is less than zero. An investment position that benefits from a decline in market price. When one sells a currency their position is short.
Short Position Limit	In respect of an eligible currency, the maximum short position a Settlement Member may have at any time in that eligible currency and, unless otherwise reduced pursuant to the CLS Bank Rules, shall equal (i) the total amount of all available committed liquidity facilities in such eligible currency (or such lesser amount that CLS Bank may determine from time to time) minus (ii) the amount of the largest available committed liquidity facility among such liquidity facilities (after taking into account any amounts already drawn.
Spot	The most common foreign exchange transaction. Spot or spot date refers to the spot transaction value date that requires settlement within two business days, subject to value date calculation.

Test Key	Internal controls used to verify the authenticity of incoming wire requests involve the use of test keys. A test key is a formula used to develop or interpret test codes or test words. Test codes or words consist of a series of numbers signifying different types of information and usually precede the text of the message. As an example, a test code may contain a bank number, the amount of the transaction, and a number indicating the day and week of the month. As an additional precaution, many test codes contain a variable (sequence number) based on the number of messages received.
XML	XML (Extensible Markup Language) is a "metalanguage" – a language for describing other languages – which lets you design your own customized markup languages for different types of documents. It is designed to improve the functionality of the Web by providing more flexible and adaptable information identification.

APPENDIX C: LAWS, REGULATIONS AND GUIDANCE

Laws

- 12 USC 248(i), (j), and (o), 342,360,464, and 4001 – 4010: Federal Reserve Act

FEDERAL RESERVE BOARD

REGULATIONS

- 12 CFR Part 210, Subpart B, Funds Transfers Through Fedwire (Regulation J)

APPENDIX D: LEGAL FRAMEWORK FOR INTERBANK PAYMENT SYSTEMS

State and federal statutes, regulations, and case law govern the payment systems in the United States. The relevant legal principles depend on the method of payment (paper-based or electronic) and in some cases the status of parties to a payment (consumer, merchant, or financial institution). Several federal laws apply to payment activities, particularly in the consumer sector. At the state level, the Uniform Commercial Code (UCC) establishes a set of model statutes governing certain commercial and financial activities, including some banking and securities market transactions. Articles of the UCC pertinent to payment and settlement activities are the following: Article 3 (negotiable instruments), Article 4 (bank deposits and collections), Article 4A (funds transfers, including wholesale ACH credit transfers) and Article 8 (investment securities).²⁸

Every state has incorporated these Articles, sometimes with local variations, into the state laws. In addition, the rules and membership agreements of private clearing and settlement arrangements provide a contractual framework for payment activity within the relevant governing law.

Fedwire Funds Service

The Federal Reserve's Regulation J governs payment transactions using the Fedwire Funds Service and incorporates the requirements of Article 4A of the UCC. The Regulation, in particular subpart B, defines the rights and responsibilities of financial institutions that use Fedwire, as well as the rights and responsibilities of the Federal Reserve Bank. Federal Reserve Bank Operating Circular 6 covers items such as Fedwire operating hours, security, authentication, fees, and certain restrictions.²⁹ It also contains time schedules, holidays, and guidelines pertaining to the extension of Fedwire hours.

Under subpart B of Regulation J and Operating Circular 6, the Federal Reserve Banks can impose conditions on an institution's use of Fedwire. In particular, the regulation and operating circular require each Fedwire participant to enter into a security procedure agreement with its Federal Reserve Bank and includes institution responsibilities for information security, business continuity, and related administrative information.

Federal Reserve Regulation CC, Availability of Funds and Collection of Checks, also regulates the time within which a depository institution receiving a Fedwire or CHIPS funds transfer on behalf of a customer must make those funds available to its customer.

²⁸ Article 4A does not apply to a funds transfer, any part of which is governed by the Electronic Funds Transfer Act of 1978, implemented as Federal Reserve Regulation E (12 CFR part 205). Fedwire funds transfers to or from consumer accounts are exempt from the Electronic Funds Transfer Act and Regulation E.

²⁹ Federal Reserve Operating Circulars are available at <http://www.frb services.org/OperatingCirculars/index.html>.

National Settlement Service (NSS)

Federal Reserve Bank Operating Circular 12 establishes the terms and conditions under which participants using NSS submit settlement files to the Federal Reserve Banks. The provision of intraday settlement finality is similar to the Fedwire Funds Service and enables the Federal Reserve Banks to manage and limit settlement risk by incorporating risk controls on extensions of daylight credit.

Messaging Systems

Payment messaging systems allow financial institutions to initiate payment orders, providing that the institution is authorized to act on behalf of its customers. It is important for financial institutions to establish the authenticity and time of receipt of payment order messages. UCC4A establishes responsibility for the execution of a payment order and requires financial institutions to agree to the terms and conditions established by the responsible messaging system with respect to security procedures.

CHIPS

Funds transfers made through CHIPS are subject to CHIPS rules and procedures. The CHIPS rules stipulate that the laws of the state of New York, which include Article 4A of the UCC, also apply to CHIPS transactions. CHIP Co. is not responsible for losses resulting from system errors. Each participant agrees to indemnify and to hold harmless CHIPS from such losses. Any participant losses are settled by a loss sharing agreement, and if a participant commits a fraud, that participant will bear the loss. CHIP Co. maintains a financial institution bond for possible employee fraud. Losses exceeding CHIPS's bond coverage are shared on a pro rata basis of each participant's average daily CHIPS usage for the 30-day calendar period preceding the notice of loss to the underwriters of the bond.

APPENDIX E: FEDERAL RESERVE BOARD PAYMENT SYSTEM RISK POLICY: DAYLIGHT OVERDRAFTS

Similar to financial institutions offering retail payment services to customers, the Federal Reserve Banks are exposed to credit risk when they process payments for financial institutions holding reserve accounts. The Federal Reserve Banks guarantee payment finality for financial institutions using their systems for Fedwire Funds, NSS, and ACH credit originations. Due to this payment guarantee, the Federal Reserve Banks may incur losses when institutions fail with overdrafts in their accounts.

An integral component of the Federal Reserve's Payments System Risk (PSR) policy controls and reduces the use of Federal Reserve Banks' daylight overdrafts and the Federal Reserve Banks' associated credit risk.³⁰ The PSR policy addresses daylight overdrafts that occur in accounts at Federal Reserve Banks as well as at financial institutions. A daylight overdraft occurs when an institution's Federal Reserve Bank account is in a negative position during the business day.

To control daylight overdrafts, the PSR policy establishes limits, or net debit caps, on the amount of Federal Reserve Bank daylight credit that a depository institution may use during a single day and over a two-week reserve maintenance period. These limits are sufficiently flexible to reflect the overall financial condition and operational capacity of each institution using Federal Reserve Bank payment services. The policy also permits the Federal Reserve Banks to protect themselves from the risk of loss by unilaterally reducing net debit caps, imposing collateralization or clearing-balance requirements, rejecting or delaying certain transactions until sufficient balances exist, or prohibiting an institution from using Federal Reserve Bank payment services.

The PSR policy established daylight overdraft fees to provide a financial incentive for institutions to control their use of Federal Reserve Bank intraday credit and to recognize the risks inherent in the provision of intraday credit. Daylight overdraft fees induce financial institutions to make business decisions concerning the amount of Federal Reserve Bank intraday credit they are willing to use based on the cost of using that credit. The daylight overdraft measurement method, which incorporates a set of nearly real time

³⁰ See <http://www.federalreserve.gov/paymentsystems/psr/default.htm>.

transaction posting rules, also supports institutions in controlling their use of Federal Reserve Bank intraday credit.

The Federal Reserve Banks use the Account Balance Monitoring System (ABMS) to monitor financial institution accounts intraday. For a limited number of institutions, the system is also used to prevent those institutions from incurring daylight overdrafts in their Federal Reserve Bank accounts beyond a certain threshold (often set to zero) for Fedwire Funds, NSS, and ACH credit origination transactions. In this situation, credit ACH transactions are required to be prefunded, including those settled on behalf of any respondents. If there are insufficient funds available in the account, the batch will reject and a notice will be sent to the ACH sending point and to the settlement financial institution.³¹

³¹ See *IT Handbook* “Retail Payment Systems Booklet” for additional information on NSS and PSR policy.

APPENDIX F: PAYMENT SYSTEM RESILIENCY

The “Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System” identifies sound practices focusing on minimizing the immediate systemic effects of a wide-scale disruption to critical financial markets. The sound practices focus on the appropriate back-up capacities necessary for recovery and resumption of clearance and settlement activities for material open transactions in wholesale financial markets.³²

The agencies, in promoting resiliency, have identified four broad sound practices for core clearing and settlement organizations and firms that play significant roles in critical financial markets. The practices involve:

- Identifying clearing and settlement activities in support of critical financial markets.
- Determining appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets.
- Maintaining sufficient geographically dispersed resources to meet recovery and resumption objectives.
- Routinely using or testing recovery and resumption arrangements.

The sound practices discussed in this paper supplement the agencies’ respective policies and other guidance on business continuity planning.

³² See SR Letter 03-9, dated May 28, 2003, Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, for further information. The agencies included the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.