FFIEC Information Technology Examination Handbook

Architecture, Infrastructure, and Operations

JUNE 2021

Contents

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

I ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS

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

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

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

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

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

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

II ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS GOVERNANCE

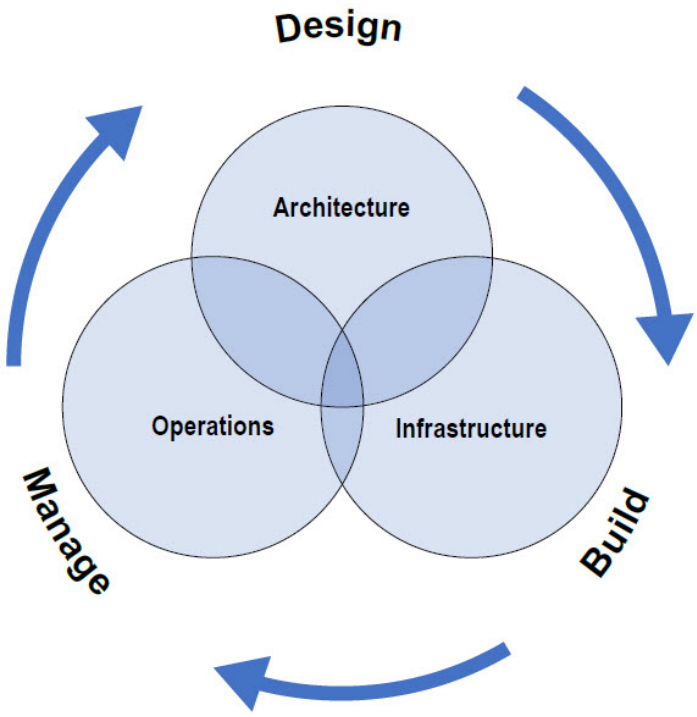
This section provides information about the governance of the AIO functions, including board and senior management responsibilities. General information about governance and risk management is contained in the *IT Handbook's* "Management" booklet and other member agency guidance.

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

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

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

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



II.A Board and Senior Management Responsibilities

Action Summary

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

Examiners should review for the following:

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

The board,[8] or its designated committee, and senior management should consider the entity's business objectives when governing the functions of AIO, including functions performed by affiliates and third-party service providers. Management should identify and evaluate risks

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

associated with AIO, set short- and long-term objectives, and create policies and procedures to mitigate those risks. Furthermore, management should consider security and resilience in the design of new products and services.

Board oversight practices should include the following:

- Aligning AIO principles and practices with the board's strategic plans and risk appetite.
- Budgeting appropriate resources to support AIO activities.
- Ensuring board members have appropriate knowledge of risks to provide a credible challenge[9] to management responsible for AIO functions.
- Enabling appropriate management training on AIO to carry out its responsibilities and manage risk.
- Reviewing AIO operating results and performance through audit reports, testing results, and management assessments and reports.

Management oversight should include the following:

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

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

II.A.1 Strategic Planning

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

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

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

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

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

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

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

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

II.A.2 Enterprise Risk Management

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

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

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

II.B Other Roles and Responsibilities

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

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

II.B.1 IT Management Responsibilities

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

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

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

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

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

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

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

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

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

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

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

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

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

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

II.B.2 IT Operations Personnel Responsibilities

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

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

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

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

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

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

II.C Policies, Standards, and Procedures

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

- Policies[11] that provide the guiding principles by which an organization designs, builds, and operates its information and technology assets and set the foundation for meeting the entity's objectives. For example, an entity may have policies outlining the types of hardware or software it will or will not use (e.g., "We will not use any unapproved software.").

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

- Standards[12] that build on the policies and provide more granular information for AIO activities. For example, standards may explain the types of data that are allowed to reside in the cloud or the types of controls to be implemented to mitigate the risks of data residing in the cloud.
- Procedures[13] that describe the specific ways for personnel to perform AIO activities. For example, AIO-related procedures may cover topics including how to harden new systems or perform architecture reviews with the necessary steps for personnel to follow.

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

Action Summary

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

Examiners should review for the following:

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

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

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

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

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

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

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

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

II.E Communication

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

II.F Board and Senior Management Reporting

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

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

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

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

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

III COMMON AIO RISK MANAGEMENT TOPICS

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

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

III.A Data Governance and Data Management

Action Summary

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

Examiners should review for the following:

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

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

Data governance and data management are fundamental to maintaining the confidentiality, integrity, and availability of information. Data governance is a set of processes for formally managing data assets throughout the entity. It establishes authority, management, and decision-

making parameters related to the data that the entity produces or manages. Additionally, data governance involves the process for setting and enforcing the business and IT priorities for managing data.[15] The data management process involves the development and execution of policies, standards, and procedures to acquire, validate, store, protect, and process data. Effective data management ensures that the required data are accessible, reliable, and timely to meet user needs. When data are no longer used, management should have a process for the data's removal or destruction and validate the effectiveness of that process.

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

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

III.A.1 Data Identification and Classification

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

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

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

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

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

III.A.2 Database Management

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

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

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

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

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

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

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

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

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

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

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

- Restrict and monitor data extraction (e.g., limiting and monitoring data queries, user abilities, and the use of standardized business intelligence tools[17] to query databases to provide standardized reporting).
- Implement and adhere to patch management processes to maintain a current and secure database and underlying operating system (OS).
- Implement OS controls (e.g., configuration settings and access control).
- Monitor OS-level privileged account activities.
- Manage application-level access (e.g., access by and through applications).

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

III.A.3 Non-Production Environments

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

- **Privacy and misuse of data.** Entities sometimes copy production data into non-production environments, potentially allowing individuals to access information beyond what is needed for their job description.
- **Security tradeoffs.** To facilitate rapid changes or for development and testing of functionality, management may disable or omit security.
- **Data corruption.** Stale or incorrect data may inadvertently corrupt production data if non-production data are not appropriately segregated from production data.
- **Transition to production.** Failure to enable production levels of security may introduce vulnerabilities into the production environment.
- **Secondary use.** At times, non-production environments or data may be used for other than their intended purposes (e.g., training), which could expose sensitive data unnecessarily. Additionally, data used may not be appropriately secured.
- **Data breach.** If non-production environments are not properly secured, malicious actors may gain access and use that access as a conduit into production environments. Additionally,

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

malicious actors may be able to access sensitive data contained within non-production environments.

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

III.A.4 Data Analytics

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

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

- Document the types of data maintained, data owners and users, and purpose for reports.
- Determine usage needs by stakeholders (e.g., internal personnel and customers) and the ability of analytics reports to meet them.
- Determine whether there are opt-in considerations based on the information type in the analytics reports.
- Determine disclosure requirements (e.g., to regulatory agencies, internal stakeholders, and customers) in the event of a security incident.
- Implement access controls and activity monitoring over analytics tools and reports.
- Define processes to remove or destroy data when no longer used in the data analytics tools.

- Identify data that are subject to applicable laws and regulations (e.g., "Interagency Guidelines Establishing Information Security Standards" [Information Security Standards],[18] the Fair Credit Reporting Act, and the Equal Credit Opportunity Act) or other relevant industry standards (e.g., PCI DSS).
- Identify data analytics processes used by the entity to comply with applicable laws and regulations (e.g., Bank Secrecy Act/anti-money laundering, the Office of Foreign Assets Control, or the Sarbanes–Oxley Act [SOX]).

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

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

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

[19] *NIST Big Data Interoperability Framework: Volume 1, Definitions.*

[20] Ibid.

III.B IT Asset Management

Action Summary

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

Examiners should review for the following:

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

ITAM is the process to track, manage, and report on information and technology assets[21] throughout their entire life cycle. ITAM plays a significant role in the AIO functions, demonstrated by the following examples. In architecture, if management is aware of the entity's current inventories, it can determine the necessary design changes to meet strategic goals and objectives. For infrastructure, ITAM allows management to acquire hardware or software components that are interoperable with the entity's existing infrastructure. With respect to operations, the ITAM inventories help management know what systems need to be patched and the patch time frames, what hardware or software is nearing its EOL, where the entity's vulnerability management focus should be, or when any additional security measures are necessary.

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

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

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

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

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

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

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

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

III.B.1 Technology Asset Inventory

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

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

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

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

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

Management should maintain a hardware[23] inventory that identifies the entity's hardware assets. The hardware inventory should identify equipment owned and managed by third parties on the entity's behalf that may be located within the entity's environment (e.g., wire transfer routers, core processing hardware, and third-party security monitoring devices). The hardware inventory should include entity-owned and entity-managed virtual infrastructures (e.g., virtual servers on the entity's premises or virtual servers in a cloud environment). To the extent possible, hardware items should be assigned a unique identifier (e.g., labels or bar codes) to allow management to identify, account for, and monitor for changes to hardware assets.

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

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

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

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

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

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

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

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

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

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

III.B.2 IT Asset End-of-Life

With respect to technology, EOL is a time frame usually defined by a technology vendor to describe when an asset has reached the end of its useful life cycle or when the vendor will no longer support the asset or continue to sell or license it. All technology, including hardware, software, and assets in the cloud, has an asset life cycle. NIST states that an asset's typical life cycle[24] includes enrollment, operation, and EOL phases. Each IT asset should be captured in the entity's ITAM inventory, tracked throughout its operational life to monitor for changes (e.g., vendor announcements regarding support or changes in functionality, reliability, or processing speed) in the asset or the changing needs of the entity, and prepared for physical removal at the end of its useful life. Management should implement policies, standards, and procedures to identify assets and their EOL time frames, to track assets' EOLs, and to replace, or upgrade, the asset. Failure to maintain effective identification, tracking, and replacement processes could have operational or security implications (e.g., unavailable or unapplied security updates [patches] that make technology vulnerable to disruption).

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

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

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

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

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

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

III.B.3 Shadow IT

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

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

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

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

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

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

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

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

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

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

III.C IT and Business Environment Representations

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

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

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

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

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

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

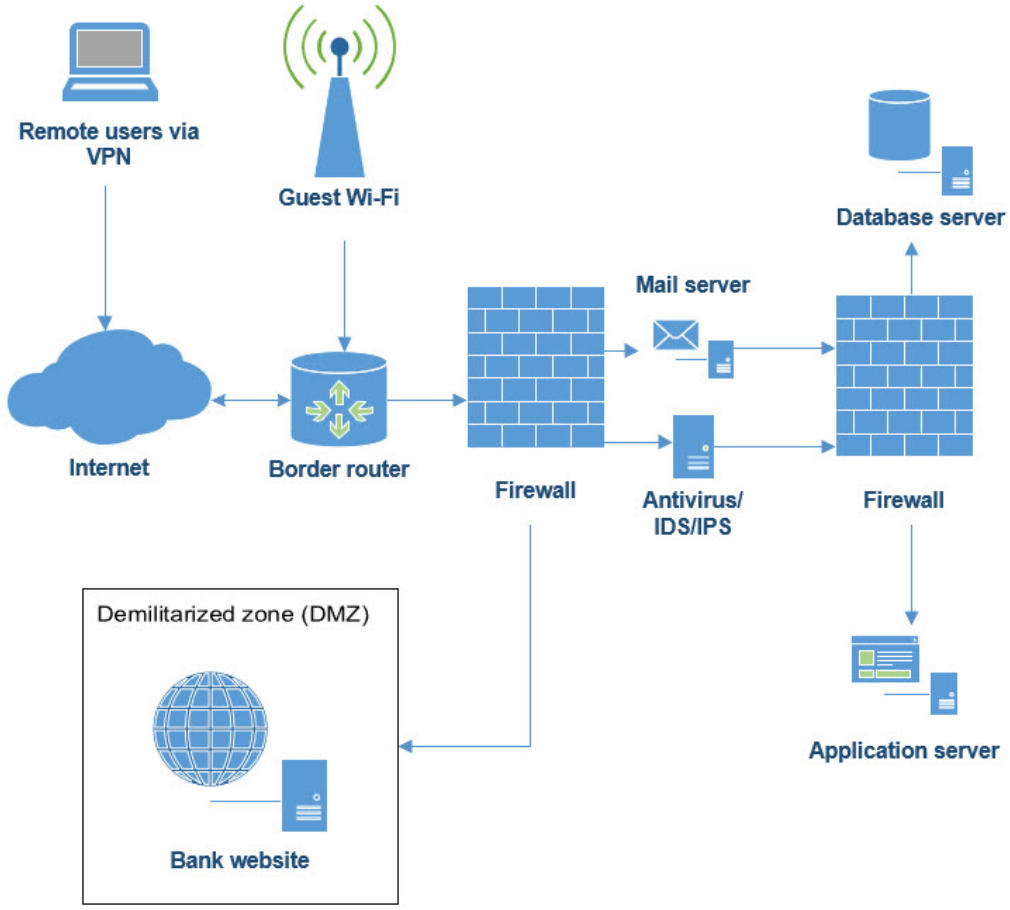
For larger or more complex entities, manual documentation and monitoring processes may not be effective at identifying all pertinent information. Therefore, automated tools may be used to document and assist in the management of the IT and business environment.

III.C.1 Network Diagrams

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

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

Figure 2. Example of a Network Diagram

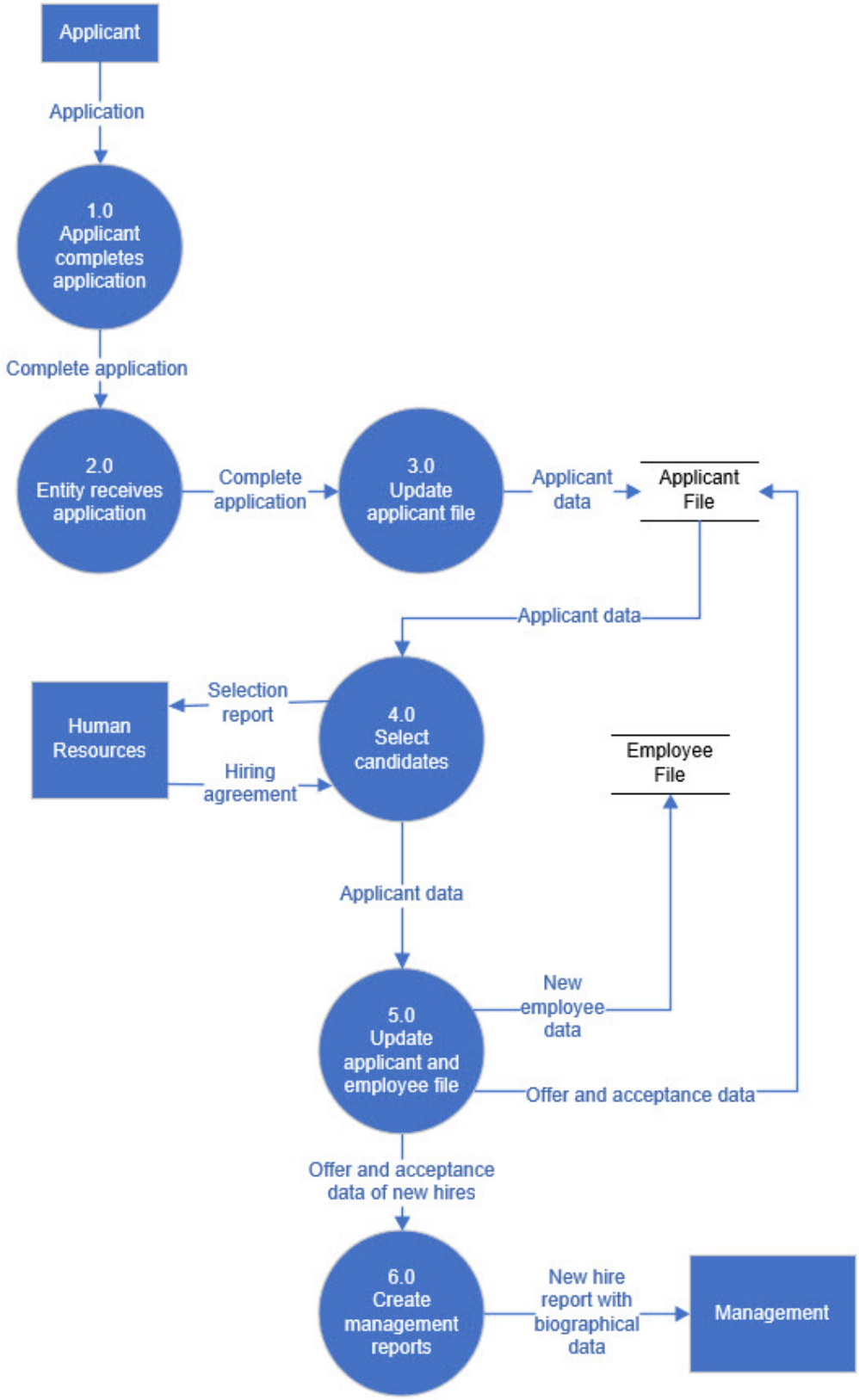


Note: Figure 2 is for illustrative purposes only and shows components a network diagram may contain.

III.C.2 Data Flow Diagrams

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

Figure 3. Example of a Data Flow Diagram



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

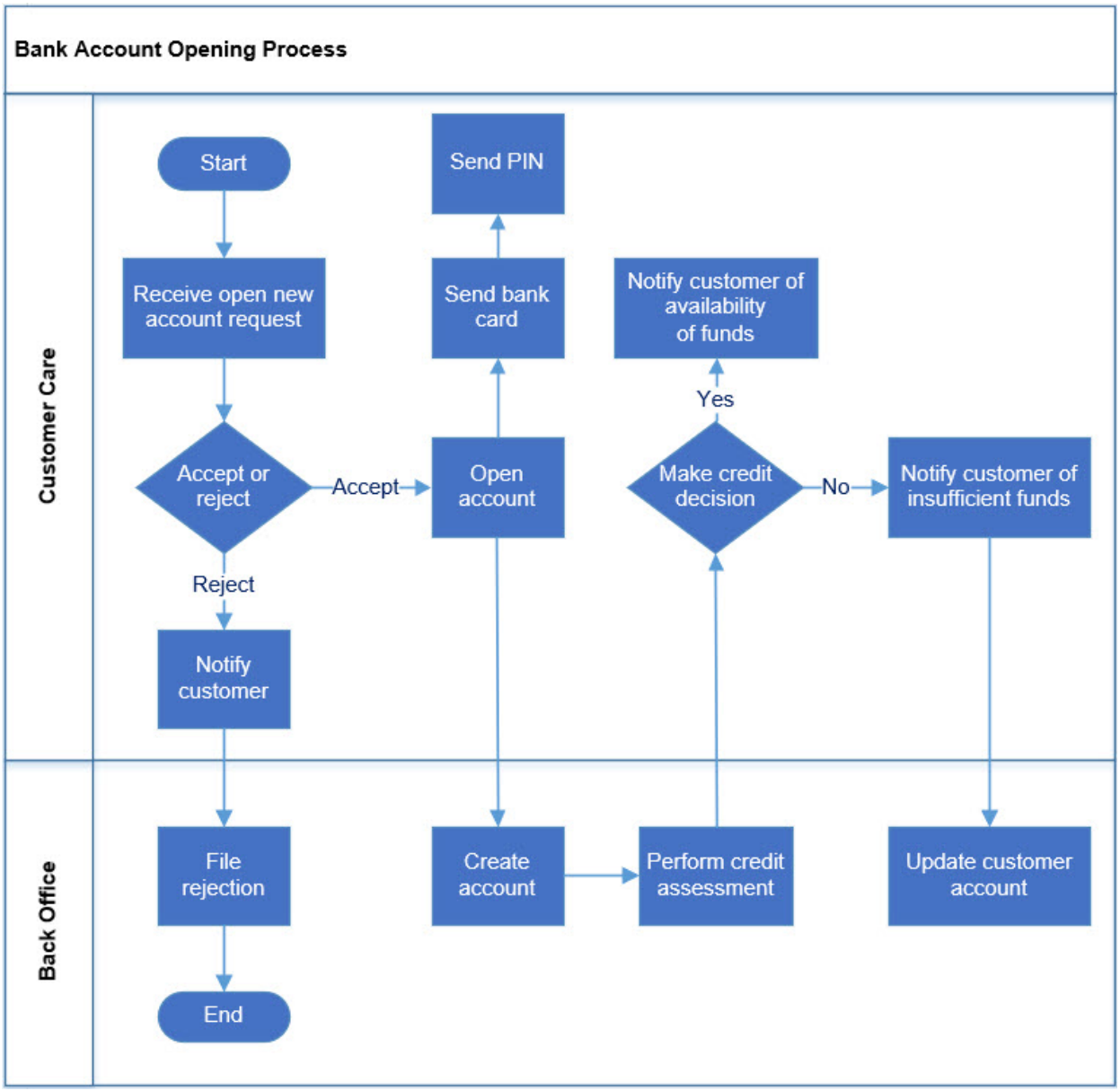
In smaller or less complex IT environments, data flow diagrams and network diagrams may be combined. In larger or more complex IT environments, the entity generally has multiple data flow diagrams and network diagrams broken out in a variety of ways (e.g., lines of business, geographic locations, network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

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

III.C.3 Business Process Diagrams and Narratives

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

Figure 4. Example of Process Flow Diagram



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

III.D Managing Change in AIO

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

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

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

III.D.1 Change Management

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

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

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

- **Request:** A documented request should outline the reasons for change (e.g., business justification) and include details of the change (e.g., system to be changed, impact analysis to identify risks and affected systems, change time frame, and back-out plan).
- **Review:** Management should review requests to determine viability and business practicality.[25] Requests may be prioritized during this stage or may be returned to the request originator for more information.
- **Approve:** There should be a documented hierarchy for approving change requests. Appropriate approval mechanisms[26] should be commensurate with the scope, cost, urgency, and overall risk to the entity and its IT environment.
- **Design and build:** Management should follow formal processes to preserve integrity throughout the development life cycle and ensure adequate controls (e.g., restrictions for moving code from staging to production).
- **Test:** Management should document that the change performs as intended, identify any flaws (e.g., integrity issues), and verify that the change integrates with other systems.
- **Implement:** Management should follow a formal process to deploy the change during off-peak hours or planned system outages.
- **Verify and close:** After deployment, management should perform a post-implementation review to verify that the change was implemented successfully and achieved performance objectives. After verification, management should follow processes to document the change's closure.

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

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

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

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

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

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

For more information, refer to the *IT Handbook's* "Development and Acquisition" booklet.

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

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

III.E Oversight of Third-Party Service Providers

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

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

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

III.F Resilience

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

Resilience of an entity's AIO functions extends beyond recovery capabilities. Resilience is achieved by taking proactive measures to maintain confidentiality, integrity, and availability and mitigating the risk of a disruptive event through system design (including backup systems), infrastructure selection, and IT deployment. The threats related to disruptive events may pose risks from multiple attack types (e.g., cyber and physical), duration (e.g., advanced persistent threat[30] [APT]), and delivery via deception (e.g., simultaneous distributed denial of service [DDOS] and business email compromise attacks). Management should design, implement, and operate its IT systems and processes to provide resilience for critical business activities. As part of its consideration for resilience of AIO functions, management should determine its reliance on people, processes, and technology, including third-party service providers, to assist in its assessment of risk.

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

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

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

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

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

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

III.G Remote Access

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

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

- Tunneling involves establishing a secure communications tunnel, via encryption, between a telework client device and remote access servers within an entity, typically a virtual private network (VPN) gateway. When determining whether to use tunneling[31] as a remote access method, management should consider the communications tunnel via encryption and the endpoints to which it is connected, as well as its capability to authenticate users and restrict access to IT systems.
- A portal[32] is a server that offers access to one or more applications through a single centralized interface. A remote user accesses a portal client (e.g., a web browser) on a client device to access the portal. When determining whether to use a portal, management should consider whether it adequately protects communications between the client devices and the portal, and also whether it can authenticate users and restrict access to the entity's internal

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

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

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

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

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

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

For more information on mitigating risks associated with entity-owned and personally owned devices, refer to the *IT Handbook's* "Information Security" booklet.

[33] Ibid.

[34] Ibid.

III.H Personally Owned Devices

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

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

III.I File Exchange

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

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

[35] Ibid.

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

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

Management should implement the following basic actions to improve the security of the entity's file exchange[38] activities:

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

[38] Ibid.

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

IV ARCHITECTURE

Action Summary

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

Examiners should review for the following:

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

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

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

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

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

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

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

IV.A Architecture Plan

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

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

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

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

IV.B Design Objectives

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

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

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

Management should include the following aspects in its architecture design:

- Performance and reliability (e.g., system processing at normal and peak loads, response time, load balancing, and uptime required by end users).
- Integrity (e.g., validation checks to promote accuracy).
- Availability and resilience (e.g., meeting recovery time objective [RTO] and recovery point objective [RPO] requirements, providing redundancy, and avoiding single points of failure).
- Scalability (e.g., the ability of systems and software to accommodate growth).
- Flexibility (e.g., the ability of systems and software to accommodate changes without requiring new hardware or code changes).
- Security and privacy throughout the entity's network (e.g., IAM controls and data loss prevention).
- Interoperability[40] and integration (e.g., among OSs, databases, networks, and user interfaces, and loose coupling).
- Ability to integrate and align with one or more third-party service providers.[41]
- Testing (e.g., integration and business continuity testing) internally and with third-party service providers as appropriate.
- Auditability (e.g., audit trails and logs).
- Advancements in technology.

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

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

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

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

IV.C IT Architecture Design

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

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

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

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

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

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

IV.D Enterprise Architecture

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

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

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

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

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

use aspects of industry frameworks[43] as appropriate for the entity's business needs. A framework may have different characteristics (e.g., informal, formal, prescriptive, principles-based, or a hybrid).

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

V INFRASTRUCTURE

Action Summary

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

Examiners should review for the following:

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

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

V.A Hardware

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

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

V.B Network and Telecommunications

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

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

[44] Refer to the NIST Glossary.

V.B.1 Network

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

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

Once management has an accurate inventory that contains network components and information, management should document the network's baseline configuration, including processes to review and approve changes. Management should regularly assess and document compliance with the entity's baseline configuration[45] to validate that settings are in place and commensurate with the board's risk appetite. Intentional or unintentional misconfigurations can lead to system issues or exploitation of vulnerable services and settings by malicious actors. To reduce exposure to potential vulnerabilities and failures arising from unused services, management should implement appropriate network configuration management and change control processes. Configuration rules allowing traffic to pass through the network should be documented with the necessary detail to justify the business need. Management should periodically review the configurations of network devices. Tools are available to verify that network devices are using approved configurations and notify management when unauthorized changes are detected.

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

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

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

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

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

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

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

V.B.2 Telecommunications

Telecommunications infrastructure should be appropriate for current and anticipated internal traffic needs and have sufficient connectivity to facilitate external communications. Telecommunications infrastructure includes both voice and data transmissions that are broken up into multiple packets to facilitate transmission of those packets over shared paths. Telecommunications packets typically incorporate message content and completion validation messages. Between telecommunications endpoints, packets can be lost, encounter interference, or arrive out of order. Capacity, latency, and connectivity issues can affect the arrival of packets or completion of messages. Therefore, management should monitor telecommunications traffic. In addition, administrators should periodically review network devices to identify any that are operating in promiscuous mode or acting as packet "sniffers" for network traffic.

Management should physically secure telecommunications equipment[46] and restrict and monitor access (e.g., through access devices, logs, and cameras). Changes to telecommunications equipment and configurations should follow enterprise change control standards, including approval, testing, and migration to production. Identification, authorization, and authentication to access (including remote access) telecommunications systems should follow entity policies, standards, and procedures, including approval and documentation of exceptions. Documented wiring strategies (e.g., schematics and color coding) and organized cables facilitate easy troubleshooting, repair, and upgrade.

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

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

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

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

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

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

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

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

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

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

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

Data communications is the transfer of data over networks[49] using a combination of telecommunications services and network devices. Networks connect devices within a single geographic site or can connect multiple geographically dispersed entity and third-party service provider sites. They connect servers, end user devices (e.g., workstations, laptops, and mobile devices), wireless routers, and network security devices, such as firewalls and IDS/IPS.

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

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

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

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

V.C Software

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

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

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

V.C.1 Internally and Externally Developed Software

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

- **Internally developed software:** An entity's internal development team can develop software or management can engage third-party development teams to develop software on the entity's behalf. Management is responsible for maintaining the software; therefore, entity personnel should have the resources and expertise to stay abreast of vulnerabilities and develop software updates and patches to promote the security and resilience to meet business needs. Refer to the *IT Handbook's* "Development and Acquisition" booklet for more information on internally developed software.

- **Externally developed software:** Externally developed software is available in multiple forms. These include the following:
  - **Commercial off-the-shelf (COTS) software:** COTS is a software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public. COTS is also referred to as off-the-shelf. COTS software is built with default functionality and configurations to accommodate a variety of uses. It offers

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

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

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

V.C.2 Software Types

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

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

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

- **OS software:** An OS is a program that runs on a computer and provides a software platform on which other programs (e.g., application software and utility software[50]) can run. An OS manages computer hardware resources and provides common services (e.g., access and security controls, file system maintenance, and communications management). There are numerous server, desktop, and laptop OSs, as well as mobile (e.g., tablet and smartphone) OSs. Regardless of the type used, if the OS is not maintained, other software may not function adequately or at all, which affects the entity's ability to conduct business. Therefore, management should oversee and maintain the OS, including testing and installing patches when appropriate. Because having access to the OS, including utility software, provides access to applications running on the OS platform, management should restrict and monitor administrator access to the OS and should limit the use of utility software.[51]

- **Core processing software:** Core processing software enables the processing of key banking functions (i.e., taking deposits and making loans) and other functions (e.g., statement rendering, payment processing, calculating interest, and customer relationship management [CRM]), and interfaces to other software (e.g., general ledger systems and reporting tools). This software should be appropriately restricted based on job responsibility and its use monitored because of the sensitive nature of the entity's and the customer's information and the impact on other systems (e.g., general ledger and customer and management reporting). Management should select core processing software with adequate capacity to support strategic goals and objectives (e.g., customer base growth or geographic diversity). The software should support usage spikes (e.g., daily, monthly, and quarterly), expected peak usage times (e.g., holidays), and future growth.

- **Productivity software:** Productivity software can refer to any software that helps to produce and manage data and improve the user's productivity. Management should consider using productivity software in its infrastructure environment to enable personnel to perform their job functions. Examples can include word processing, spreadsheet, database, video conferencing, and presentation software. "The line between web applications and locally installed applications has blurred over time to the point where a number of web application providers offer web versions of common desktop productivity tools, including word processors, spreadsheets, and calendars. ... As such, these web applications may need to support the ability to store and process mobile code associated with office documents (or any user-generated files), opening up web applications to many [risks associated with web applications]."[52] "Common management and operational controls used to safeguard systems against other security threats also apply to active content."[53] These controls include IAM, configuration management, and monitoring of logs. There is a risk that data may fail to synchronize correctly, which could negatively affect data integrity. An attacking entity may intercept messages in transit and modify their contents, substitute other contents, or simply replay the transmission dialogue later in an attempt to disrupt the synchronization or integrity

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

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

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

[53] Ibid.

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

- **Enterprise software:** Enterprise software helps management make better and more informed decisions through enterprise data aggregation. Enterprise software examples include communication, collaboration (e.g., SharePoint), CRM, digital and content creation, enterprise resource planning, project and portfolio management, and supply chain management. Enterprise software can encompass a vast array of subjects, methods, models, and reporting. Management should consider how enterprise software integrates in the entity's infrastructure environment. Because of the sensitive or critical nature of the information available within this type of software, management should limit access and editing capabilities and monitor user activity.

- **Security software:** Security software is designed with the goal of preventing an attacker from reaching the intended target or limiting the damage of an attack. The software can be designed to track the damage incurred from an attack. Malicious code continuously evolves; therefore, management should use security software that is current, deployed effectively, and designed to keep up with the evolution of malicious code. The software can be controlled by either a third-party service provider or the entity. Because of the sensitive security information contained within the software or technology assets being monitored by the software, administrative access to this type of software should be restricted. Security software types may include the following:
  - IAM.
  - Antivirus.
  - Encryption management.
  - Application firewall.
  - IDS/IPS.
  - Log management.
  - Security information and event management.
  - Patch and vulnerability management.

  For more information, refer to the *IT Handbook's* "Information Security" booklet.

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

[54] Ibid.

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

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

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

Unlike proprietary software, open source software[56] can be accessed, used, modified, and shared by anyone.[57] Management may leverage a variety of open source software. Open source software may provide several advantages, including cost and availability. Management should identify unique security issues (e.g., public availability of the code, ability for users to alter the code, licensing issues, difficulty in tracking patches, and publicized exploits) with the use of open source software. Management should implement security controls and procedures to mitigate risks, including the following:

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

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

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

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

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

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

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

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

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

There are several software-based access control security tools[58] available for managing security of critical mainframe system resources. These tools are generally add-on software products that provide security for a mainframe and protect system resources by granting access only to authorized users. Tools provide the ability to do the following:

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

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

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

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

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

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

- Secure IPs (e.g., HTTPS) to encrypt data during transmission from the web browser to a web server.
- Password hashing to validate the integrity of the message.
- Restriction of secret information (e.g., API keys, session tokens, and user IDs) from website addresses to prevent unnecessary information transmission.
- Industry standard authorization protocols[60] to securely authenticate users.
- Strong validation to ensure a user knows what to input (i.e., client-side validation) and on the web server to ensure data are accurate and in the correct format (i.e., server-side validation) to help mitigate malicious attacks.
- Time stamping of API requests to provide traceability of the request.
- Rate limiting of API calls to protect against malicious attacks (e.g., DDOS).
- API traffic monitoring to determine the locations from where requests originate allowing the ability to take action (e.g., monitor activity or block IP addresses).
- API gateways configured appropriately throughout the entity's IT environment to facilitate principles of least privilege to information and services.

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

- **Internal or private APIs:** Internal or private APIs are restricted from external access. They are used by internal teams or business units to access internal data, services, and tools. Advantages of using internal APIs include the following:
  - Standardization of connections to internal services (e.g., eliminating hard-coded connections).
  - Decreased code development time through use of existing and already tested APIs.
  - Control over coding practices (e.g., secure coding).
  - Access restrictions over the API.
  - Auditability of API access and requests.

  Management should implement an appropriate level of security before internal APIs are made available for use by other entity business units.

- **Public or open APIs:** Public or open APIs (also referred to as third-party APIs) are accessible by external parties (e.g., developers). External parties register for access with the entity and, in return, receive an API key.[61] In some cases, however, no registration is required. Management should implement adequate security and restrictions to protect sensitive customer and entity data. Management should perform appropriate testing to verify the adequacy of security controls before and after going public.

- **APIs between customers and unaffiliated third parties:** In this situation, the relationship is between the customer and a third party (e.g., a fintech firm that is separate from the financial institution where the customer has the account). This type of API has a specific purpose and may have a fee associated with its usage. As part of its customer awareness

[60] For an example refer to Internet Engineering Task Force, RFC 7591, *OAuth 2.0 Dynamic Client Registration Protocol*, DOI 10.17487/RFC7591, July 2015.

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

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

V.C.3 Software Hosting

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

- **Internally hosted software:** Internally hosted (also referred to as on-premise) software refers to software that the entity hosts and manages. Usually, the internal IT department is responsible for software administration. When hosting software internally, there is a risk that the entity personnel does not have the appropriate skills and expertise to effectively manage the hosting environment. Management should identify personnel (e.g., internal or third party) with relevant skills and expertise and allocate resources to provide necessary training to maintain their knowledge. If the entity develops software, management should use a system development life cycle that incorporates security to limit the number and severity of vulnerabilities in the software.

- **Externally hosted software:** Externally hosted software (also known as hosted services) is hosted at an entity's third-party service provider. Access generally occurs through an internet connection. Hosted services may include core processing, web hosting (e.g., online banking and website), off-site backup, and virtual desktop infrastructure. Possible risks with externally hosted software include a lack of control over the infrastructure and any changes made to it by the third-party service provider. Management should have contract provisions addressing the notification of infrastructure changes and the third party's use of any subcontractors (sometimes referred to as "fourth parties"). For more information, refer to the *IT Handbook's* "Outsourcing Technology Services" booklet.

- **Hybrid hosted software arrangement:** A hybrid hosted software arrangement refers to an agreement involving software that resides at the entity (on premise) and on the third-party service provider's servers (e.g., productivity software as a service). Examples of this arrangement include the following:
  - Internally deployed software at the entity where all data are maintained on the third-party service provider's servers.

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

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

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

V.D Environmental Controls

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

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

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

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

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

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

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

V.D.1 Heating, Ventilation, and Air Conditioning

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

V.D.2 Smoke and Fire

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

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

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

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

[66] These systems are also known as clean agent systems.

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

V.D.3 Water

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

V.D.4 Power

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

- Independent electrical feeds drawing from separate power grids. When multiple feeds or backup power generators are used, automatic fail-over to a live power source should be considered. When power is available only through one grid or one provider, management should evaluate and mitigate the risk in other ways (e.g., using generator(s) or batteries).
- Methods to monitor, condition, or stabilize the electricity source voltage to minimize the effects of power fluctuations with specialized devices (e.g., surge protectors or capacitors).
- Appropriate power configurations based on the entity's power needs.
- Alternative, or backup, power sources for IT facilities independent of local power grids. Those sources could include a combination of uninterruptible power supply (also referred to as UPS) and generators[69] powered by diesel or natural gas, and management should consider

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

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

[69] The generator should run on something other than electricity.

the risks of these options. These may be used to mitigate disruptions, allow an orderly power down of systems, or transition systems to a longer-term alternate power source.
- Processes to power down IT systems in an orderly manner to maintain critical information for later recovery, in cases where power cannot be maintained (e.g., during emergencies).
- Automated emergency lighting that activates to illuminate the entity's critical infrastructure, evacuation routes, and emergency exits, in the event of a power outage or disruption.

V.E Physical Access Controls

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

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

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

VI OPERATIONS

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

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

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

VI.A Operational Controls

Action Summary

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

Examiners should review for the following:

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

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

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

VI.A.1 Operating Centers

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

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

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

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

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

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

VI.A.2 Authorization Boundary

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

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

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

VI.A.3 Identity and Access Management

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

VI.A.4 Personnel Controls

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

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

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

VI.B IT Operational Processes

Action Summary

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

Examiners should review for the following:

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

VI.B.1 Maintenance

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

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

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

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

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

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

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

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

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

VI.B.2 Configuration Management

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

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

VI.B.3 Vulnerability and Patch Management

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

VI.B.3(a) *Vulnerability Management*

To have systems that are operationally functional and secure and perform as intended, management should implement a vulnerability management program that identifies systems and software vulnerabilities, prioritizes the vulnerabilities and the affected systems in order of risk, and performs timely remediation, according to the risk associated with the vulnerability. The program should include an entity's systems and software[73] operating in the cloud for which the entity is responsible and those managed by the entity on its premises. Management should monitor industry third parties (e.g., United States Computer Emergency Readiness Team [US-CERT[74]], NIST, and Financial Services Information Sharing and Analysis Center [FS-ISAC[75]]) that report vulnerability exposures and address any relevant exposures within the entity's systems and software.

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

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

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

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

[75] Refer to FS-ISAC.

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

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

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

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

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

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

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

VI.B.4 Backup and Replication Processes

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

Management should maintain the following:

- Policies, standards, and procedures that document the entity's backup methodologies, delineate responsibilities of personnel, and promote uniform performance throughout the entity.
- Inventories of backup media, storage location, and access controls for the media or physical location.
- Documented periodic physical reviews to confirm that all relevant backup material is available.
- Procedures to verify adherence to backup schedules.
- Processes to regularly test backup copies for readability.
- Capability to restore operations to a previous trusted state.
- Backups of configurations and data off-site and on a separate system or media.
- VM versioning, replication, and life cycle policies for backup processes.
- Data encryption and access controls to protect backup or replicated data from unauthorized access, destruction, or corruption.[78]
- Proper sanitization[79] and disposal of data when they are no longer needed to prevent the disclosure of information to unauthorized users.

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

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

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

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

VI.B.5 Scheduling

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

VI.B.6 Capacity Management

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

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

- Platform processing speed.
- Primary working memory[80] for each platform's central processing unit (CPU).
- Additional data storage capacity.
- Voice and data communication bandwidth.

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

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

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

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

VI.B.7 Log Management

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

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

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

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

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

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

VI.B.8 Disposal of Data and Media

Management should implement policies, standards, and procedures to address media[81] and equipment disposal or transfer. Disposal processes are a shared responsibility among several of an entity's functions, including operations, information security, and third-party service provider management. Controls involved in the disposal process should be risk-based relative to the sensitivity of the information as defined by the entity's data classification[82] policy and the type of media used. The procedures should define methods for disposal based on the type of data to be removed. For example, management may choose to physically destroy media that contain customer sensitive information to prevent data recovery and misuse. Management should consider using techniques to remove data even when transferring the media between internal departments, as not all internal departments require access to sensitive or confidential information. For example, often media is reused after an employee leaves the entity; if someone in a customer-facing function with access to sensitive customer information leaves the entity, the information should be removed from the laptop before issuing it to other employees. Management should have appropriate procedures for the disposal of equipment (e.g., printers), which may contain residual data. Periodically, management should perform a review to ensure the timely disposal of decommissioned equipment.

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

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

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

VI.C Service and Support Processes

Action Summary

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

Examiners should review for the following:

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

VI.C.1 Service Management

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

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

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

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

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

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

VI.C.2 Operational Support

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

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

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

VI.C.3 IT Support

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

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

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

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

Management should maintain well-trained and knowledgeable IT support personnel to effectively support clients and users. If IT support software is used, IT support personnel should have appropriate training to perform their duties. IT support should follow procedures to authenticate users to prevent unauthorized access to information or credentials. The entity may choose to use different levels of authentication depending on the method of contact (e.g., telephone, website, or chat), the problem reported, the type of action requested, or the platform, system, or data involved. Management should consider layered security and supplemental authentication techniques,[83] including out-of-band methods for changes to account maintenance activities (e.g., address or password changes) and for those involving high-risk transactions[84] to limit attempted fraud through social engineering or identify theft. Refer to the *IT Handbook's* "Information Security" booklet for more information.

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

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

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

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

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

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

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

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

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

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

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

VI.D Ongoing Monitoring and Evaluation Processes

Action Summary

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

Examiners should review for the following:

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

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

VI.D.1 Monitoring and Reporting

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

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

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

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

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

VI.D.2 IT and Operations Key Performance Indicators

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

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

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

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

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

VI.D.3 Control Self-Assessments

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

VI.D.4 Continuous Improvement

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

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

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

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

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

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

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

VII EVOLVING TECHNOLOGIES

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

VII.A Cloud Computing

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

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

As defined by NIST, "cloud computing has five essential characteristics, three service models, and four deployment models."[87]

VII.A.1 Essential Characteristics

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

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

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

[87] Ibid.

[88] Ibid.

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

VII.A.2 Cloud Service Models

There are generally three key cloud service models[89] used in cloud computing implementations.[90] The optimal architecture for a given application or service is determined by consideration of the entity's requirements, including data classification, data residency, service or application availability, and interfaces with external services and data stores.

NIST describes the service models[91] as follows:

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

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

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

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

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

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

VII.A.3 Cloud Deployment Models

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

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

Entities may use more than one cloud service provider for different operations or to augment continuity and resilience for operations in the cloud. The use of multiple cloud service providers may reduce single-provider reliance. Entities may rely on cloud bursting[93] capabilities for situations requiring increased capacity or for business continuity purposes. Entities may use a cloud broker to act as an informed intermediary between management and the cloud service provider. The use of a cloud broker may also supplement the capabilities of entity management and staff.

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

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

VII.A.4 Shared Responsibilities

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

Depending on the service and deployment model used, management should understand the shared responsibilities associated with cloud computing. As presented by NIST, "compared to traditional IT systems, where one organization has control over the whole stack of computing resources[94] and the entire life cycle of the systems, cloud service providers and cloud consumers collaboratively design, build, deploy, and operate cloud-based systems. The split of control means both parties now share the responsibilities in providing adequate protections to the cloud-based systems." It is important to understand what controls are implemented by the cloud service provider for the cloud service provider's own operations and what security controls are implemented and operated to ensure the security of the entity's content and applications.

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

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

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

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

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

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

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

VII.A.5 Risk Considerations for Cloud Computing

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

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

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

Third-party assurance reviews (e.g., SOC reviews, penetration tests, and vulnerability assessments) can provide an understanding of the cloud service provider's control environment and its ability to meet an entity's control expectations (e.g., compliance with applicable laws and regulations). Refer to the FFIEC's joint statement[96] for more information.

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

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

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

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

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

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

[96] FFIEC, *Security in a Cloud Computing Environment*.

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

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

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

VII.B Zero Trust Architecture

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

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

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

---

[98] Ibid.

[99] NIST SP 800-207, *Zero Trust Architecture.*

[100] Ibid.

[101] Ibid.

[102] Ibid.

[103] Ibid.

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

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

VII.C Microservices

Microservices are a set of containers that work together to compose an application. Essentially, each microservice is an independent building block used for building an application, including the communications and authentication. Each microservice is a mini application loosely coupled[105] to serve a singular function (e.g., database access or messaging) that can be integrated to collectively build an application. During the communication events of any pair of interactions (e.g., client-to-microservice, microservice-to-microservice, or microservice-to-egress service), each party has distinct identities and performs mutual authentication.

Each microservice typically implements one (rarely more) distinct business process or functionality (e.g., storing customer details or displaying a product catalog). NIST 800-204A[106] states that a microservice has two broad functions:

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

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

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

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

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

The implementation of microservices infrastructure differs from legacy distributed systems as there are multiple services configured to operate at designated locations (IP address and port number). When using microservices-based applications, the following are key elements[108] to consider in the entity's infrastructure:

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

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

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

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

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

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

[111] Ibid.

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

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

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

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

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

VII.D Artificial Intelligence and Machine Learning

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

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

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

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

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

[115] Ibid.

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

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

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

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

VII.E Internet of Things

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

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

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

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

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

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

APPENDIX A: EXAMINATION PROCEDURES

Examination Objectives

These examination procedures (also known as the work program) are intended to assist examiners in determining the quality and effectiveness of the entity's AIO functions and their related activities. Examiners are not limited[118] by the examination procedures presented here and may choose to use only certain components of the work program based on the size, complexity, and nature of the entity's business. Depending on the examination scope and objectives, examiners may sample processes related to a particular line of business or review the process at an enterprise level.

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

1. Review past reports for outstanding issues or previous problems. Consider the following:

    a. Regulatory reports of examination.
    b. Internal and external audit reports.
    c. Reports by independent risk management.
    d. Independent assurance and security reports (e.g., penetration tests and vulnerability assessments) and internal reports that self-identify concerns related to AIO issues.
    e. Regulatory, audit, and SOC reports on the entity's third-party service providers.
    f. The entity's overall risk assessment and profile.

2. Review management's response to issues identified during or subsequent to the last examination. Consider the following:

    a. Adequacy and timing of corrective action.
    b. Resolution of root causes rather than symptoms.
    c. Status of uncorrected issues.
    d. Retesting to validate corrective action.

3. Interview management and review responses to pre-examination information requests to identify changes to the entity's technology related to new products and services that could affect the areas of review within AIO. Consider the following to identify changes:

    a. Any significant changes in business strategy or activities that could affect the AIO environment (e.g., new lines of business or a decision to move from in-house to a cloud service provider).
    b. Products or services delivered to either internal or external users.
    c. Network diagrams, including configuration or component changes and the entity's internal and external connections.
    d. Hardware, software, and telecommunications inventories.

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

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

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

1. Determine whether management implemented a process to continuously manage technology to support operational needs and mitigate AIO-related risks. Determine whether the entity's risk management processes include the following governance mechanisms:

   a. Delineation of board and senior management responsibilities.
   b. Strategic planning.
   c. ERM.
   d. Delineation of other roles and responsibilities.
   e. Policies, standards, and procedures.
   f. Internal audit, independent reviews, and certifications.
   g. Communications.
   h. Board and senior management reporting.

2. Determine whether oversight includes the following:

   a. Board and senior management consideration of the entity's business objectives, including functions performed by affiliates and third-party service providers.
   b. Management identification and evaluation of AIO-related risks, definition of short- and long-term objectives, and creation of policies and procedures to mitigate those risks.
   c. Management consideration of security and resilience in the design of new products and services.

3. Determine whether board oversight includes the following:

   a. Aligning AIO principles and practices with the board's strategic plans and risk appetite.
   b. Budgeting appropriate resources to support AIO activities.
   c. Ensuring board members have appropriate knowledge of risks to provide a credible challenge to management.
   d. Enabling appropriate management training on AIO to carry out its responsibilities and manage risk.
   e. Reviewing AIO operating results and performance (e.g., audit reporting, testing results, and management and assessment reports).

4. Determine whether management oversight includes the following:

    a. Validating through audits and other independent assessments that the following are comprehensive, meet enterprise-wide business and strategic plan objectives, and can assist in the identification of AIO-related risk.
        - Architectural designs and integration across the entity.
        - Infrastructure testing.
        - Operational testing.
    b. Addressing risks self-identified by management, from AIO-related audits, and from other independent assessments.
    c. Assessing and updating management's strategies and plans for AIO functions.
    d. Promoting alignment and integration between functions of AIO.

5. Determine whether the board and senior management evaluate whether the IT strategic plan aligns with the enterprise-wide business and strategic plan, as well as established priorities and whether the planning addresses the following:

    a. Participation of senior management by supporting AIO activities, confirming that those activities are in the IT strategic plan, reviewing the strategic planning process, and incorporating changes.
    b. Responsibilities within the AIO functions through defining those responsibilities and determining the effectiveness of the IT strategic planning process.
    c. Evaluation of architecture, including the entity's current architecture and whether it meets enterprise-wide business and strategic plan objectives.
    d. Impact of IT infrastructure by understanding the relationship between IT infrastructure and the entity's needs.
    e. Post-implementation evaluation of the performance and results of IT projects and initiatives to determine whether each project achieved the anticipated goals.

6. As part of the evaluation of question 5, determine whether management does the following:

    a. Evaluates whether past and current IT performance demonstrates an ability to support IT strategic plans.
    b. Takes steps to ensure and validate that IT services are delivered on time, within budget, and to business specifications.
    c. Balances resource investments.

7. If an entity provides IT services internally or externally as a third-party service provider, determine whether management considers the following in the IT strategic planning process:

    a. IT services strategy management that helps management to meet the needs of the entity while also providing for availability, capacity, continuity, and security.
    b. Financial management for IT services to allocate the cost of providing services.
    c. SPM that enables the entity to balance investment in AIO with the ability to meet business outcomes.

d. Demand management, which balances customer demand for services with the capacity to meet that demand.

8. *This examination procedure may be coordinated with related examination procedures in the "Management" booklet.* Determine whether the entity's ERM structure incorporates the functions of AIO. Evaluate whether, as part of ERM, there is the following:

   a. Consistent and current review of the entity's products, processes, applications, infrastructure, interconnectivity, and other related risks to business operations.
   b. An effective risk management process for initiating and overseeing all AIO-related activities, including those that are outsourced, that includes:
      - Initial assessment of the AIO-related risk.
      - Architecture designed to meet the entity's goals or objectives.
      - Infrastructure that supports the entity's strategic objectives.
      - Identification of infrastructure assets (e.g., hardware and software) and associated interconnectivity critical to business and IT operations.
      - Ongoing monitoring that identifies and evaluates changes in risk and periodic updates to the risk profile assessment.
      - Roles, responsibilities, procedures, and reporting mechanisms for risk management in AIO activities.
      - Risk tolerances and risk and performance metrics for AIO activities.

9. Determine whether management assigned responsibilities for the AIO functions based on the complexity of the architecture needs and assess the effectiveness of the entity's separation of duties across the functions, particularly in situations where architecture responsibilities are combined with other functions. Evaluate the effectiveness of the assignment of the following responsibilities:

   a. Architecture-related responsibilities:
      - Review of the centralization processes for the IT functions and understanding of interrelationships between the entity's IT and business functions.
      - Development and maintenance of the enterprise model, including a common understanding, vocabulary, and blueprint for all stakeholders.
      - Responsibility for designing the IT architecture and accommodating IT changes.
      - Communication of challenges to the board and senior management.
      - Maintenance of representations (e.g., blueprints, network diagrams, and topologies) of the IT environment, review of existing infrastructure and operations to determine IT systems capabilities and needs.
      - Working with other members of management to evaluate architectural changes.
      - Maintenance and use of IT architecture knowledge.
      - Development of IT architecture policy and terminology.
      - Oversight of IT architecture product development, use, and refinement.
      - Maintenance and ownership of the IT architecture repository.
   b. Data-related responsibilities:
      - Governance and use of information or data, protection of that data, and derivation of maximum value from it.

- Development of data-related policies, management of the data life cycle and the entity's data assets, oversight of compliance with applicable laws and regulations, and conformance with industry practices.
- Provision of input to the chief architect in the design of IT systems to promote alignment with enterprise-wide business and strategic plan objectives.
- Oversight of data management and data analysis and management of data-related projects.
- Analysis of whether the entity's products and services meet enterprise-wide business and strategic plan objectives from a data perspective.
- Use of data and reporting tools, maintenance of data quality, and promotion of data integrity.
- Ownership of the entity's strategic use of data and communication of information and data analytics.
- Definition of a data strategy, evaluation of data and its usage (including the consideration of data planning and the analytics platform), and development of metrics for monitoring data activities.

c. Operations-related responsibilities:
   - Oversight of the IT environment.
   - Management of the capacity, performance, and availability of the components used in an entity's infrastructure.
   - Support for line-of-business and functional operations.
   - Day-to-day operation and maintenance of infrastructure components.
   - Management of network infrastructure (e.g., network and connectivity, remote access, and telecommunications management) and server and device management (e.g., servers, storage, and devices).
   - Management of the IT environment (e.g., facilities, help desk, IAM, backup and replication, configuration management, resilience, and cyber and information security).
   - IT project management.
   - Database administration, systems analysis, client support, systems administration, and network administration.

10. Determine whether management documents, implements, and maintains policies, standards, and procedures related to AIO that address the following:

    a. Scope.
    b. Responsibilities.
    c. Accountability.
    d. Authority.
    e. Guidance to develop and maintain effective processes related to AIO.

11. Determine whether the board and senior management engage qualified audit or use other independent review functions to assess the AIO design, implementation, and operational effectiveness, including the adequacy of policies and procedures and the effectiveness of controls. Evaluate the appropriateness of the following:

a. Review of the entity's AIO functions and activities and management's ability to oversee and control AIO-related risks.
b. Qualifications, training, and experience of auditor (or independent reviewer) in reviewing the functions and activities of AIO.
c. Independence of auditor from the AIO functions and activities being reviewed.
d. Reports to the board and senior management containing the results of audits or other independent reviews and an assessment of management's ability to oversee the entity's AIO functions and activities. Validate whether the review scope and frequency are appropriate for the complexity of the entity's AIO functions.
e. Whether auditors or reviewers:
   - Evaluate that management's AIO decisions align with the entity's business strategy, security, and resilience needs.
   - Leverage SOC and other external audit reports from third-party service providers.
   - Identify and report AIO issues to senior management and the board.

12. Determine whether management effectively communicates relevant AIO information to the entity's staff, applicable customers, and third parties.

13. Determine the effectiveness and comprehensiveness of board and senior management reporting related to AIO. Evaluate whether the following activities are performed:

a. Management reports to the board periodically on the status of AIO initiatives, progress, issues, and metrics.
b. The board regularly monitors strategy, security, and resilience activities.
c. Board minutes reflect significant AIO-related discussions, credible challenge, and approvals.
d. Management measures performance and risks against defined baseline metrics.

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

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

1. Determine whether management governs and manages data based on the entity-assigned data classification.

2. Evaluate whether management has an effective process for data removal or destruction when data are no longer used.

3. Evaluate whether business line management is consulted to assist in data classification, recovery standards development, and appropriate control validation.

4. Determine whether management has data governance and data management processes that include defining responsibility and processes for governing data, including the identification,

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

5. Determine whether management identifies and classifies the entity's data effectively. Determine whether management does the following:

   a. Identifies and understands the nature of the entity's data, including:
      - Sensitivity, criticality, and importance of the data.
      - Frequency, recurrence, and use of the data.
      - Format in which data are maintained.
   b. Uses the results of the data classification process to implement controls to safeguard data, including sensitive data.
   c. Understands where data reside and maintains the effectiveness of controls over that data.
   d. Regularly updates the information and technology asset inventories for new assets, both internal assets and those residing at third-party service provider locations.

6. Determine whether management has effective database management, including the following:

   a. Securely designs, builds, and operates databases.
   b. Implements a process to secure and oversee databases.
   c. Ascertains the effectiveness of database controls and updates the information asset and technology inventories.
   d. Ensures databases are appropriately located and structured, have sufficient capacity, and are resilient.
   e. Regularly monitors for new or changed databases and reports on misconfigured or out-of-compliance databases.
   f. Understands how databases interconnect throughout the entity.
   g. Focuses on identifying, managing, and securing the data; identifying business uses; and providing appropriate access regardless of how the data are stored.
   h. Has appropriate staff (e.g., DBAs) that
      - Is responsible for database configuration, access controls, and maintenance, as well as training.
      - Monitors databases and maintains normal operations.
      - Works with information security staff.
      - Monitors for anomalous database activities.
      - Is familiar with procedures to protect sensitive information, restores normal operations, and notifies the information security officer when necessary.
   i. Limits and independently monitors accounts belonging to DBAs.

7. Verify that management implemented effective database security controls, such as the following:

   a. Changes passwords for default user accounts and, subsequently, disables or deletes those accounts where possible.
   b. Tracks and monitors activity for default accounts that cannot be disabled or deleted.

c. Restricts account access and limits privileges and permissions.
d. Implements password management tools or activities.
e. Employs an appropriate level of encryption according to the entity's data classification policy.
f. Configures and reviews audit logs.
g. Regularly monitors database activity logs.
h. Independently monitors DBA and privileged account activities.
i. Classifies data maintained within the database.
j. Restricts and monitors data extraction.
k. Implements and adheres to patch management processes.
l. Implements OS controls.
m. Monitors OS-level privileged account activities.
n. Manages application-level access.

8. Determine whether management considers design, placement, and effective security controls for non-production environments (e.g., development, test, and quality assurance). Consider the following:

   a. Independence of non-production environments from production environments to maintain data integrity and resilience.
   b. Use of simulated synthetic data in non-production environments, when possible.
   c. Controls to prevent testing in production environments to maintain confidentiality, integrity, and availability of data.
   d. Use of masked or sanitized test data in non-production environments when production is used; if this is not feasible, approvals to use non-sanitized data with implementation of the same level of controls in non-production environments as in production environments.

9. Determine whether management appropriately considers the uses and risks of data analytics and performs the following:

   a. Limits access to analytics tools and related outputs.
   b. Incorporates confidentiality, integrity, and availability when designing or selecting analytics tools.
   c. Inventories the data sources, assesses the information type according to the entity's data classification policy, and appropriately secures those sources.
   d. Develops design requirements and parameters for analytics.
   e. Obtains sufficient knowledge for management and personnel to interpret dashboards and reports.
   f. Considers the following when implementing and using data analytics:
      - Documentation of the data types maintained, data owners and users, and purposes of reports.
      - Determination of stakeholders' usage needs.
      - Determination of potential opt-in considerations, based on information type, in analytics reports.
      - Determination of disclosure requirements in the event of an incident.

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

Objective 4: Management implements appropriate ITAM processes to track, manage, and report on the entity's information and technology assets. (III.B, "IT Asset Management")

The examination procedures in this objective may be coordinated with related examination procedures in the "Information Security" booklet.

1. Determine whether management has a comprehensive inventory of its electronic (or digital) and physical information assets, in accordance with the Information Security Standards. Evaluate whether management specifically identifies its information assets, determines the appropriate classification of those assets, and protects them according to the entity's data classification process.

2. Determine whether management implemented policies, standards, and procedures to govern all aspects of ITAM, including information and technology assets. Assess whether those processes include the following:

    a. Identifying the technology assets the entity possesses and manages.
    b. Determining each asset's status (e.g., active or inactive).
    c. Specifying the life cycle phase of those assets.
    d. Regularly reviewing and validating the accuracy of the inventories.
    e. Identifying personally owned technology assets that are allowed to connect to the entity's network.

3. Determine whether management uses appropriate inventory mechanisms to effectively document, track, and oversee the entity's information and technology assets, including its hardware and software. As part of the technology asset inventory, determine whether management considers IT assets that do not fall into traditional hardware or software inventories. Evaluate whether management has a process to periodically review and update the inventories. Assess the adequacy of management's technology asset inventory process for the following:

    a. Hardware inventory process that does the following:

- Identifies the entity's hardware assets.
- Identifies equipment owned and managed by third parties on the entity's behalf.
- Includes entity-owned and entity-managed virtual infrastructures.
- Assigns a unique identifier for hardware assets.
- Contains information about the network and telecommunications equipment.
- Contains appropriate information on each piece of hardware.

b. Software inventory process that does the following:
   - Provides detailed information on software used in the entity's IT environment.
   - Contains appropriate information on the entity's software.

4. Assess whether each IT asset is captured in the entity's ITAM inventory, tracked throughout its operational life, and prepared for physical removal at the end of its useful life. Determine whether management implemented policies, standards, and procedures to identify assets and their EOL time frames, to track assets' EOLs, and to replace or upgrade the asset. Determine the effectiveness of EOL management through the following:

   a. Addresses EOL in contract provisions with its third-party service providers.
   b. Adds assets to the inventories and tracks changes made to assets.
   c. Conducts risk assessments to determine assets' EOLs.
   d. Reviews EOL time frames for existing assets to determine accuracy and relevance.
   e. Develops replacement plans for assets nearing obsolescence.
   f. Establishes procedures for the secure destruction or data wiping of hardware and software.
   g. Considers the following when reviewing new technology assets:
      - Incorporates EOL considerations in strategic planning.
      - Plans for obsolescence during initial project stages (e.g., during requests for proposals or proofs of concept).
      - Registers and tracks assets in the inventories and includes EOL information.
      - Develops plans for maintaining IT assets beyond EOL, if necessary.

5. Determine whether management understands and communicates the risks of shadow IT to entity personnel. Additionally, determine whether internal audit evaluates management's processes to monitor, identify, and remove unapproved devices, software, or services. Assess whether management performs the following:

   a. Establishes IT governance practices and security controls for shadow IT, including policies, standards, and procedures.
   b. Includes shadow IT in security awareness training.
   c. Considers the use of IT detection tools to monitor for and identify shadow IT.
   d. Employs appropriate data protection and data loss prevention tools.
   e. Considers appropriate methods to address shadow IT, including:
      - Identifying security risks associated with shadow IT in use and determining whether there is malicious intent.
      - Identifying the reason for its use.
      - Determining clients or processes supported by shadow IT.

- Verifying interconnectivity between shadow IT and third-party service providers or existing software integration.
- Determining appropriate disposition of shadow IT.
- Reviewing policies, processes, and tools to understand any gaps that may allow shadow IT to occur.

f. Has processes to monitor, identify, and remove shadow IT that can be evaluated by internal audit.

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

1. Determine whether management documents and maintains accurate representations (e.g., network diagrams, data flow diagrams, business process flow diagrams, and business process narratives) of the current IT and business environments and employs processes to update the representations.

2. With the representations, assess whether management does the following:

   a. Coordinates the development of representations among stakeholders.
   b. Aligns diagrams and narratives with each other and across the entity's lines of business.
   c. Periodically reviews documented diagrams and narratives to confirm the accuracy of the representations of the IT and business environment.
   d. Provides for the resilience of this documentation by maintaining current and accurate backups.
   e. Implements appropriate access and editing privileges to the representations.

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

The examination procedures in this objective may be coordinated with related examination procedures in the "Development and Acquisition" booklet.

1. Determine whether the IT environment and its products and services, whether internally or externally provided, are adaptable to change, and stakeholders from across the entity have input into the change process.

2. Depending on the complexity of the change, determine the adequacy of the processes to manage the change. Verify that changes to any IT system or service are supported by an orderly, adaptable, documented, and measurable process.

   a. If the entity implements more complex types of changes (e.g., core conversions, migrations to cloud-based environments, or implementing a system to support a new product), assess whether formal planning and management oversight processes are in place and adequate.

b. If the entity implements less complex, but planned changes (e.g., implementation of patches), assess the appropriateness of the change process.

3. Determine whether the entity's policies, standards, and procedures address change management, including each step of the change process. Assess whether the process includes the following:

   a. Categorization of changes by severity.
   b. Specification of corresponding approval processes.
   c. Identification of responsible staff, applicable stakeholder working groups, or entity committees.
   d. Preservation of the IT environment's confidentiality, integrity, and availability.
   e. Identification of metrics to track the efficiency and success of the change.
   f. Implementation of changes with the goal of preserving confidentiality, integrity, and availability.
   g. Incorporation of appropriate segregation of duties and monitoring throughout the change management process.

4. Review and evaluate the entity's change management process to implement changes that preserve systems' security and are based on the change type (e.g., planned, routine, and emergency). Determine whether management follows pre-defined processes, such as the following:

   a. Request that includes the reasons for the change and details of the change.
   b. Review of requests to determine viability, business practicality, and prioritization.
   c. Approval through the appropriate documented hierarchy commensurate with the scope, cost, urgency, and overall risk.
   d. Design and build, including formal processes to preserve integrity throughout the development life cycle and ensure adequate controls.
   e. Testing, which documents that the change performs as intended, identifies flaws, and verifies that the change integrates with other systems.
   f. Implementation that includes a formal process to deploy the change.
   g. Verification and closure, including a post-implementation review and processes to document the change's closure.

5. When reviewing change management, evaluate the following transition processes:

   a. Management implements a process to transition system changes from a strategic change management process to day-to-day operations.
   b. Knowledge is adequately transferred to personnel who will be responsible for operating the systems and processes.
   c. Change management processes allow for the transition of responsibilities and knowledge and are part of the overall system development life cycle.

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

1. Determine whether management identifies internal and external roles and responsibilities for AIO activities and implements processes to oversee those activities performed by third-party service providers. Assess whether management appropriately assigned and defined the responsibility and oversight of those activities.

2. Verify whether management identifies and addresses all risks according to contracts and other agreements (e.g., SLAs).

3. With respect to data destruction processes at the third-party service provider, determine the following:

    a. Management is aware of the data destruction processes maintained by the entity's third-party services providers, including cloud service providers.
    b. SLAs outline adequate third-party service providers' data destruction measures.

4. Determine whether management reviews independent audit or other assurance reports demonstrating the third-party service provider's ability to meet the entity's AIO needs.

5. Verify that management reports to the board on the effectiveness of any AIO activities performed by third-party service providers. Assess whether the reporting included any issues uncovered through the entity's third-party risk management processes.

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

1. Evaluate whether management integrates the entity's AIO functions into the entity's BCM program to mitigate threats, respond to and recover from disruptions, and incorporate lessons learned to strengthen the entity's resilience.

2. Determine whether management designs, implements, and operates its IT systems and processes to provide resilience for critical business activities. Assess whether management does the following:

    a. Determines its reliance on people, processes, and technology, including third-party service providers, to assist in its assessment of risk.
    b. Ensures the entity's business strategy and reliance on business functions drive the design for the entity's resilience.
    c. Designs systems and software with resilience and information and cybersecurity at the beginning of the architecture process.
    d. Uses infrastructure that supports varying levels of resilience depending on the criticality of the systems and software to ongoing business operations.

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

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

1. Evaluate whether management considers the implications of remote access in AIO and does the following:

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

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

1. Determine whether management adequately considered AIO in the decision to allow the use of personally owned devices. Specifically, evaluate the effectiveness of the following:

    a. Due diligence to determine types of devices that can be used.
    b. Consideration of the architecture of the entity's IT systems, such as where and how the devices will access the bank's network.
    c. Determination of additional infrastructure needed to support the secure use of personally owned devices.
    d. Controls needed to adequately safeguard the network.
    e. Use of technical policy enforcement to manage or restrict devices used.

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

1. Determine whether management considers risks related to exchange files and implements effective mitigation, such as the following:

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

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

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

a. Consideration of the entity's architecture requirements for its existing technology and any planned changes.
b. Understanding by business units of their portion of the design.
c. Alignment with management's defined mission and any strategic initiatives for architecture.
d. Identification of the entity's IT assets, external constraints, industry IT architecture trends, and the entity's needs for the desired future state.

2. Determine whether management has policies, standards, and procedures to govern the entity's architecture design process and whether the design process addresses the following:

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

3. Evaluate the adequacy of the entity's documented and approved architecture plan. Consider whether management considers the following in relationship to the plan:

a. Alignment with the entity's strategic plan and support for the business and strategic objectives of the entity.
b. Development of policies, standards, and procedures to govern architecture initiatives and changes to the architecture plan.
c. Inclusion of processes for obtaining approvals, making changes to the plan, and reporting, as appropriate.
d. Alignment of the formality of the architecture plan and processes with number and complexity of the architecture initiatives.
e. For larger or more complex architecture changes, maintenance of a project management process that includes the following:
    - Planning.
    - Execution.
    - Closeout.

4. With respect to design objectives, determine whether management does the following:

a. Uses defined terminology.
b. Evaluates its needs and considers:
    - Collaboration between IT and business units.
    - Prioritization of investments.
    - Comparison of existing architecture with anticipated future changes.
    - Establishment of processes to evaluate and procure technology.
    - Storage, backup, and capacity needs to accommodate the entity's strategic plans.

- Type of applications the architecture will support.

c. Includes the following aspects in its architecture design:
   - Performance and reliability.
   - Integrity.
   - Availability and resilience.
   - Scalability.
   - Flexibility.
   - Security and privacy.
   - Interoperability and integration.
   - Ability to integrate and align with one or more third-party service providers.
   - Testing internally and with third-party service providers, as appropriate.
   - Auditability.
   - Advancements in technology.

d. Includes considerations for avoiding the potential for shadow IT and the capability to monitor and alert for its use.
e. Considers how evolving technologies (e.g., cloud, IoT, and AI/ML) can affect its design.
f. Plans for obsolescence, EOL, and decommissioning of systems.

5. Evaluate whether management has a process to determine appropriate deployment environments (e.g., in-house or serviced, virtualization and cloud, or hybrid) as part of the design process. Determine whether the process includes the following considerations:

   a. Identification of risks and benefits of each type of deployment environment.
   b. Use of physical versus virtual components in the design.
   c. Type of virtualization solution and design risks associated with the following elements:
      - VMs and the design of secure virtual infrastructures to provide the ability to oversee the interconnectivity and segmentation of VMs.
      - Hypervisors and the design of where the hypervisors sit and the connectivity between hypervisors and VMs.
      - Containers, including the design for storing data outside of the container and implementation of vulnerability management processes, segmentation, and the ability to monitor containers.
      - Microservices, including a design process that allows for the use of microservices as an integrated component to overall IT operations and the ability to address the risks of security, reliability, and latency in the entity's development process.
   d. Placement and selection of storage, design of network topology, availability of bandwidth, and need for management reporting systems, as well as implementation of monitoring tools.

6. In larger or more complex entities, determine whether management considered using EA to align its architecture with the entity's strategic plans and business functions. Describe management's implementation of EA and use of architecture frameworks, if appropriate. Regardless of entity size, determine whether management incorporated the following:

   a. Evaluation of approaches to implement and build security and resilience throughout its architecture.

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

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

1. Determine whether the entity's IT infrastructure implementation includes considerations for server and data redundancy and resilience of telecommunications lines.

2. *This examination procedure may be performed in coordination with the examination procedures in Objective 4 (ITAM).* Determine whether management has effective processes related to ITAM to track and monitor all hardware assets (whether or not they are connected to the network) to maintain an accurate and current record of the technology assets in its environment. As part of these processes, determine whether management does the following:

   a. Identifies unauthorized technology assets and determines their disposition.
   b. Evaluates how unauthorized devices gained access and whether any compromise occurred.
   c. Updates the related policy or procedures or provides additional training.

3. *This examination procedure may be performed in coordination with the examination procedures in Objective 4 (ITAM).* Determine whether management documents and maintains a current inventory of network and telecommunications hardware and software and the standard network configuration for them. Additionally, determine whether management does the following:

   a. Implements appropriate redundancy capabilities for the entity's telecommunications infrastructure.
   b. Understands the limitations of the entity's third-party telecommunications providers' infrastructure.
   c. Documents the network's baseline configuration, including processes to review and approve changes.
   d. Regularly assesses and documents compliance with the entity's baseline configuration.
   e. Appropriately controls networked devices by managing ports, protocols, and services and maps them to the devices on the technology asset inventory.
   f. Installs the latest version of security-related updates on network devices, when appropriate.
   g. Maintains standard images of the entity's servers and stores them securely. Uses clean (i.e., trusted) images to restore the server if a server needs to be rebuilt and documents, reviews, and approves deviations from the standard image.
   h. Implements security and monitoring throughout the entity's network, analyzes incoming and outgoing data traffic, and alerts authorized personnel if anomalous activity is detected. Additionally, determine whether the following security and monitoring mitigation strategies are in place:

- Use of software tools to protect against and monitor internet-accessible services or open ports.
- Implementation of firewalls and port filtering.
- Deployment of IDS/IPS.
- Use of internal tools to detect, identify, and prevent misuse by entity personnel.

i. Performs administrative activities from dedicated workstations.
j. Uses multi-factor authentication over encrypted network connections for administrators accessing and managing network devices.
k. Monitors telecommunications traffic and periodically reviews network devices.
l. Appropriately controls telecommunications equipment, including:
   - Physically securing it and restricting and monitoring access to it.
   - Following enterprise change control standards.
   - Following entity policies, standards, and procedures for identification, authorization, and authentication to access telecommunications systems.
m. Designs and builds telecommunications infrastructure components for resilience (e.g., implement route diversity), including selecting infrastructure components and telecommunications providers that help avoid a single point of failure.
n. Addresses voice communications risks through development and acquisition processes, and in written policies, standards, and procedures. If the entity uses VoIP for voice communications, determine whether management performs a comprehensive risk assessment to ensure confidentiality, integrity, and availability in voice communications.
o. Implements physical and logical controls in the VoIP environment, evaluates options for backup systems, and considers control solutions specific to VoIP, such as VoIP-ready firewalls.
p. Monitors incoming and internal data communications traffic for problems.
q. Implements redundant telecommunications services and establishes work-around procedures for situations where needed.

4. Evaluate whether management determines the types of software needed to implement the entity's strategic objectives and considers the software's scalability, interoperability, and portability. As part of its software infrastructure planning, determine whether management performs the following:

   a. Tracks and monitors the entity's software assets.
   b. Maintains an accurate and current record of its software assets (e.g., with a software inventory).
   c. Periodically reviews existing software.

5. *This examination procedure may be performed in coordination with related examination procedures in the "Development and Acquisition" booklet.* Determine whether management appropriately chooses software (e.g., to meet the entity's infrastructure and operational requirements) and considers whether to develop software internally or obtain it from a third party.

a. With internally developed software, evaluate whether management is responsible for maintaining the software, and entity personnel have the resources and expertise to stay abreast of vulnerabilities and develop software updates and patches.
b. With externally developed software, evaluate whether management performed the following:
   - Determined whether COTS software meets the entity's needs and security requirements or if it will integrate with existing software and require further configuration.
   - Determined whether custom software was designed to integrate with the existing enterprise software, hardware, and data, and whether management considered issues related to obsolescence, patching, and availability of expertise.
c. Regardless of the type of externally developed software selected, determine whether management performed the following:
   - Approved the selected software's use and determined that it met the entity's infrastructure requirements and strategic objectives.
   - Allocated resources to support the software (e.g., financial and personnel) and determined that personnel have the expertise to maintain and patch the software.

6. *This examination procedure may be performed in coordination with related examination procedures in the "Development and Acquisition," "Information Security," and "Outsourcing Technology Services" booklets.* Determine whether management is aware of and implements risk mitigations for general risks (e.g., software vulnerabilities and unauthorized access) associated with software in the entity's infrastructure environment. With respect to specific software types, determine whether management does the following:

a. For OS software:
   - Oversees and maintains the OS, including testing and installing patches when appropriate.
   - Restricts and monitors administrator access to the OS.
   - Limits the use of utility software.
b. For core processing software:
   - Restricts software based on job responsibility.
   - Monitors its use.
   - Selects core processing software with adequate capacity.
   - Chooses software that can support usage spikes, expected peak usage times, and future growth.
c. For productivity software:
   - Considers the use of it to enable personnel to perform their job functions.
   - Safeguards systems against security threats and employs IAM, configuration management, and log monitoring.
   - Employs mitigation strategies to address synchronization issues.
d. For enterprise software:
   - Considers how enterprise software integrates in the entity's infrastructure environment.
   - Limits access and editing capabilities.
   - Monitors user activity.

e. For security software:
   - Uses security software that is current, deployed effectively, and designed to keep up with the evolution of malicious code.
   - Restricts administrative access to this type of software.

f. For system auditing software:
   - Uses system auditing software to augment audit personnel.
   - Uses the software to assist in the identification of gaps in infrastructure security and resilience.
   - Documents software for system audit use and defines its purpose.

g. For open source software:
   - Identifies security issues with its use.
   - Implements security controls and procedures to mitigate risks, including the following:
     - Defining acceptable use (or restriction) guidelines and documenting a process for modifying and reviewing the code.
     - Restricting access to unapproved shareware sites.
     - Using tools to help discover unapproved open source software.
     - Identifying the type and version of open source software in use, where it is used within the entity, and its purpose.
     - Implementing version and patch control guidelines for open source software in use.
     - Monitoring for vulnerabilities of the open source software employed by the entity.
   - Evaluates implications of open source components in third-party software and addresses their use in contract provisions.
   - Evaluates open source software components during software due diligence.

h. For mainframe security software:
   - Implements access controls (e.g., role-based access, segregation of duties, and multi-factor authentication).
   - Uses security controls.
   - Encrypts sensitive information.
   - Enables activity log settings (e.g., user access, failed login attempts, and security setting changes).
   - Implements real-time monitoring and alerting.
   - Performs timely patch management.
   - Verifies mainframe security auditing (e.g., regular review and validation of security controls, privileges, roles, and access profiles).
   - Independently monitors privileged accounts (e.g., system and security administrators).
   - Maintains appropriate mainframe security expertise.

i. For APIs:
   - Assesses and implements security needs for APIs.
   - Addresses authorization, authentication, and encryption.
   - Implements API security tools and gateways with controls for requests and responses.
   - Performs sensitive data filtering.

- Places restrictions on size and number of resources requested.
- Identifies API request checkpoints for information leaving the network.
- Performs appropriate API logging and monitoring.
- Implements other security controls (e.g., secure IPs, password hashing, restriction of secret information, authorization protocols, validation mechanisms, time stamping, rate limiting, API traffic monitoring, and API gateway configuration) as appropriate for internal APIs.
- Implements adequate security and restrictions over the use of public APIs to protect sensitive customer and entity data and performs appropriate testing to verify the adequacy of security controls over a third party's APIs.
- As part of its customer awareness program, makes security awareness information available to its customers using unaffiliated third-party API services. Determine whether the information addresses protections available and not available when the customer allows access to its data.

7. *This examination procedure may be performed in coordination with related examination procedures in the "Outsourcing Technology Services" booklet.* Determine whether management performs the following, depending on the type of software hosting involved:

   a. For internally hosted software, determine whether management:
      - Identifies personnel (e.g., internal or third-party) with relevant skills and expertise.
      - Allocates resources for necessary training to maintain knowledge.
      - Follows a system development life cycle that incorporates security if the entity develops software in-house.
   b. For externally hosted software, determine whether management:
      - Has contract provisions addressing the notification of infrastructure changes and the third party's use of any subcontractors.
   c. For hybrid hosted software arrangements, determine whether management:
      - Performs an adequate risk assessment to prepare for a potential service interruption.

8. *This examination procedure may be performed in coordination with related examination procedures in the "Business Continuity Management" booklet.* Determine whether management developed, documented, and implemented environmental control policies, standards, and procedures to safeguard facilities, technology, data, and people. Specifically, determine whether management has effective environmental controls to identify and mitigate risks from infrastructure and operational issues. Evaluate whether remotely available environmental controls (including IoT devices used for environmental monitoring), whether by a third-party service provider or not, have appropriate access controls, monitoring of remote access activity, and regular review of privileges. Additionally, determine whether third-party service provider access for maintenance and administrative purposes are appropriately controlled.

9. Review the effectiveness of management's mitigation of the risks associated with the following:

   a. HVAC controls, including:

- Maintaining appropriate temperature and humidity levels.
- Monitoring HVAC.
- Implementing automated monitoring and providing an alarm or notification of significant temperature changes.
- Considering the entity's need for redundant HVAC equipment components.

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

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

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

Objective 14: Management develops and implements operational controls to safeguard the entity's operational environment. (VI.A, "Operational Controls")

The examination procedures in this objective may be performed in coordination with related examination procedures in the "Information Security" booklet.

1. With respect to operating centers, describe the entity's operating center type and key responsibilities and determine whether functions such as security and network management are addressed. Evaluate the appropriateness of the entity's processes and controls, such as the following:

   a. Responsibility for the physical location as well as the on-premise equipment and systems in entity-owned versus outsourced operating centers.
   b. Contract(s) specifying equipment ownership and responsibility, if management of the operating center is outsourced.
   c. Operating centers located in areas less prone to environmental threats.
   d. Appropriate security and environmental controls within the entity's infrastructure, including:
      - Use of smoke, water, and power detection and mitigation devices and systems, as well as fire suppression systems.
      - Use of security zones limiting access within restricted spaces.
      - Implementation of physical security controls.
      - Use of devices to restrict and log access to the site.
      - Procedures for appropriate site maintenance.
   e. Responsibilities for implementing security and environmental controls.
   f. Operating center responsibilities, including:
      - Training staff to operate and maintain the entity's equipment and systems.
      - Deploying appropriate connectivity.
      - Managing incidents and events.

2. Determine whether management defines the entity's authorization boundary(ies) and implements appropriate security controls according to the contents of the authorization boundary, including controls over the following:

a. Internal and external communication systems within and across the entity's authorization boundary(ies).
b. The connection between the entity and its third parties.
c. Physical, logical, and environmental controls.
d. Perimeter protection devices.
e. People and processes supporting the entity's missions and business functions.

3. Determine whether management implements appropriate IAM processes and does the following:

a. Appropriately provides access to the entity's resources.
b. Considers enhanced authentication, especially for privileged access.
c. Considers its implementation of cloud services and addresses the unique access control requirements for cloud environments, as appropriate.
d. Maintains a policy and implements related standards and procedures to identify users and restrict their access.

4. Determine whether management has processes for employee recruitment, hiring, and placement and provides for thorough applicant screening and background checks at the time of employment. Review the following and evaluate their effectiveness:

a. Performance of background checks at an appropriate frequency.
b. Definition of duties, responsibilities, expectations, and accountability.
c. Implementation of dual control and segregation of duties.
d. Independently monitoring activities.
e. Implementation of rotation of duties.
f. Reviewing and monitoring of activities performed during rotation of duties.

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

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

1. Determine whether management has assigned responsibility for the performance of maintenance on the entity's equipment. Evaluate whether the following is effective:

a. Routine maintenance by data center employees is performed according to manufacturers' recommendations.
b. Preventive maintenance follows a predetermined schedule.
c. Operations employees document both internal routine (if any) and externally provided maintenance in logs and other records.
d. Management reviews maintenance records.

e. For equipment owned or leased from a third party, management obtains a separate agreement to manage maintenance. The agreement includes:
   - Preventive maintenance to be performed.
   - Provisions for repair services.
   - Schedule for maintenance and time frame for repair.

f. Management provides time and resources for scheduled preventive maintenance, which includes:
   - Limiting the service representative's access to the minimum necessary.
   - Having at least one computer operator present when the service representative is on site.
   - Reviewing system activity logs to monitor access to programs or data during maintenance.
   - Following established security procedures to ensure representatives have only the necessary access at predetermined times to perform specific tasks.

g. If there is an arrangement with a contractor to manage the entity's preventive maintenance and repair services, the contract or agreement guarantees timely performance of maintenance.

h. If computer maintenance is performed online, the online maintenance schedule is available to prevent interference with normal operations and processing.

i. Maintain a log of all hardware or software problems and downtime encountered between maintenance sessions.

2. Evaluate whether management has policies, standards, and procedures for configuration management and defines and implements appropriate configuration settings. In addition, verify whether management does the following:

   a. Appropriately defines and applies configuration settings on IT products at the entity.
   b. Ensures that systems and software used to support entity operations have appropriate configuration management capabilities, including configuration of audit log settings, and enforces configuration management.

3. Determine whether management establishes procedures to stay abreast of system vulnerabilities and software vendor patches, tests patches in a segregated environment, and installs them when appropriate. Additionally, determine the effectiveness of the following:

   a. Management implements a vulnerability management program that identifies systems and software vulnerabilities, prioritizes the vulnerabilities and the affected systems in order of risk, and performs timely remediation according to the risk of the vulnerability. The vulnerability management program includes the following:
      - Systems and software operating in the cloud for which the entity is responsible as well as those managed by the entity on its premises.
      - Processes to monitor industry third parties (e.g., US-CERT, NIST, and FS-ISAC) that report vulnerability exposures and address any relevant exposures within the entity's systems and software.
      - Processes to periodically assess systems and software for vulnerabilities using scanners with current vulnerability lists.

- Vulnerability scans of all systems and software in the entity's hardware, software, and telecommunications inventories.
- Appropriate controls over vulnerability scanning tools, including controls to protect against unauthorized use or access to sensitive information.
- Use of dedicated accounts for authenticated vulnerability scans.
- Methods to track and report on nonconformance to entity policies and the timeliness and remediation progress of all identified vulnerabilities, including those related to security procedures, physical layout, or internal controls.

b. Management implements a patch management program that includes documentation of any patch installations. The patch management program includes the following:
   - Processes to document patch installations as part of the entity's change management procedures.
   - Systems and software for automated patch management or other demonstrated effectiveness in keeping up with patch identification, testing, and installation.
   - Records of the system and software versions in place and regular monitoring of online and industry resources for information on product enhancements, security or other issues, patches, or upgrades.
   - Communication and integration with the entity's third-party service providers to align the entity's patch management program with those of the third-party service providers.

4. *This examination procedure may be coordinated with the examination procedures in the "Business Continuity Management" and "Information Security" booklets.* Determine whether management implements backup methods, including replication, based on the risk and criticality of the systems and data.

   a. As part of its backup and replication processes, determine whether management maintains the following:
      - Policies, standards, and procedures.
      - Inventories of backup media, storage location, and access controls for the media or physical location.
      - Documented periodic physical reviews to confirm that all relevant backup material is available.
      - Procedures to verify adherence to backup schedules.
      - Processes to regularly test backup copies for readability.
      - Capability to restore operations to a previous trusted state.
      - Backups of configurations and data off-site and on a separate system or media.
      - VM versioning, replication, and life cycle policies for backup processes.
      - Data encryption and access controls to protect backup or replicated data from unauthorized access, destruction, or corruption.
      - Proper sanitization and disposal of data when it is no longer needed to prevent the disclosure of information to unauthorized users.
   b. When using third-party service providers for backup and replication, determine whether management validates that the third-party service provider performs the processes above.

5. To meet scheduling needs, determine whether management implements policies, standards, and procedures for creating and changing job schedules and analyzing and maximizing the entity's resources.

6. Determine whether management implements adequate capacity management processes. Additionally, evaluate whether the processes provide for the following:

   a. Integration with the budgeting and strategic planning processes.
   b. Addressing internal and external factors.
   c. Routine assessment of capacity against baselines to ensure adequate performance in the following:
      - Platform processing speed.
      - Primary working memory for each platform's CPU.
      - Additional data storage capacity.
      - Voice and data communication bandwidth.
   d. Analysis of capacity trends (e.g., increasing capacity usage) to understand capacity usage.
   e. Analysis of help desk records, as appropriate, for capacity issues.
   f. Periodic analysis of projected versus actual capacity.
   g. Verification through testing to ensure systems and software meet the entity's demands during periods of high volume.
   h. Meeting between IT management and business line management to determine future projects that may impact capacity needs.
   i. Consideration of flexibility to accommodate the entity's future capacity requirements.
   j. Evaluation of third-party service providers' performance in combination with internal performance to determine whether capacity can meet existing and future demands.

7. Determine whether management has a log management process to use logs to identify, track, analyze, and resolve problems that occur during day-to-day operations. Describe how management collects and collates logs and how management uses logs to respond to issues. Evaluate how management addresses the following:

   a. Identification and disposition of false positives and adjustment of logging parameters to minimize the volume of false positives in future log review.
   b. Implementation of policies, standards, and procedures for log management activities that address the following:
      - Objectives for logging.
      - Types of logs to be collected.
      - Controls to restrict access to log settings.
      - Response time for log review.
      - Retention time frames and storage policies of logs.
      - Escalation processes for anomalies.
   c. Configuration of logging to match the entity's risk and complexity of the entity and identify and address anomalies.
   d. Consideration of tools to automate log analysis and extract important events or patterns.
   e. Implementation of controls to protect logs.

8. Determine whether management implements policies, standards, and procedures to address media and equipment disposal or transfer. Evaluate whether management addresses the following:

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

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

1. Determine whether management designs the entity's service management functions with an emphasis on preventing issues and ensuring continuous reliability and resilience where possible. Evaluate whether management performs the following:

    a. Considers the following as part of its service management planning:
        - Services offered and SLA, OLA, or contractual provisions.
        - Activities performed by third-party service providers.
        - Known limitations (e.g., capacity or resources) that may affect service management activities.
        - Applicable legal and regulatory requirements.
        - Resources necessary to carry out service management functions and activities.
        - Metrics and measurements used to evaluate service management effectiveness.
    b. Utilizes documented OLAs or another method to communicate and coordinate the entity's business requirements to personnel responsible for the execution of service management functions.
    c. Coordinates its processes with third-party service providers, when used, to ensure seamless functionality to the entity's lines of business.
    d. Coordinates meetings between process owners from both business and technology functions to discuss known issues, changes in progress, and future changes.

2. As part of the entity's operational support processes, determine whether the following is performed:

    a. Management implements the following:
        - Processes to verify that incoming data transmissions and processing are complete and accurate.

- Controls to verify that external data transmissions and processing are securely received.
- Controls to verify that data were not corrupted during transmission or processing failures.
- Mechanisms to report transmission and processing errors.

b. Operational support personnel report errors or problems with the systems or software and provide updates on resolution.

3. Determine whether the entity has an IT support function. If there is, evaluate it for the following:

   a. Processes for recording and tracking incoming issues, whether handled by human operators or automated systems.
   b. Tracking system documentation that includes:
      - User name and contact information.
      - Problem description.
      - Request type and category.
      - Affected system.
      - Prioritization code.
      - Current status toward resolution.
      - Individual or group responsible for resolution.
      - Root cause, when identified.
      - Target resolution time frame.
      - Comments related to user interaction with IT support and other information.
   c. Well-trained and knowledgeable IT support personnel.
   d. Appropriate training for IT support personnel to perform their duties, if IT support software is used.
   e. Procedures to authenticate users to prevent unauthorized access to information or credentials.
   f. Layered security and supplemental authentication techniques for changes to account maintenance activities and for high-risk transactions.
   g. For outsourced IT support functions, management's IT support expectations and responsibilities for the third-party service provider are included in the contract.

4. *This examination procedure may be coordinated with related examination procedures in the "Business Continuity Management" and "Information Security" booklets.* Determine whether management has processes to manage events, incidents, and problems. Evaluate the effectiveness of the following:

   a. Implementation of entity processes to plan for and manage events, incidents, and problems, including:
      - Coordinating and defining roles and responsibilities.
      - Conducting testing to identify interdependencies.
   b. Establishment and maintenance of appropriate processes and controls, including:
      - Identifying the event, incident, or problem.
      - Determining the impact.

- Assigning a severity rating based on risk.
- Performing root cause analysis.
- Identifying, logging, tracking, and analyzing events, incidents, and problems.
- Maintaining contact information for individuals and groups for notification purposes.
- Informing the help desk of the event, incident, or problem and how to respond.
- Resolving the event, incident, or problem, including approval processes for system or software changes to correct the issue.
- Documenting any interim actions, compensating controls, and risk acceptance for issues that cannot be immediately resolved.
- Developing longer-term action plans to monitor and address issues.
- Reporting on the progress of the action plans to senior management.
- Implementing procedures for escalation and reporting.
- Implementing procedures to correlate events.

c. Performance of periodic trend analysis to find recurring or related issues that may be tracked to a common root cause.
d. Maintenance of management plans that cover hardware, software, and security devices.
e. Communication of processes to manage events, incidents, and problems to appropriate personnel.
f. Coordination and inclusion of processes with the entity's incident response program.

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

1. Determine whether management implements processes to monitor IT operations and periodically reports on the effectiveness of established controls to senior management and other stakeholders. Evaluate the following:

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

e. If an entity has outsourcing arrangements in the cloud, determine whether management explores the use of tools designed for cloud computing.

2. Determine whether management defines objectives for IT and operations and KPIs to help management measure those objectives. Additionally, evaluate whether management does the following:

   a. Aligns KPIs with the entity's ERM processes and uses those KPIs to assess the performance of IT and operations across the entity.
   b. Sets KPI benchmarks to achieve and analyzes deviations from those benchmarks.
   c. Automates the collection of KPIs, where possible.
   d. Has a useful set of KPIs.
   e. Regularly reviews KPI reports and provides appropriate reporting up to the board.
   f. Implements corrective action plans to address deviations or negative trends, assigns individuals responsible, and monitors progress to completion.
   g. Meets with stakeholders to review IT and operations KPIs to determine whether they are appropriate indicators of the ability to meet the entity's strategic objectives.

3. Determine whether management uses control self-assessments, risk control self-assessments, or other methods to monitor the effectiveness of IT operations controls and gauge performance, assess the criticality of systems, and identify existing risks. Determine whether management evaluates results and uses them to continuously improve the entity's operations.

4. Determine whether management has a continuous improvement process in place to recommend changes to the entity's IT environment. Evaluate whether management does the following:

   a. Develops improvement strategies for operations and prioritizes projects.
   b. Bases improvement decisions on the potential benefit and ease of implementation, with a focus on important IT processes and core competencies.
   c. Maintains a process to measure the results of continuous improvement efforts and includes the following:
      - Ongoing practice of process improvement.
      - Enterprise-wide practice of service improvement that augments the ability to provide value to its stakeholders and customers.

Objective 18: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the examiner-in-charge regarding the following:

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

2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.

3. Document conclusions in a memorandum to the examiner-in-charge that provides report-ready comments for all relevant sections of the report of examination and clarifying guidance to future examiners.

4. Organize work papers to show clear support for significant findings by examination objective.

APPENDIX B: GLOSSARY

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

When a NIST definition existed:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

APPENDIX C: ABBREVIATIONS

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

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

APPENDIX D: REFERENCES

Laws

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

Consumer Financial Protection Bureau

Regulations

12 CFR 1005, "Electronic Fund Transfers (Regulation E)"
12 CFR 1016, "Privacy of Consumer Financial Information (Regulation P)"
12 CFR 1022, "Fair Credit Reporting Act (Regulation V)"

Guidance

CFPB Compliance Bulletin and Policy Guidance; "2016-02: Service Providers" (October 2016)

Federal Deposit Insurance Corporation

Regulations

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

Guidance

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

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

Federal Reserve

Regulations

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

Guidance

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

National Credit Union Administration

Regulations

12 CFR 748, "Security Program, Report of Suspected Crimes, Suspicious Transactions, Catastrophic Acts and Bank Secrecy Act Compliance"
12 CFR 748, appendix A, "Guidelines for Safeguarding Member Information"

12 CFR 749, "Guidelines for Safeguarding Member Information, Records Preservation Program and Appendices—Record Retention Guidelines; Catastrophic Act Preparedness Guidelines"
12 CFR 749, appendix A, "Record Preservation Program and Record Retention"

Guidance

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

Risk Alerts

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

Office of the Comptroller of the Currency

Regulations

12 CFR 5.30, "Establishment, Acquisition, and Relocation of a Branch of a National Bank"
12 CFR 5.31, "Establishment, Acquisition, and Relocation of a Branch and Establishment of an Agency Office of a Federal Savings Association"
12 CFR 30, appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness"

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

Guidance

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

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

Other References

American Institute of Certified Public Accountants (AICPA), *SOC 2 Examinations and SOC for Cybersecurity Examinations: Understanding the Key Distinctions* (2017)

Center for Internet Security (CIS), *Control 3: Continuous Vulnerability Management* (March 2017)

Financial Services Information Sharing and Analysis Center, *FS-ISAC*

International Organization for Standardization / International Electrotechnical Commission, ISO/IEC 27002:2013, *Information Security Management Section 11: Physical and Environmental Security* (October 2013)

Internet Engineering Task Force (IETF), *RFC 7591 OAuth 2.0 Dynamic Client Registration Protocol* (July 2015)

Martzloff, François, *A New IEC Standard on the Measurement of Power Quality Parameters* (2000)

National Institute of Standards and Technology (NIST) Resources:

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

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

Open Web Application Security Project (OWASP) Foundation, *OWASP API Security Project* (2019)

U.S. Department of Defense (DoD), *Summary of the 2018 Department Of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (2019)

U.S. Department of the Treasury, *Data Governance Board Charter* (January 2020)