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 entity's AIO functions and their related activities. Examiners are not limited[1] 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.

	Work Paper Ref	Examiner Comments
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).		

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

	Work Paper Ref	Examiner Comments
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. 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.		

	Work Paper Ref	Examiner Comments
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 fromother 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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
▪ 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:		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
▪ 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		

	Work Paper Ref	Examiner Comments
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")		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
▪ 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")		
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		

	Work Paper Ref	Examiner Comments
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:		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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).		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
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)		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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)		

	Work Paper Ref	Examiner Comments
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: o Defining acceptable use (or restriction) guidelines and documenting a process for modifying and reviewing the code. o Restricting access to unapproved shareware sites.		

	Work Paper Ref	Examiner Comments
○ 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 its 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		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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).		

	Work Paper Ref	Examiner Comments
▪ 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		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
▪ 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:		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
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.		

AUDIT 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

	Work Paper Reference	Comment
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		

	Work Paper Reference	Comment
▪ 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.

	Work Paper Reference	Comment

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.		

	Work Paper Reference	Comment

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;		

	Work Paper Reference	Comment
▪ 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.		

	Work Paper Reference	Comment

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,		

	Work Paper Reference	Comment
▪ 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		

	Work Paper Reference	Comment
▪ 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		

	Work Paper Reference	Comment
▪ 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.		

	Work Paper Reference	Comment

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.		

	Work Paper Reference	Comment
▪ 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.		

	Work Paper Reference	Comment
▪ 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.		

	Work Paper Reference	Comment
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.		

	Work Paper Reference	Comment
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		

	Work Paper Reference	Comment
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.		

	Work Paper Reference	Comment
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.		

Examiner | Date

Reviewer's Initials

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

	Work Paper Reference	Comment
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;		

	Work Paper Reference	Comment
▪ 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;		

	Work Paper Reference	Comment
▪ 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.		

	Work Paper Reference	Comment

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 reconcilement 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 clearinghouse (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 reconcilement; ▪ 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.		

Examiner | Date

Reviewer's Initials

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.

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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 tests, training, and exercises are comprehensive and consistent with the exercise strategy. g. Resolving weaknesses identified in tests, training, and exercises. h. Meeting regularly to discuss policy changes, training, and testing plans. 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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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 reconcilement 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:		

	Work Paper Ref	Examiner Comments
▪ 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 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.

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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. a. Project or program manager. d. Business change manager. e. Program management office or organization personnel. f. 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.		

	Work Paper Ref	Examiner Comments
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:		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
• 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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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:		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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*		

	Work Paper Ref	Examiner Comments
• 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:		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		
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		

	Work Paper Ref	Examiner Comments
• 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		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.

	Work Paper Ref	Examiner Comments
• 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		

	Work Paper Ref	Examiner Comments
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:		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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)		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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:		

	Work Paper Ref	Examiner Comments
▪ 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.		

	Work Paper Ref	Examiner Comments
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 c. 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. d. Follow processes, after verification of changes, to document completion of the change and close the change request. e. Report on the status of the change after closing and monitor the implemented change for unintended issues. f. Integrate security into its change control processes to help ensure that modifications do not adversely affect the security posture of varying systems. g. 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. h. Perform a post-implementation review to verify that the change was deployed according to the implementation plan and functions appropriately. i. Follow processes after verification to document completion of the change and close the change request.		

	Work Paper Ref	Examiner Comments
j. 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		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
▪ 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: k. 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. l. 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. m. Review reports of emergency modifications periodically for appropriateness of classification. n. Control attempts by personnel to circumvent routine modification or planned change control processes by		

	Work Paper Ref	Examiner Comments
classifying changes as emergencies to avoid resource constraints (e.g., time, personnel, and cost). o. 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		

	Work Paper Ref	Examiner Comments
for all relevant sections of the report of examination and clarifying guidance to future examiners.		
4. Organize work papers to ensure clear support for significant findings by examination objective.		

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.

	Work Paper Ref	Examiner Comments
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 and audit 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 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. 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.		

	Work Paper Ref	Examiner Comments
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,		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.)[1]		
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. 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.		
11. 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.)[2]		

[1] See the *IT Handbook's* "Audit" booklet examination procedures.

[2] See the *IT Handbook's* "Management" booklet examination procedures.

	Work Paper Ref	Examiner Comments
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.		
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.		

	Work Paper Ref	Examiner Comments
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 though 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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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).		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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.) 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		

	Work Paper Ref	Examiner Comments
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. 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.		

	Work Paper Ref	Examiner Comments
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.[3]		
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.[4]		
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,		

[3] See the FFIEC's "Outsourced Cloud Computing" statement.

[4] Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for the MSSP Examination Procedures.

	Work Paper Ref	Examiner Comments
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.		
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.		

	Work Paper Ref	Examiner Comments
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. l. Back-office operations and transaction processing. m. Customer service. n. Systems development and support. o. Internal controls and processes. p. Capacity planning.		
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		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
d. Confidentiality, integrity, and availability of the institution's information. e. Confidentiality of test plans and data. f. Frequency.		
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: 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 examiner-in-charge that provides report-ready comments for all relevant sections of the report of examination and guidance to future examiners.		

	Work Paper Ref	Examiner Comments
4. Organize work papers to ensure clear support for significant findings by examination objective.		

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.

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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,		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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. d. 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. e. 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.		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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,		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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.		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
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).		

	Work Paper Ref	Examiner Comments
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,		

	Work Paper Ref	Examiner Comments
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		

	Work Paper Ref	Examiner Comments
whether the institution has developed the following: e. A process to adequately identify and monitor relevant external threats and vulnerabilities. f. Effective risk monitoring that provides tangible feedback on the quality of the implementation of controls and risk mitigation strategies. g. A reporting process that assembles and reports IT risk-related information in a timely, complete, transparent, and relevant manner. h. 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.		

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 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,
        - 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 and criticality of outsourced services;
   - 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;
   - FIs 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).

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, turnover, 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.
   - 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 reviews, 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 OBJECTIVE 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.

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 reconcilement 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 reconcilement, preparation of general ledger entries, posting to customers accounts, investigations, and reconcilement 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,
     - Reconcilement 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 reconcilement 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 reconcilement 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 reconcilement, preparing general ledger entries, posting to customer accounts, investigations, and reconcilement 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 line, 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 performance and service delivery;
   - 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.

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 Servicefunds 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

	Work Paper Reference	Comment

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		

	Work Paper Reference	Comment
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: Review the financial institution's		

	Work Paper Reference	Comment
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		

	Work Paper Reference	Comment
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. Ability to recover transaction data and supporting books and records based		

	Work Paper Reference	Comment
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		

	Work Paper Reference	Comment
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		

	Work Paper Reference	Comment
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		

	Work Paper Reference	Comment
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. 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 reconcilement policies and procedures as they relate to the funds transfer department. Determine if: ▪ The funds transfer department prepares a daily reconcilement of funds transfer activity (incoming and outgoing) by dollar amount and number of messages. ▪ The funds transfer department performs end-of-day reconcilements for messages sent to and received from intermediaries (e.g., Federal Reserve Bank, servicers, correspondents, and clearing facilities). ▪ The daily reconcilements account for all pre-numbered forms, including cancellations. ▪ Supervisory personnel review the reconcilements 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 if the institution has enacted sufficient physical and logical security to protect the data security of the funds transfer department.

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: 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 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 backup 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.		

Examiner | Date

Reviewer's Initials

_____