FFIEC Information Technology Examination Handbook

Management

NOVEMBER 2015

Contents

INTRODUCTION 3

I GOVERNANCE 4

I.A IT Governance 4

I.A.1 Board of Directors Oversight 4

I.A.2 IT Management 6

I.A.3 Enterprise Architecture 9

I.B IT Responsibilities and Functions 10

I.B.1 IT Risk Management Structure 10

I.B.2 Information Security 10

I.B.3 Project Management 11

I.B.4 Business Continuity 12

I.B.5 Information Systems Reporting 12

I.B.6 Planning IT Operations and Investment 14

I.B.7 Other Functions 18

II RISK MANAGEMENT 20

II.A Operational Risk 20

III IT RISK MANAGEMENT 21

III.A Risk Identification 22

III.A.1 Ongoing Data Collection 22

III.B Risk Measurement 24

III.C Risk Mitigation 26

III.C.1 Policies, Standards, and Procedures 27

III.C.2 Personnel 27

III.C.3 Information Security 28

III.C.4 Business Continuity 30

III.C.5 Software Development and Acquisition 31

III.C.6 IT Operations 31

III.C.7 Insurance 32

III.C.8 Third-Party Management 34

III.D Monitoring and Reporting 36

III.D.1 Metrics 36
III.D.2 Performance Benchmarks 37
III.D.3 Service Level Agreements 37
III.D.4 Policy Compliance 37
III.D.5 Effectiveness of Controls 38
III.D.6 Quality Assurance and Quality Control 38
III.D.7 Reporting 38

APPENDIX A: EXAMINATION PROCEDURES 40

APPENDIX B: GLOSSARY 57

APPENDIX C: REFERENCES 63

Introduction

The "Management" booklet is one of 11 booklets that make up the *Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook* (*IT Handbook*). The "Management" booklet rescinds and replaces the June 2004 version. This booklet provides guidance to examiners and outlines the principles of overall governance and, more specifically, IT governance. Additionally, this booklet explains how risk management is a component of governance and how IT risk management (ITRM) is a component of risk management. This booklet describes the interaction of these components. The examination procedures in this booklet assist examiners in evaluating the following:

- IT governance as part of overall governance in financial institutions.
- Processes for ITRM as part of risk management in financial institutions.[1]

IT supports most aspects of a financial institution's business; therefore, effective ITRM is not limited to technology. The IT department typically manages back-office operations, network administration, and systems development and acquisition, and is involved in business continuity and resilience, and third-party management. IT management provides expertise in choosing and operating technology solutions for an institution's lines of business (e.g., commercial credit and asset management) or for enterprise-wide activities (e.g., security and business continuity planning).

IT management is critical to the performance and success of a financial institution. ITRM involves more than containing costs and controlling operational risks and does not work in isolation. A financial institution capable of aligning its IT infrastructure to support its business strategy adds value to the institution and positions itself for sustained success. Financial institutions face many challenges in today's marketplace, including cybersecurity threats, increasing the need for effective IT management and ITRM.

An institution's IT systems may connect with affiliates, customers, internal lines of business, third parties (e.g., third-party providers[2]), and the public. IT creates interdependencies among infrastructure, applications, and Web content. These interdependencies affect the decision-making process necessary to support existing products and services and provide for the delivery of new products and services. Timely, accurate, and secure information is critical to meeting business requirements throughout the institution. Technology evolves rapidly, requiring enhancements to existing systems and prompting new investment in infrastructure, systems, and applications. New technology requires expertise, which creates competition for the necessary

[1] The term "financial institution" includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions, as well as technology service providers that provide services to such entities. The term is used interchangeably with "institution" in this booklet. This booklet may refer to technology service providers specifically in cases where the agencies do not mean to include financial institutions.

[2] Third-party providers, also called third-party service providers, include technology service providers or other third parties that perform critical business activities for or on behalf of an institution.

talent, knowledge, and skill sets. ITRM includes addressing new sources of risk that arise with new or evolving technology.

I Governance

Action Summary

Financial institution boards of directors should oversee, while senior management should implement, a governance structure that includes the following:

- Effective IT governance.
- Appropriate oversight of IT activities.
- Comprehensive IT management, including the various roles played by management.
- Effective enterprise architecture.

Governance refers to how financial institutions manage and control their institution. Governance provides the structure through which an institution sets and pursues objectives while taking into account the regulatory and market environment and culture of the institution. The governance structure specifies the responsibilities for the board of directors, managers, auditors, and other stakeholders and specifies the level of authority and accountability for decision making. Governance also includes mechanisms for monitoring actions and decisions enterprise-wide.

I.A IT Governance

IT governance is "an integral part of governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."[3] IT governance objectives are to ensure that IT generates business value for the institution and to mitigate the risks posed by using technology.

I.A.1 Board of Directors Oversight

The board of directors sets the tone and direction for an institution's use of IT. The board should approve the IT strategic plan, information security program, and other IT-related policies. To carry out their responsibilities, board members should understand IT activities and risks. The board or a board committee should perform the following:

- Review and approve an IT strategic plan that aligns with the overall business strategy and includes an information security strategy to protect the institution from ongoing and emerging threats, including those related to cybersecurity.

[3] *Board Briefing on IT Governance*, 2nd edition, IT Governance Institute, 2003.

- Promote effective IT governance.
- Oversee processes for approving the institution's third-party providers, including the third parties' financial condition, business resilience, and IT security posture.
- Oversee and receive updates on major IT projects, IT budgets, IT priorities, and overall IT performance. The board of directors may need to approve critical projects and activities, such as expanding the institution's product line to include mobile financial services.
- Oversee the adequacy and allocation of IT resources for funding and personnel.
- Approve policies to escalate and report significant security incidents to the board of directors, steering committee, government agencies, and law enforcement, as appropriate.
- Hold management accountable for identifying, measuring, and mitigating IT risks.
- Provide for independent, comprehensive, and effective audit coverage of IT controls.

The board may delegate the design, implementation, and monitoring of specific IT activities to management or a committee (e.g., IT steering committee). An IT steering committee[4] generally comprises senior management and staff from the IT department and other business units. Committee members do not have to be department heads, but members should understand IT policies, standards, and procedures (collectively, policies[5]). Each member should have the authority to make and be held accountable for decisions within their respective business units. If the institution has a formal risk management function, risk management staff should participate in an advisory capacity.

The steering committee typically is responsible for reporting to the board on the status of IT activities. The reports enable the board to make decisions without having to be involved in routine activities. While the board may delegate the design, implementation, and monitoring of certain IT activities to the steering committee, the board remains responsible for overseeing IT activities and should provide a credible challenge[6] to management. The steering committee is typically responsible for strategic IT planning, oversight of IT performance, and aligning IT with business needs. The steering committee should have a charter that defines its responsibilities.

The steering committee should receive appropriate information from IT, lines of business, and external sources. Additionally, it should coordinate and monitor the institution's IT resources. The steering committee should review and determine the adequacy of the institution's training, including cybersecurity training, for staff. The steering committee should also document meeting minutes and decisions and inform the board of directors of the committee's activities.

[4] In smaller or less complex financial institutions that may not have steering committees, these functions would be performed by management, IT department personnel, the board, or a board committee.

[5] For the purposes of this booklet, policies generally include policies, standards, and procedures, unless stated otherwise. When the booklet refers to policies and practices, it is the combination of the formal and approved policies, standards, and procedures and the actual practices in place.

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

I.A.2 IT Management

IT management is responsible for IT performance and administering the day-to-day operation of an institution. IT management should perform the following:

- Implement IT governance.
- Implement effective processes for ITRM, including those that relate to cybersecurity.
- Review and annually approve processes for ITRM.
- Assess the institution's inherent IT risks across the institution.
- Provide regular reports to the board on IT risks, IT strategies, and IT changes.
- Establish and coordinate priorities between the IT department and lines of business.
- Establish a formal process to obtain, analyze, and respond to information on threats and vulnerabilities[7] by developing a repeatable threat intelligence and collaboration program.[8]
- Ensure that hiring and training practices are governed by appropriate policies to maintain competent and trained staff.

I.A.2(a) *Executive Management*

Executive management, including the chief executive officer (CEO), the chief operating officer (COO), and often the chief information officer (CIO), plays a significant role in IT management at a financial institution. Executive management develops the strategic plans and objectives for the institution and sets the budget for resources to achieve these objectives. To carry out its responsibilities, executive management should understand at a high level the IT risks faced by the institution and ensure that those risks are included in the institution's risk assessments. In the event that executive management is unable to implement an objective or agree on a course of action, executive management should escalate that matter to the board for more guidance.

I.A.2(b) *Chief Information Officer or Chief Technology Officer*

The CIO or chief technology officer (CTO) is responsible and should be held accountable for the development and implementation of the IT strategy to support the institution's business strategy in line with its risk appetite. In less complex institutions, the IT manager may take on these responsibilities. This position typically oversees the IT budget and maintains responsibility for performance management, IT acquisition oversight, professional development, and training. In addition, the CIO or CTO is responsible for implementing the IT architecture and participating in planning activities. The IT management reporting structure should enable this position to accomplish these activities and ensure accountability for security, business resilience, risk reporting, and alignment of IT with business needs. The CIO or CTO should play a key role in

[7] See the FFIEC's "Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement," November 3, 2014.

[8] For example, a repeatable threat intelligence and collaboration program could include internal resources, such as audit reports and fraud detection tools, or external resources, such as information sharing networks like the Financial Services–Information Sharing and Analysis Center (FS-ISAC) and the Federal Bureau of Investigation's (FBI) InfraGard.

the strategic planning as well as supporting activities of peers in various lines of business. The position often has a leadership role on the steering committee.

I.A.2(c) *Chief Information Security Officer*

The chief information security officer (CISO) is responsible for overseeing and reporting on the management and mitigation of information security risks across the institution and should be held accountable for the results of this oversight and reporting. Often, the CISO is responsible for implementing an information security program satisfying the Interagency Guidelines Establishing Information Security Standards[9] (Information Security Standards), which were issued pursuant to the Gramm–Leach–Bliley Act (GLBA). While in the past the office of the CISO was considered a technology function, the role has become a strategic and integral part of the business management team. The CISO should be an enterprise-wide risk manager rather than a production resource devoted to IT operations.

To ensure independence, the CISO should report directly to the board, a board committee, or senior management and not IT operations management. While cost and benefit decisions will always need to be made, IT security decisions and funding should not be unduly influenced by operational ease or budgetary constraints. The reporting structure should demonstrate that the CISO has the appropriate authority to carry out the responsibilities of that position and should avoid conflicts of interest that could interfere with the ability of the CISO to make decisions in line with the board's risk appetite. The institution's size and complexity plays a role in the reporting structure. A smaller or less complex institution may have an information security officer perform the responsibilities of the CISO and report to senior management. A larger or more complex institution may have additional reporting lines for the CISO into other independent functions, such as risk management.

The CISO is typically responsible for the following:

- Implementing the information security strategy and objectives, as approved by the board of directors, including strategies to monitor and address current and emerging risks.
- Engaging with management in the lines of business to understand new initiatives, providing information on the inherent information security risk of these activities, and outlining ways to mitigate the risks.
- Working with management in the lines of business to understand the flows of information, the risks to that information, and the best ways to protect the information.
- Monitoring emerging risks and implementing mitigations.
- Informing the board, management, and staff of information security and cybersecurity risks and the role of staff in protecting information.
- Championing security awareness and training programs.

[9] 12 CFR 30, appendix B (Office of the Comptroller of the Currency (OCC)); 12 CFR 208, appendix D-2 (Board of Governors of the Federal Reserve System); 12 CFR 364, appendix B (Federal Deposit Insurance Corporation (FDIC)); and 12 CFR 748, appendix A (National Credit Union Administration (NCUA)). Refer to appendix C of this booklet for a listing of laws, regulations, and agency guidance.

- Participating in industry collaborative efforts to monitor, share, and discuss emerging security threats.
- Reporting significant security events to the board, steering committee, government agencies, and law enforcement, as appropriate.

I.A.2(d) *IT Line Management*

IT line managers supervise the resources and activities of a specific IT function, department, or subsidiary. They typically coordinate services between the data processing area and other departments. They report to senior IT management on the plans, projects, and performance of their specific systems or departments. Some IT functions that often rely on line managers include data center operations, network services, application development, systems administration, telecommunications, customer support, and disaster recovery. Frontline managers coordinate daily activities, monitor current production, ensure adherence to established schedules, and enforce appropriate policies and controls in their areas.

I.A.2(e) *Business Unit Management*

Managers in an institution's lines of business or business units also have IT responsibilities. Examples of these responsibilities include the following:

- Establishing processes for ongoing communication of business needs, information systems reporting needs, and product development plans to IT support or line management.
- Ensuring that IT development efforts are prioritized, funded, and aligned with business strategy in the business unit.
- Establishing processes to test compliance with IT-related control policies in the business unit.
- Ensuring that required backup IT resources are available.
- Documenting information flows throughout the business unit and notifying the CISO when business processes change.
- Performing due diligence reviews for prospective third-party providers and ongoing monitoring of third-party providers with which the institution has established relationships.
- Engaging with the CISO to discuss inherent information security risks of new business unit initiatives.

The specific technology roles in IT and business unit management may vary depending on the institution's approach to risk management and policy enforcement. Institutions can approach technology management using either a centralized or a decentralized strategy.

In a centralized IT environment, IT management typically acquires, installs, and maintains technology for the entire institution. IT management has a greater ability to control and monitor the institution's technology investment. A centralized approach may promote greater operational efficiencies. The business unit managers retain the responsibility for enforcing internal controls within their areas.

In a decentralized IT environment, IT management serves in an advisory role in some business units' acquisition, installation, and maintenance of technology. The decentralized approach is

more common in larger or more complex institutions, where IT management can expedite decisions on IT services by transferring decision-making authority to strategically significant departments. In this approach, business line management has a much greater responsibility for ensuring that technology investments are consistent with enterprise-wide strategic plans. Institutions should ensure system compatibility and enforcement of enterprise-wide policies in a decentralized environment. IT management should still have a role in defining the institution's control requirements, but enforcement of enterprise-wide policies may be more difficult.

I.A.3 Enterprise Architecture

Enterprise architecture (EA) is the overall design and high-level plan that describes an institution's operational framework and includes the institution's mission, stakeholders, business and customers, work flow and processes, data processing, access, security, and availability. An EA program facilitates the conceptual design and maintenance of the network infrastructure, related IT controls, and policies. Management of financial institutions with highly complex systems or those experiencing growing IT costs without corresponding benefits should consider using or adjusting an EA program. As EA has evolved, different methodologies to implement EA programs have been developed. The underlying principle for all EA programs is that business IT requirements follow a predefined process that begins with a business need and ends with an IT solution that conforms to the policies approved by senior management and the board of directors. An effective EA program can result in the following:

- Enhanced interoperability from using IT to drive business adaptability.
- Closer partnership between business and IT groups.
- Improved focus on the institution's goals.
- Reduced numbers of failed IT systems.
- Reduced complexity of IT systems.
- Improved agility of IT systems.
- Closer alignment between IT deliverables and business requirements.
- Assurance that all software, including operating systems, is current and vendor supported.
- Improved morale, as more staff members see a direct correlation between their work and the institution's success.

Key considerations when developing an EA program include security, business resilience, data management, external connectivity, and alignment with the institution's goals and objectives. To effectively implement an EA program, the institution should analyze the risks and potential impact of threats to all of the institution's activities. A comprehensive EA program based on prudent practices can help an institution better develop processes to manage IT issues and identify, measure, and mitigate technology-based risks and threats.

I.B IT Responsibilities and Functions

Action Summary

As part of the governance structure, financial institution management should ensure development, implementation, and maintenance of the following:

- An effective IT risk management structure.
- A comprehensive information security program.
- A formal project management process.
- An enterprise-wide business continuity planning function.
- An accurate and timely process for information systems reporting.

I.B.1 IT Risk Management Structure

The institution should have an adequate ITRM structure. Depending on the size and complexity of the financial institution, this structure can take different forms. In a large or complex institution, the ITRM function may be an independent business unit.[10] In a small or less complex institution, ITRM may be integrated with functional areas, such as information security, business continuity planning, third-party management, and regulatory compliance. Internal audit, specifically IT audit, can provide independent assurance on the effectiveness of risk management, but should not be responsible for its implementation. Regardless of the structure used, management should ensure that lines of authority are established for enforcing and monitoring controls.

I.B.2 Information Security

The institution should have a comprehensive information security program that addresses all technology and information assets and that complies with the Information Security Standards; these standards and the GLBA are discussed in detail in the "Protecting Sensitive Customer Information" section of this booklet. The information security program should include appropriate administrative, technical, and physical safeguards based on the inherent risk profile and the individual activities, products, and services of the institution. The board should delegate responsibility to the CISO or other appropriate personnel for assessing whether IT operations conform with policies. The CISO should ensure appropriate consideration of risks involved with new products, emerging technologies, and information systems. Testing of the controls identified in the information security program should be delegated to an independent auditor.[11]

[10] Some agencies have guidance on ITRM for larger, more complex financial institutions.

[11] An independent audit function can include internal auditors with sufficient independence to perform an adequate review, outside consultants or auditors, or a combination of both.

The institution should separate information security program management and monitoring from the daily security duties of IT operations. The IT department should have personnel with daily responsibility for implementing the institution's security policy. Responsibility for making changes and granting exceptions to policy should be segregated from the enforcement of the controls. Refer to the *IT Handbook's* "Information Security" booklet for more information.

I.B.3 Project Management

An effective project management process is a key factor in a well-managed IT operation and includes applying knowledge, skills, tools, and techniques to achieve project objectives. The operational complexity of the institution dictates the degree of formality of project management practices. Generally, project management consists of initiating, planning, executing, controlling, and completing projects. The institution's ability to manage projects drives its ability to adapt to changes in its business requirements and satisfy its strategic objectives. Management uses project management techniques to control projects for systems acquisition and development, systems conversions, product enhancements, infrastructure upgrades, and system maintenance.

Project teams should balance resource investments of time, money, and expertise with a project's priority, risk, and requirements. Management should monitor projects closely to control costs and assure adherence to project management policies. A formal project management system, if used, should employ well-defined and proven techniques for managing projects at all stages. Regardless of the system used, management should include the following elements in its project management process:

- Oversight by experienced and skilled project managers, whether they are employees of the institution or consultants hired for specific projects.
- Accepted and standardized project management practices.
- Senior management support, including a review process around significant projects.[12]
- Defined and monitored institution-wide project risk assessment methodology.
- Approval processes to ensure that projects are defined, go through a risk assessment process, and meet requirements.
- Established project requirements with collaboration among stakeholders and project management staff for each phase of the project.
- Target completion dates to track each task or phase of the project.
- Timely project status updates to compare actual completion dates with target dates.
- Procedures to track and measure project performance against requirements.
- A defined change management process, including approval requirements.
- Sufficient testing at all appropriate stages of the project to ensure that the new system or process will not negatively impact existing systems.
- Training for end users and designated staff responsible for ongoing support.
- A well-managed process for transition in ownership from implementation teams to operational teams.

[12] The significance of projects will depend on the institution's activities and its size and complexity.

Based on an institution's size and complexity, an institution pursuing a more-than-moderate growth path should consider establishing a project management office to promote sound management practices and principles. Refer to the *IT Handbook's* "Development and Acquisition" booklet for more information.

I.B.4 Business Continuity

Business continuity is defined as the ability to maintain operations and services, both technology and business, in the event of a disruption to normal operations and services. The board of directors should oversee implementation and approve policies relating to business continuity planning. Senior management should establish and implement policies, standards, and procedures and define responsibilities for enterprise-wide business continuity planning. Because business continuity is important for both business processes as well as technology operations, business continuity planning should be approached on an enterprise-wide basis. Business continuity planners should assess the ability for all lines of business to remain resilient or recover from disruptions or degradations. The business continuity function often resides in the risk management organizational structure. A specific member of management should be assigned responsibility for the oversight of the business continuity function, and both business and technology departments should assign personnel to develop and maintain the individual business unit plans. Refer to the *IT Handbook's* "Business Continuity Planning" booklet for more information.

I.B.5 Information Systems Reporting

A variety of systems can provide management with the information necessary to manage an institution effectively. These systems are often referred to as management information systems, decision support systems, and risk control self-assessments, to name just a few. While the precise definitions vary, these information systems are used by management to assess the performance of the business, report on the risks and challenges it faces, and assist management in the successful operation of the business.

Management should design its information systems to do the following:

- Provide management with information that is timely, accurate, consistent, complete, and relevant.
- Provide an objective system for recording and aggregating information.
- Provide key risk performance trends and indicators; and measure performance against risk tolerances.
- Support the institution's strategic plan.
- Ensure the confidentiality, integrity, and availability of data.
- Reduce labor-intensive manual activities.
- Enhance communication among staff.

Information systems reporting supplies decision makers with facts, supports and enhances the overall decision-making process, and can improve job performance throughout an institution. At the most senior levels, information systems reporting provides the data and information to help

the board and management make strategic decisions. At other levels, information systems reporting allows management to monitor the institution's activities and distribute information to staff, customers, and members of management.

Advances in technology have increased the volume of data and information available to management and directors for planning and decision making. Because report generation systems can rely on manual data entry or extract data from many different financial and transaction systems, management should establish appropriate control procedures to ensure that data and information are correct and relevant. Because information systems reporting can originate from multiple technology platforms, the controls should be designed to maintain the integrity of the information and the processing environment.

To function effectively as a feedback tool for management and staff, information systems reporting should meet five essential elements:

- **Timeliness:** To facilitate prompt decision making, an institution's information systems should be capable of providing and distributing current information to appropriate management or staff.
- **Accuracy:** A sound system of automated and manual internal controls should exist to ensure the validity of the information and should include appropriate editing, balancing, and internal control checks.
- **Consistency:** To be reliable, data should be processed and compiled in a uniform manner. Variations in data collection and reporting methods can distort information and trend analysis.
- **Completeness:** Reports should contain the necessary information to inform decision makers without voluminous detail.
- **Relevance:** Information systems should provide current, applicable, and actionable information.

In a complex institution, information systems reporting can be highly structured and automated. In a less complex institution, it can be informal and less dependent on sophisticated technology systems. Institution management should adopt information systems reporting capabilities commensurate with the size and complexity of the institution.

I.B.6 Planning IT Operations and Investment

Action Summary

Financial institution boards should oversee, while senior management should implement, an IT planning process with the following elements:

- Long-term goals and the allocation of IT resources to achieve them, usually within a three- to five-year horizon.
- Alignment of the IT strategic plan with the enterprise-wide business plan.
- Identification and measurement of risk before changes or new investment in technology are made.
- An IT infrastructure to support current and planned business operations.
- Integration of IT spending into the budgeting process and weighing of direct and indirect benefits against the total cost of ownership of the technology.

Planning involves preparing for future activities by defining goals and the strategies used to achieve them. Future activities may include releasing a new product or service, planning mergers and acquisitions, or preparing for the end of service for an IT system. IT is an integral part of financial institution operations. Therefore, institution management should integrate consideration of IT resources and investments into the overall business planning process. Major investments in IT resources have long-term implications on both the delivery and performance of an institution's products and services.

Plans may vary significantly depending on institutions' size and structure. Management should strive to achieve a planning process that constantly adjusts for new risks or opportunities and maximizes IT's value. Management should document its plan; a written plan, however, does not guarantee an effective planning process. Management should measure the effectiveness of a specific plan by whether the plan meets the institution's business needs. A sound plan should involve the board of directors, senior management, and staff in the planning process. The board of directors should provide a credible challenge to management when the board reviews and approves the plan. Senior management participates in formulating and implementing the plan. The individual departments and functional areas identify specific business needs and, ultimately, implement the plan.

An institution that uses third-party providers should verify that the provider can continue to support the institution's plans and that the plans and actions of the provider do not negatively impact the institution. As part of the institution's ongoing monitoring process, management should participate in third-party provider client user groups. Institution management should also consider a review of client portals, news articles, provider newsletters, and press releases to maintain awareness of provider activities, changes in strategy and products, future plans, and potential or actual service or security issues.

I.B.6(a) *Strategic IT Planning*

Strategic IT planning should address long-term goals and the allocation of IT resources to achieve them. Strategic IT planning focuses on a three- to five-year horizon and helps ensure that the institution's technology plans are consistent and aligned with the institution's business plan. Effective strategic IT planning can ensure delivery of IT services that balance cost and efficiency, while enabling the business units to meet the competitive demands of the marketplace. The IT strategic plan should address the budget, periodic board reporting, and the status of risk management controls.

Tactical plans support the larger IT strategic plan by defining specific steps necessary to fulfill it. Tactical plans outline specific steps, personnel, tools, and timetables to achieve the goals laid out in the IT strategic plan, typically using a one-year time frame. These tactical plans typically address hardware and software architecture, end-user computing resources, and processing done by third-party providers. These plans are often created by mid-level managers.

The operational IT plan is used to achieve the goals and objectives of both the tactical plans and the larger strategic plan. It provides the detailed information to perform the tasks needed to implement the tactical plans of an institution. The operational IT plan includes the milestones and tasks that must be undertaken, the individuals who have responsibility for each milestone and task, the timelines in which they must be completed, the conditions for success, and the financial resources necessary to complete each milestone and task. Operational plans should flow logically from both the tactical plans and the larger IT strategic plan. Front-line management typically creates and revises operational plans as needed based on changes in the underlying business needs.

Strategic IT planning should consider a number of factors:

- Marketplace conditions.
- Customer demographics.
- Institution growth targets.
- Mergers and acquisitions.
- Technology standards.
- Regulatory requirements (e.g., privacy, security, consumer disclosures, and other reporting requirements).
- Cost containment.
- Process improvement and efficiency gains.
- Customer service and technology performance quality.
- Third-party relationship opportunities versus in-house expertise.
- Optimal infrastructure, including systems and software replacement.
- Ability to adopt and integrate new technology.

These factors should align with the institution's business plans. Well-implemented IT plans enable the institution to deliver business value in terms of market share, earnings, and capital growth. If used, the IT steering committee's cross-functional membership makes the committee well-suited for balancing or aligning the institution's IT investment with its strategic objectives.

Typically, institutions that align IT with changing business goals and objectives have more effective operations.

Technology expenditures should be commensurate with the financial condition of the institution. They should also be appropriate to meet the changing IT strategy, provide enterprise-wide value, support necessary growth, ensure appropriate security and business resilience, and mitigate technology incompatibilities. For example, delaying investments and spending too conservatively on infrastructure or new products may lead to ineffective operations and service levels. Without a full understanding of the available technology, the institution is not able to update processes and products or achieve productivity gains or increased revenues. To create the appropriate balance, institutions should link strategic and operational plans between IT and the business units.

Management should address the following four key factors of IT planning:

- **Senior management participation:** Senior management should understand and support the IT strategic plan and established priorities.
- **Role of IT:** Management should clarify the role of IT and determine whether the current IT planning process enables personnel to work toward achieving enterprise-wide goals and objectives.
- **Impact of IT infrastructure:** Management or the IT steering committee should understand the relationship between the IT infrastructure and applications and the business strategic and operating plans. The IT infrastructure should directly support the goals and objectives of these plans.
- **Accurate scorecard on past performance:** Management or the IT steering committee should monitor past IT projects and initiatives after implementation to determine whether the institution realized the anticipated costs and benefits. The scorecard should be based on a set of objective measures.

Management should also create and maintain an alignment between IT and enterprise-wide strategies by performing the following:

- Reviewing whether IT strategic plans are aligned with the business strategy.
- Reviewing whether IT performance supports the planned strategy.
- Ensuring that the IT department is delivering on time, within budget, and to specification.
- Balancing investments between systems that support current operations and systems that transform operations and enable business units to grow and compete in new areas.
- Focusing IT resource decisions on specific business objectives, such as entry into new markets, enhanced competitive position, revenue growth, improved customer satisfaction, or customer retention.

I.B.6(b) *IT Resources*

Management should provide IT resources that are adequate to meet the current operational needs of the institution. Operational planning should consider the impact of any changes on critical business processes. Business processes are the integration of people, technology, and procedures

used to accomplish a task or complete a transaction. Changes in business processes should be coordinated and aligned with available IT resources. IT resources include the following elements:

- **Infrastructure:** Power, telecommunications capacity, network architecture, and facilities.
- **Hardware:** Mainframes, network servers, personal computers, communications networks, mobile devices, storage devices, and peripherals.
- **Operating software:** Operating systems, compilers, and utilities designed to enable the equipment and applications software to function effectively, both internally and externally.
- **Application software:** Programs designed to permit application users to perform a specific task or function. Application software runs on top of operating system software.
- **Personnel:** Staff and training programs.

Management should consider sufficient capacity for current and future needs for each of these elements.

I.B.6(c) *Budgeting*

Budgeting is another step in the operational planning process. The board should assess management's plans and its success in defining and meeting budgetary goals as one means of evaluating management's performance. The budget is a coordinated financial plan used to estimate and control the institution's activities. By assessing future economic developments and conditions, management creates an action plan and records changes in the balance sheet accounts and profitability (predicated on implementation of the plan). The budget not only projects expected results, but also serves as an important check on management.

When considering new IT projects, management should look at the entry costs of the technology and the post-implementation support costs. Increasingly, institutions are demanding, and third-party providers are providing, information regarding the total cost of ownership (TCO) beyond initial entry costs. IT projects often have undocumented costs, including the resources required to configure, maintain, repair, support, upgrade, and manage the technology over its lifetime. Readily available TCO models, as well as historical data, provide management with tools to incorporate such costs into the selection and budgeting process.

Some institutions budget IT as a separate department. A financial analysis of an IT department should include a comparison of the cost-effectiveness of the in-house operation versus contracting with a third-party provider. The analysis may also include a peer group comparison of operating costs and ratios. Depending on its size and complexity, the institution may allocate costs to the institution's lines of business. When cost allocation is used, management should ensure equitable assignment of the costs to each line of business. Equitable assignment of the costs is often accomplished by use of a chargeback system that records usage of resources based on a performance metric such as central processing unit cycles.

In some instances, a separate subsidiary of the holding company manages the IT function. An IT subsidiary can provide essential services at costs below those of third-party providers or individual institutions. Some relationships, however, may not result in a cost savings. Any

transaction between the institution and its affiliates must comply with applicable laws and regulations.[13] Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

I.B.7 Other Functions

Action Summary

The IT function at a financial institution is influenced by several other functions, which should include the following:

- The human resources function should hire and maintain competent and motivated IT staff.
- The IT audit function should validate appropriate controls to mitigate IT risk.
- The compliance function should validate that systems and applications adhere to applicable laws and regulations.

I.B.7(a) *Human Resources*

Human resources (HR) supports the IT function's ability to hire and maintain a competent and motivated staff. IT management should integrate its management of HR with IT planning to ensure optimum development and availability of IT skills.

Components of an effective IT HR management process include compensation planning, performance reviews, knowledge transfer mechanisms (e.g., rotational assignments), training, and mentoring. The board should actively and effectively provide oversight of incentive compensation programs for IT management to ensure that the programs appropriately balance risk and reward and are compatible with effective controls and risk management.

An institution should have programs in place to ensure that staff members have the expertise necessary to perform their jobs and achieve company goals and objectives. The institution may need to look externally to find necessary expertise for specialized areas.

[13] Sections 23A and 23B of the Federal Reserve Act, codified at 12 USC 371c and 12 USC 371c-1, govern transactions between certain financial institutions, such as Federal Reserve member banks, national banks, and federal savings associations, and the institutions' affiliates. Specifically, section 23B(a) states that an institution and its subsidiaries may engage in certain transactions with an affiliate, including the payment of money or the furnishing of services to an affiliate under contract, lease, or otherwise. The transactions must be on terms and under circumstances, including credit standards, that are substantially the same, or at least as favorable to such institution, as those prevailing at the time for comparable transactions with or involving other nonaffiliated companies. In the absence of comparable transactions, the statute requires that such transactions be on terms and under circumstances, including credit standards, that in good faith would be offered to, or would apply to, nonaffiliated companies. See 12 USC 371c-1(a).

Management should develop training programs for new technology and products before their deployment in the institution. The institution may use its own certification program or encourage employees to obtain an external certification to ensure that the staff maintains the necessary expertise to support the business.

The board and senior management should consider appropriate succession and transition strategies for key managers and staff members. Some strategies include the use of employment contracts, professional development plans, and contingency plans for interim staffing of key management positions. Management should have backup staff for key positions and should cross-train additional personnel. The objective is to provide for a smooth transition in the event of turnover in vital IT management or IT operations.

I.B.7(b) *IT Audit*

The audit department should send IT audit reports to appropriate management and directly to the board of directors or a designated board committee. The board of directors is responsible for overseeing the IT auditors' performance and compensation, including whether the IT auditors have the necessary expertise and the audit coverage is adequate, timely, and independent. Depending on the institution's size and complexity, the board of directors may completely outsource the IT audit function. In those cases, the outsourced auditor should be engaged by the board or audit committee.

IT auditors should validate that IT controls are designed appropriately to mitigate risk and are operating as management intended. IT audit should be completely independent, should have no role in designing or implementing controls, and should not have primary responsibility for enforcing policy. Management should have processes in place to monitor and enforce policy compliance. IT audit should verify that those processes function effectively and report the results to the board.

Senior management should ensure cooperation between business unit management and IT audit. Management should also ensure timely and accurate response to audit concerns and exceptions and ensure appropriate and timely corrective action.

Refer to the *IT Handbook's* "Audit" booklet for more information.

I.B.7(c) *Compliance*

Senior management should ensure that compliance staff reviews new products, systems, applications, or changes to ensure compliance with applicable laws and regulations. New implementations or changes can cause noncompliance through, for example, inaccurate interest rate calculations, inadequate or inaccurate disclosures, weak security controls over the creation, storage, or transmission of customer information, or poor customer verification procedures.

II Risk Management

Financial institution management should understand and evaluate risk across the institution, including the definitions and categories of risk. Risk is the potential that events, expected or unanticipated, may have an adverse effect on a financial institution's earnings, capital, or reputation. For regulatory purposes, risk is categorized as operational, liquidity, interest rate, credit, price, reputation, strategic, and compliance (legal). Although financial institution management should be aware of all potential risks as part of its overall risk management program, operational risk is the primary risk associated with IT.

II.A Operational Risk

Operational risk is the risk of failure or loss resulting from inadequate or failed processes, people, or systems. Operational risks from IT are present not only in back-office operations and transaction processing but also in areas such as customer service, systems development and support, internal controls and processes, and capacity planning. Operational risk may cross all lines of business and can be caused by internal or external events. Operational risk from IT primarily affects reputation, strategic, and compliance risks, although other risks may be affected.

Management should be aware of the implications of operational risk from IT, including the following:

- Strategic risk can stem from inaccurate information or analysis that causes management to make poor IT strategic decisions.
- Compliance risk can result from an institution's inability to meet the regulatory and legal requirements associated with its products and services. Compliance risk can also result from an institution's dependence on products and services to meet its operations and reporting requirements.
- Reputation risk can stem from errors, delays, omissions, unauthorized access to IT systems, or loss of confidential information that become public knowledge. Such occurrences may directly affect business partners and customers and may result in a loss of customers, customer withdrawal of funds, and loss of trust in the institution's products or services.

Management should have a comprehensive view of operations and business processes that are supported by technology. IT management should maintain an active role in institution strategic planning to align IT with established business goals and strategies. Additionally, management should ensure that effective IT controls exist throughout the institution, either through direct oversight or by holding lines of business accountable for IT-related controls. From a control standpoint, management should participate in the ITRM process to identify and measure risk from the use of IT, support decisions on how to mitigate the risks, implement the mitigation decisions, and monitor and report on the resulting outcomes.

III IT Risk Management

Action Summary

Financial institution management should develop an effective ITRM process that supports the broader risk management process. As part of the ITRM process, management should perform the following:

- Identify risks to information and technology assets within the financial institution or controlled by third-party providers.
- Measure the level of risk.
- Mitigate the risks to an acceptable residual risk level in conformance with the board's risk appetite.
- Monitor changing risk levels and report the results of the process to the board and senior management.

The ITRM process supports the enterprise-wide risk management framework through four activities: (1) risk identification, (2) risk measurement, (3) risk mitigation, and (4) risk monitoring and reporting. Risk identification generally documents inventories of systems and information necessary to financial institution operations and defines the potential threats to the institution's systems and operations. Risk measurement is a process of determining the likelihood of an adverse event or threat occurring and the potential impact of such an event on the institution. Risk mitigation includes the implementation of appropriate controls to reduce the potential for risk and bring the level of risk in line with the board's risk appetite. Monitoring and reporting provide the board and senior management with regular updates demonstrating the effectiveness of the risk management process.

Management should identify, measure, mitigate, monitor, and report IT risks that threaten the safety and soundness of an institution. An effective ITRM process is regularly updated and aligns IT and business objectives. This process should have a higher level of formality in more complex institutions.

The ITRM process is not complete without consideration of the overall IT environment. Management may need to consider risks associated with IT environments from two different perspectives:

- A centralized IT environment supports lines of business across shared infrastructure.
- A decentralized IT environment supports lines of business with separately managed infrastructure.

The following sections detail the processes involved in each of the ITRM activities.

III.A Risk Identification

Action Summary

Financial institution management should maintain a risk identification process that is coordinated and consistent throughout the institution. Risk identification includes ongoing data collection from existing activities and new initiatives.

All activities within a financial institution present a degree of risk. The nature of such risk, before applying controls and other mitigations, is called inherent risk. Senior management should ensure that IT risk identification efforts at the enterprise-wide level are coordinated and consistent throughout the institution. Management should maintain inventories of assets (e.g., hardware, software, and information), event classes (e.g., natural disaster, cyber, and insider abuse or compromise), threats (e.g., theft, malware, and social engineering), and existing controls as an important part of effective risk identification. Inventories should include systems and information hosted or maintained externally. Comprehensive IT risk identification should include identification of cybersecurity risks as well as details gathered during information security risk assessments required under guidelines implementing the GLBA.[14] Participation in an information-sharing forum, such as FS–ISAC,[15] should be a component of the risk identification process because sharing information may help the institution identify and evaluate relevant cybersecurity threats and vulnerabilities.[16]

Senior management should make risk management decisions based on a full understanding of identified risks. Small institutions with less complex systems may have a more simplified risk identification process. Regardless of the complexity, the process should be formal and adapt to changes in the IT environment. The effectiveness of the risk identification process is demonstrated by management's understanding and awareness of risk, the adequacy of formal risk assessments, and the effectiveness of the risk mitigation, including policies and internal controls.

III.A.1 Ongoing Data Collection

Understanding an institution's environment is the first step in any risk identification process. In identifying risks, management should collect and compile the following information regarding the institution's IT environment:

[14] Refer to the "Information Security" booklet of the *IT Handbook* for more information on the GLBA and the "Interagency Guidelines Establishing Information Security Standards."

[15] Refer to "FFIEC Releases Cybersecurity Assessment Observations, Recommends Participation in Financial Services Information Sharing and Analysis Center," November 3, 2014.

[16] Ibid.

- **IT systems inventories:** These are critical to understanding the institution's IT infrastructure, as well as identifying the access and storage points for confidential customer and institution information.
- **IT strategic plan:** Such a plan can provide insight into the institution's planning process. Review and analysis of the strategic plan as part of the risk identification process may highlight developing risk exposures or other deficiencies that limit the institution's ability to implement strategic priorities.
- **Interconnectivity:**[17] Management should comprehensively identify connections with third-party providers, including other financial institutions and financial institution intermediaries, because of the potential for significant operational risk through these interdependencies. In addition, management should identify all access points and connection types that pose risk, such as local or wide area network (LAN/WAN) connections to other networks or Internet service providers, cloud services, Wi-Fi, and cellular connections.
- **Information flow:** Management should document the flows of information throughout the institution, including flows of sensitive customer information. This documentation is critical to understanding what information assets the institution owns, where they are stored and transmitted, and who has access to them.
- **Business continuity and disaster recovery plans:** These plans prioritize the availability of various lines of business and often encompass restoration and provision of control and customer service and support. These plans can offer insight into the institution's critical operations and control environment.
- **Third-party management program:** Due diligence and monitoring present valuable information on the third-party provider's control environment. This information is necessary to identify the risks in an institution's IT environment.
- **Call center:** Issue tracking reports can often indicate potential performance or control issues if the problem reports are aggregated and analyzed for repetitive or common issues.
- **Self-assessments:** Assessments specifically on IT-related controls can provide early identification of policy noncompliance or weaknesses in controls.
- **IT audit findings:** These findings provide insight into the effectiveness of internal controls and staff and management's commitment to policy compliance.
- **Threat intelligence information:** By working with industry forums and groups, institutions can obtain information about emerging threats and the ways other organizations manage those threats.

In the process of collecting and compiling this information, management should include the potential cybersecurity risks associated with these areas of the financial institution's IT environment.

[17] This term refers to the connections between networks that are owned and operated by different entities.

III.B Risk Measurement

Action Summary

Financial institution management should develop risk measurement processes that include the following elements:

- Measuring risk using qualitative, quantitative, or a hybrid of methods.
- Recognizing that risks do not exist in isolation.
- Prioritizing the risks based on the results of risk measurement.

Risk measurement typically is performed according to policies governing the enterprise-wide risk management process. Measurement is helpful in estimating the likelihood of an adverse event and its potential impact across the institution. Measurement across the financial institution is particularly important when an event impacts shared services and infrastructure or a shared customer base.

Measurements may be qualitative, quantitative, or a hybrid of both. Qualitative measures rely on experience, judgment, and intuition and are subject to potential flaws due to bias and other factors. Types of qualitative assessments include questionnaires or surveys to measure risk. Quantitative measures, on the other hand, are based on numerical values, such as dollar amounts or number of systems out of compliance. Quantitative measurement methods may include top-down and all-encompassing measures as well as measures that are limited to discrete activities and management choices. Hybrid measurements are frequently used and typically combine qualitative and quantitative measures to provide a more comprehensive analytical approach. A hybrid assessment could include a survey of staff to gain individual insight combined with numerical data inputs. Important considerations when evaluating hybrid measures include those presented above for both qualitative and quantitative measures.

Regardless of the method used, management should estimate the likelihood of occurrence and severity of the impact of the identified risk. When analyzing the potential impact, management should consider financial, reputation, or other impact to the institution. Organizational impacts are highly variable and not always easy to quantify. They include such considerations as lost revenue, data recovery and reconstruction expense, costs of litigation and potential judgments, loss of market share, and increases to premiums or denials of insurance coverage.

There are a variety of techniques, including the use of applications, to measure risk. Applications to provide measurement-related information may be developed in-house, acquired, or both. IT's role in development and acquisition should be consistent with the guidance in the *IT Handbook's* "Development and Acquisition" booklet.

The following are common types of risks that often have significant impact:

- **Security breaches:** Including internal and external breaches, weak program code used to perpetrate fraud, and computer viruses.
- **System failures:** Including telecommunication failures, LAN and WAN failures, hardware and software failures, interconnectivity failures, and backup system failures.
- **External events:** Including weather-related events, earthquakes, pandemics, terrorism, cyber attacks, cut utility lines (e.g., telecommunication, water, and power), or widespread power outages.
- **Insider events:** Including intentional or unintentional acts by staff, such as carelessness, social engineering that results in inappropriate access or the installation of malware, and improper changes to transactions, systems, or databases.
- **Development and acquisition issues:** Including strategic platform or supplier risk, inappropriate definition of business requirements, incompatibility with existing systems, inadequate project management, programming errors (internal or external), change management issues, failure to integrate and/or migrate systems or applications successfully, or obsolescence of software.
- **Capacity planning issues:** Including inadequate capacity planning or inaccurate forecasts of growth.
- **Third-party provider issues:** Including deficiencies in the oversight of third-party providers in areas such as reporting, breach notification, business continuity and resilience testing, and subcontracting (fourth-party) risk management.

The institution should recognize that no risk exists in isolation; there are interdependencies among risks. This reinforces the need for an integrated approach for risk management. To ensure accurate risk measurement, management should ensure that risk assessments are updated regularly, and as changes occur, to address new technologies, products, services, and connections before deployment.

The IT department can have a specialized and unique role in the measurement and prioritization of IT-related threats, based on its expertise in the development, application, and use of IT. Institution management should use that expertise, as well as the expertise provided by others (e.g., auditors, third-party providers, and other third parties), in the risk measurement process. Once management identifies and measures the institution's IT risk, it should rank the risks and prioritize its response.

III.C Risk Mitigation

Action Summary

Financial institution management should implement effective control and risk transfer practices as part of its overall IT risk mitigation strategy. These practices should include the following:

- Establishing, implementing, and enforcing IT policies, standards, and procedures.
- Documenting policies for hiring and training personnel.
- Implementing internal controls for information security risks.
- Establishing and implementing effective cybersecurity controls.
- Developing and testing formal business continuity plans.
- Establishing and implementing a well-managed and controlled software development and acquisition function.
- Controlling, managing, and monitoring an IT operations function.
- Reviewing insurance for IT operations, including cyber insurance.
- Developing an effective third-party management program.

Risk mitigation is the process of reducing risks through the introduction of specific controls. Risk mitigation decisions are implemented through the use of controls or risk transfer. Risk transfer can be accomplished through mechanisms such as insurance. After implementing controls or transferring the risk, management should determine the level of residual risk, or the risk that cannot be fully mitigated or avoided. Both controls and risk transfer should be considered when evaluating whether a residual risk is within the financial institution's risk appetite. Risk appetite is the amount of risk a financial institution is prepared to accept when trying to achieve its objectives.

Controls are implemented in financial institution activities and may be performed either manually by staff or through automated systems. Controls can be classified by timing (preventive, detective, corrective) or nature (administrative, technical, physical). Refer to the *IT Handbook's* "Information Security" booklet for more information. The IT department generally implements controls within the institution for assets that are under the IT department's control. Non-IT-related controls implemented elsewhere in the financial institution should be coordinated with the IT department to ensure their adequacy.

Controls should be evaluated for effectiveness against identified threats or vulnerabilities. Evaluation typically is accomplished by tools that supplement and complement assurance and audit activities. Two examples of tools used are control self-assessments and scenario analysis. Control self-assessments, used internally to assess the effectiveness of ITRM processes and related controls, typically are performed by departments or lines of business periodically testing and validating their controls. Scenario analysis is a process of analyzing possible future events by considering alternative outcomes. It can be a valuable tool for gaining an overall

understanding of the exposure to existing, expected, and plausible (including potentially severe) events, as well as the robustness of—or gaps in—controls or other risk mitigation. Additionally, a control self-assessment should encompass external requirements, such as laws, regulations, and widely accepted control standards and practices.[18] Failure to comply with external requirements, whether in law, regulation, or contract, can result in compliance risk as well as strategic, reputation, or other risks. Conformance with widely accepted control standards and practices can demonstrate due care in the operation of IT and potentially reduce operational risk.

Conformance with external requirements alone is not sufficient to ensure that the overall ITRM process is adequate. The ITRM process encompasses risk posed by the operation of the financial institution in its specific internal and external environment. Accordingly, the ITRM process should consider whether the IT control structure, when combined with controls outside the IT systems, adequately mitigates risk associated with the use of IT.

III.C.1 Policies, Standards, and Procedures

In general, a policy is a governing principle that provides the basis for standards and is adopted by the board. The policy is an overall statement of the institution's philosophy or intent. Standards are mandatory criteria that ensure conformity with policy, government regulations, and acceptable levels of control. Procedures are typically documents that describe, in detail, the behavior or processes used to adhere to the criteria mandated by standards. Clearly written and frequently communicated policies can establish clear assignments of duties, help staff coordinate and perform their tasks effectively and consistently, and aid in training staff. Senior management should ensure that policies, standards, and procedures are current, well documented, and integrated with the institution's information security strategy.

Institution management should create, document, maintain, and adhere to policies, standards, and procedures to manage and control the institution's IT risk. The level of detail depends on the complexity of the IT environment but should enable management to monitor the identified risk posture. Review of adherence to documented policies, standards, and procedures may be performed internally, by a risk or compliance function in the institution, or through independent audit. This review often helps to identify problems early so they can be corrected before they become serious.

III.C.2 Personnel

The institution should mitigate risks posed by IT staff by performing appropriate background checks and screening of new staff. The controls in this section also are relevant for third-party provider staff, consultants, and temporary personnel who support the IT function. Typically, the minimum verification considerations should include the following:

[18] Examples of widely accepted industry standards include National Institute of Standards and Technology (NIST) publications, the Control Objectives for Information and Related Technology (COBIT) framework, and the Information Technology Infrastructure Library (ITIL).

- Background checks, including confirmations of prior experience, academic credentials, professional qualifications, or criminal records.[19]
- Confirmation of identity from government-issued identification.
- Character references.

The institution should use job descriptions, employment agreements (usually for higher-level or higher-sensitivity positions), training, and awareness programs to promote understanding and increase individual accountability. The job descriptions should detail duties and responsibilities and be routinely updated by managers responsible for the positions with assistance from HR. Management should document and confirm access privileges for each staff member based on his or her job description. Additionally, management should establish a timely process to review, update, and remove access privileges associated with any party when appropriate. The lack of such a process may result in unauthorized or inappropriate activity. Failure to remove access privileges when appropriate, particularly for those individuals with high levels of privilege, represents significant risk.

The institution should protect the confidentiality of information about its customers and organization by having new hires sign agreements covering confidentiality, nondisclosure, and authorized use as a condition of their employment. Employment agreements set both the expectations and limits associated with the staff member's functions. Management should obtain signed confidentiality and nondisclosure agreements before granting new staff members, contractors, and temporary staff access to IT systems. In addition, management should require periodic acknowledgement of acceptable use policies for the network, software applications, Internet, e-mail, confidential data, and social media. Information security awareness and training programs help support information security and other management policies.

III.C.3 Information Security

Financial institutions are critically dependent on their information and technology assets—hardware, software, and data. Management should protect information and technology assets to ensure operational continuity, financial viability, and the trust of customers. The unauthorized loss, destruction, or disclosure of confidential information can adversely affect a financial institution's reputation, earnings, and capital.

The board of directors is responsible for overseeing the development, implementation, management, and maintenance of the institution's information security program. This oversight includes assigning specific responsibility and accountability for the program's implementation and reviewing reports from management. The board should provide management with guidance, review the effectiveness of management's actions, and annually approval written information

[19] Section 19 of the Federal Deposit Insurance Act prohibits, without the prior written consent of the Federal Deposit Insurance Corporation (FDIC), a person convicted of any criminal offense involving dishonesty or breach of trust or money laundering (covered offenses), or who has agreed to enter into a pretrial diversion or similar program in connection with a prosecution for such offense, from becoming or continuing as an institution-affiliated party, owning or controlling, directly or indirectly an insured depository institution (insured institution), or otherwise participating, directly or indirectly, in the conduct of the affairs of the insured institution, See 12 U.S.C. 1829.

security policies and a written information security program. Key elements that should be addressed in the information security program include the following:

- Central oversight and coordination.
- Areas of responsibility.
- Risk measurement.
- Implementation of controls.
- Monitoring and testing of effectiveness of controls.
- Reporting.
- Acceptable residual risk.

The information security program should be coordinated across the institution. To ensure the effectiveness of the information security program throughout the institution, management should have a process to hold staff accountable for complying with the information security program. Institution management should perform the following:

- Develop and implement processes to identify and protect against security events and incidents.
- Develop, implement, and periodically test incident response procedures, which should address escalation, remediation, and reporting of events and incidents.
- Develop and implement a threat intelligence and collaboration process to identify and respond to information on threats and vulnerabilities.
- Consider information security risks when developing, implementing, or updating products.
- Ensure that products are developed or updated in accordance with established information security policies and procedures.
- Perform penetration tests before launching or making significant changes to critical systems, including Internet- and client-facing applications. Management should review all findings and develop processes to ensure the timely remediation of issues identified by the tests.
- Conduct initial due diligence and ongoing monitoring to fully understand the types of connections and mitigating controls in place between the financial institution and its third-party providers. In conjunction with this, management should require by contract that the third-party providers notify the institution of the use of any subcontractors or changes to subcontractor relationships.[20]
- Implement a governance process to establish, monitor, maintain, and test controls to mitigate interconnectivity risk.
- Develop a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulator based on thresholds defined by the financial institution and applicable legal requirements. Relevant thresholds could include significant financial impact, significant operational downtime, operational or system breach, or loss of critical infrastructure.

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

[20] Refer to the *FFIEC IT Handbook's* "Outsourcing Technology Services" booklet.

III.C.3(a) *Protecting Sensitive Customer Information*

The Information Security Standards require management to develop, and the board to approve, an information security program to protect the security and confidentiality of customer information. This program may be a component of the institution's overall information security program.

The institution should protect customer information from threats to security or integrity. The institution should also protect customer information from unauthorized access or use that would result in substantial harm or inconvenience to any customer. The board should also annually review a written report, prepared by management, regarding the financial institution's actions toward GLBA compliance.

III.C.3(b) *Cybersecurity*

Institutions should take a comprehensive approach to maintain the security and resilience of their IT infrastructure, including the establishment of cybersecurity controls. Although an institution is not required to have a separate cybersecurity policy or program, its information security program should identify, measure, mitigate, monitor, and report on the heightened risks associated with cybersecurity. To address cybersecurity risk, the information security program should consider the following:

- Cyber risk management and oversight.
- Threat intelligence and collaboration.
- Cybersecurity controls.
- External dependency management.
- Cyber incident management and resilience.

Additional information on these topics is available in the FFIEC Cybersecurity Assessment Tool.[21]

III.C.4 Business Continuity

The board should approve policies, while senior management should establish and implement policies, procedures, and responsibilities for the enterprise-wide business continuity program. The board should annually approve the institution's business continuity program. Management should document, maintain, and test the plans and backup systems periodically to mitigate the consequences of system interruptions, natural and other disasters, and unauthorized intrusions that could result in the loss, damage, or degradation of data, systems, or services. Management should also provide to the board on an annual basis a written report on the overall status of the business continuity program and the results of testing of the plan and backup systems. Refer to the *IT Handbook's* "Business Continuity Planning" booklet for more information.

[21] Refer to the FFIEC Cybersecurity Assessment Tool, June 2015. Use of the Cybersecurity Assessment Tool by institutions is optional.

III.C.5 Software Development and Acquisition

Management should assess and mitigate operational risks associated with the development or acquisition of software. Management should develop applicable policies that specify risk management controls for the development and acquisition of systems. Management should guide the development or acquisition of software by using a system development life cycle (SDLC) or similar methodology appropriate for the specific IT environment. The extent or use of the SDLC depends on the size and complexity of the institution and the type of development activities performed. If the institution primarily acquires software, management should verify the effective use of an SDLC by the third-party provider.

Each phase of the SDLC should have procedures that verify the maintenance and integrity of controls before the start of the next phase. When identifying the controls to be implemented in each phase, the institution should incorporate the fundamental principles of confidentiality, integrity, and availability. Audit should review the SDLC to ensure that appropriate controls are incorporated during development. Management should analyze the operational impact early in the process to identify any additional cost and support issues.

Management should test new technology, systems, and products thoroughly before deployment. Testing, which should include tests of security, validates that equipment and systems function properly and produce the desired results. As part of the testing process, management should verify whether new technology systems operate effectively with other technology components, including vendor-supplied technology. Pilot programs or prototypes can be helpful in developing new technology before management accepts the technology for use on a broad scale. Management should conduct retesting periodically to help manage risk exposure on an ongoing basis.

Institutions that outsource the development of software should have a process to review their third-party provider's control environment, reputation, and capabilities. Institutions often employ structured acquisition methodologies similar to the SDLC when acquiring significant hardware and software products.

Refer to the *IT Handbook's* "Development and Acquisition" booklet for more information.

III.C.6 IT Operations

Management should be aware of and mitigate risks associated with IT operations. The institution and its service providers may have one or more IT operations groups. The number and types vary across institutions. Common examples of IT operations are data center or computer operations, network services, distributed computing, personal or desktop computing, change management, project management, security, resource management, and contingency and resiliency planning.

Many operations functions have significant risk factors that should be addressed through effective management and control. Rapidly evolving threats require an effective monitoring and response program to ensure that vulnerability remediation occurs in a timely manner. Ongoing

business-driven changes to applications should have effective change control programs to ensure that application updates are implemented in a timely manner. The institution should have controls over systems changes, including the following:

- Testing, authorization, and approval.
- Timing of implementation.
- Post-implementation review.
- Rollback or recovery of systems when changes are unsuccessful.

Refer to the *IT Handbook's* "Operations" booklet for more information.

III.C.7 Insurance

The institution may rely on insurance policies as part of a mitigation strategy. Traditional business insurance policies include coverage for errors and omissions, commercial general liability, and directors' and officers' liability policies. Management should understand the institution's insurance needs and the limitations of insurance coverage. These policies generally exclude, or may not include, liability for all areas of IT operations and cybersecurity.

In establishing an insurance program, management should recognize its exposure to loss, the extent to which insurance is available to cover potential losses related to information assets and technology, and the cost of such insurance. The insurance program should be commensurate with the size, complexity, and risk of the institution. Management should weigh these factors to determine how much risk the institution assumes directly. In assessing the extent of that residual risk, the institution should analyze the potential effect of an uninsured loss on itself and any affiliates or parent companies. Management should consider seeking the help of insurance consultants, attorneys, and other professionals, as necessary, to fully identify and measure the risk. Management should also review a company's financial condition or credit rating when deciding on an insurance company.

Management should understand that it cannot insure against all risks. Insurance complements, but does not replace, an effective system of controls. Thus, an overall appraisal of the control environment is important in assessing the adequacy of the insurance program.

Management can insure against risks covered in standard insurance policies. Insurance that covers physical disasters often specifically excludes computer hardware and software. To the extent that policies cover physical storage media, they generally omit the extra cost of reconstructing the recorded information found on the media. Management should clearly understand what is covered and document any gaps in coverage.

Before purchasing insurance, management should assess the costs of obtaining insurance. Estimates of these costs enable management to choose the types and amounts of insurance to carry. These estimates also allow management to determine to what extent the institution may choose to self-insure against certain losses.

Insurance policies provide a variety of coverage for events that could affect an institution's IT. The policies can be adapted to a particular institution's IT environment. The evolving threat environment is contributing to increasing interest in and purchase of insurance related to cyber risks. Insurance companies can provide coverage for items including the cost of conducting an investigation into a breach, notifying customers, reputational and crisis management, business interruption, credit monitoring for affected customers, and legal costs. Management should exercise appropriate due diligence in the review of such policies, including policy exclusions to ensure the coverage aligns with management's goals.

As part of the decision to purchase insurance, management should consider the institution's size and complexity and the level and efficacy of controls in place to mitigate risk. Types of insurance may include the following:

- **IT equipment and facilities:** Damage to the information assets and technology throughout the institution. Coverage should include leased equipment if the lessee is responsible for hazard coverage.
- **Media reconstruction:** Damage to IT media, such as magnetic tape and disks, if the institution owns and is liable for the media. Insurance is available for on-premises, off-premises, or in-transit situations. Insurance should cover the actual replacement and reproduction cost of the media or, if reproduction is not possible, the value of the media. Additional considerations to determine the amount of coverage should include programming costs and backup expense.
- **Extra expense:** The extra costs of continuing operations following damage or destruction to the institution's physical location.
- **E-banking activities:** Loss or liability arising from electronic banking activities such as Internet banking, bill payment services, and mobile financial services.
- **Business interruption:** Reimbursement for monetary losses resulting from suspension of operations because of the loss, damage, or degradation of data, systems, or services.
- **Valuable papers and records:** Cost to restore or replace papers and records (not defined as media) in case of direct physical loss or damage.
- **Errors and omissions:** Protection against claims arising from negligent acts, errors, or omissions that occur in performing IT services for others. These policies can contain the following exclusions:
  - Employee dishonesty.
  - Libel, slander, or defamation of character.
  - Liability of others assumed by the insured under contract or agreement.
  - Liability of loss or damage to property of others.
  - Personal or bodily injury or sickness.
  - Liability arising out of advice from third parties on methods, procedures, and practices, etc.
  - Liability for preparation of income tax returns.
  - Loss caused intentionally by, or at the direction of, the insured.

Once management has acquired appropriate insurance coverage, it customarily establishes procedures to review and ensure the adequacy of the coverage. These procedures should include an annual program review by the board of directors.

III.C.8 Third-Party Management

Action Summary

As part of a financial institution's third-party management program, management should ensure that third-party providers effectively provide support by doing the following:

- Negotiating clear and comprehensive contracts with appropriate terms that meet the institution's requirements.
- Ensuring receipt of audited financial statements from third-party providers at least annually.
- Reviewing results of independent audits of IT controls at third-party providers.
- Monitoring the responsiveness of third-party provider's customer service, including client user group support.

Financial institutions increasingly rely on third-party providers and software vendors. Larger or more complex institutions are more likely to have institution-wide third-party management programs that encompass all of these relationships. IT departments can contract with third-party providers for several services, including data processing, software development, equipment maintenance, business continuity, data storage, Internet access, and security management. In smaller or less complex institutions with less formal third-party management programs, the procurement of third-party services should be reviewed by institution staff familiar with the operational, financial, security, and compliance requirements for such relationships. The oversight of the relationship should be performed by staff with knowledge of the services provided.

The board of directors should hold senior management responsible for ensuring appropriate oversight of third-party relationships. Technology needed to support business objectives is often a critical factor in deciding to outsource. Managing such relationships is not just a technology issue; it is an enterprise-wide governance issue. An effective third-party management program should provide the framework for management to identify, measure, mitigate, monitor, and report risks associated with the use of third-party providers. Management should develop and implement enterprise-wide policies and procedures to govern the third-party management program, including establishing objectives and strategies, selecting a provider, negotiating the contract, and monitoring the outsourced relationship.

Management should evaluate the quality of service, control environment, and financial condition of the third parties providing the institution with critical IT services. Third parties can include financial institution affiliates, other financial institutions, and third-party service providers. As

appropriate, these third parties should support the responsibilities of their financial institution clients to adhere to all applicable laws, regulations, and supervisory guidance. Financial institution management should expect third-party support at a level consistent with the criticality of the services provided to the institution. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

When financial institution management contracts with third-party providers for some or all IT services, it should ensure that controls over outsourced activities provide the institution with the same level of assurance as controls over those activities performed in-house. Management should also consider additional oversight or controls over third-party providers that operate in foreign locations. Management should have mitigation strategies that address risks related to foreign-based third-party providers, if applicable. In the event that the financial institution locates any of its own operations offshore and develops third-party relationships at those locations, specific risk mitigation plans should be considered to address related foreign-based third-party risks.

Management should address exposures from third-party risks through an effective third-party management program. Some factors that management should consider or address include the following:

- Assessing whether each third-party relationship supports the institution's overall objectives and strategic plans.
- Evaluating prospective third-party providers based on the scope and importance of the services they provide.
- Tailoring the institution's third-party management program based on an initial and ongoing risk assessment of the institution's third parties and the services they provide.

The time and resources devoted to managing third-party relationships effectively depend on several factors, such as the critical nature of outsourced processes, staff knowledge, and complexity of systems. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information. Additionally, some agencies have specific guidance on third-party relationships and managing third-party relationship risk.[22]

Refer to the *IT Handbook's* "Audit" booklet for more information on independent reviews of third-party providers and to the "Business Continuity Planning" booklet, appendix J, "Strengthening the Resilience of Outsourced Technology Services," for guidance focusing on cyber resilience.

[22] "Third Party Risk: Guidance for Managing Third Party Risk," FDIC FIL-44-2008, June 6, 2008; OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," October 30, 2013; Federal Reserve Board Supervision and Regulation Letter 13-19 "Guidance on Managing Outsourcing Risk," December 5, 2013.

III.D Monitoring and Reporting

Action Summary

Financial institution management should ensure satisfactory monitoring and reporting of IT activities and risk. These practices should include the following:

- Developing metrics to measure performance, efficiency, and compliance with policy.
- Developing benchmarks for reviewing performance.
- Establishing and reviewing service level agreements (SLA) with critical third-party providers.
- Developing, implementing, and monitoring a process to measure IT compliance with established policies, standards, and practices.
- Evaluating the effectiveness of mitigation strategies and controls.
- Implementing a quality control or quality assurance program to monitor and test systems and applications.
- Implementing timely and effective reporting processes.

Risk monitoring provides information about the effectiveness of risk mitigation activity and should address changing threat conditions in both the financial industry and in organizations that use similar technology. Risk monitoring is ongoing within the lines of business and should include reviews of metrics (e.g., threat intelligence), performance benchmarks, SLAs, and compliance with internal policies. In addition, as part of the monitoring process, institution management should review the effectiveness of controls and ensure that quality assurance and control practices are appropriately included. Management should ensure that there is clear assignment of responsibilities and accountability for both monitoring and escalation procedures. Management should also develop an IT risk reporting process that includes defined reporting channels to ensure accurate, timely, and relevant reporting to appropriate levels of management.

III.D.1 Metrics

Metrics aid management in its ability to assess the overall IT environment. The specific metrics reported, and the frequency with which they are reported, depend on the institution's IT environment. The following are common examples:

- Number of risk issues identified for IT activities (updated regularly to reflect new or mitigated issues). This may include information gathered through the threat intelligence and collaboration process.
- Number of risk acceptance issues approved by senior management. This information may be maintained in a database or other repository of the descriptions, mitigation options, and documentation of management acceptance.

- Number of current and historical events or issues (external and internal events that deviate from the control standards).
- Number of current or outstanding (i.e., unresolved) issues identified by the business unit, internal audit, external audit, or regulator.

Many tools can be used to provide management with metrics to facilitate risk monitoring, such as key risk indicators[23] and key control indicators.[24] These are indicators that correlate with changes in risk and control effectiveness. When developed and monitored correctly, metrics can direct management's attention to areas of potential problems.[25] As appropriate, certain metrics or summary reports of metrics should be provided to the board.

III.D.2 Performance Benchmarks

Management should periodically review the institution's IT functions and determine whether plans, goals, and expectations are on target. Given the cost of and business reliance on IT functions, failure to perform such monitoring could put an institution at risk. Management should establish performance benchmarks or standards for IT functions and monitor them on a regular basis. Such monitoring can provide assurance that IT functions are meeting the defined benchmarks and can identify potential problem areas. Areas to consider include mainframe and network availability, data center availability, system reruns,[26] out-of-balance conditions, response time, error rates, data entry volumes, special requests, and problem reports. Management should evaluate outsourced relationships by measuring performance against SLAs.

III.D.3 Service Level Agreements

The institution should establish formal SLAs with its IT providers, including affiliates and third-party providers. Larger or more complex institutions should consider establishing SLAs for internally provided services, for example, by another division or department of the same institution. SLAs establish mutual expectations and provide a baseline for measuring IT performance. Management can tie SLAs to incentive and penalty actions. SLAs should be comprehensive to provide the institution with a high level of comfort in setting expectations. The use of performance benchmarks and outcome-based measurements could identify potential issues with attaining expectations set in the SLAs.

III.D.4 Policy Compliance

Management should develop, implement, and monitor a process to measure IT compliance with the institution's established policies. In addition to the traditional reliance on internal and third-

[23] A key risk indicator is a measure used to indicate the level of risk associated with an activity.

[24] A key control indicator is a metric that indicates the potential for a control to fail within an organization.

[25] Refer to the "Metrics" section of the *IT Handbook's* "Information Security" booklet for more information.

[26] A system rerun is a method of correcting an error that occurs during processing. An entire job or selection of jobs may have to be rerun to correct the error.

party audit functions, the institution should perform periodic self-assessments. The scope and frequency of self-assessments depend on the scale and historical performance of the IT function. Self-assessments provide management with an understanding of whether the institution is in compliance with the policies approved by the board.

III.D.5 Effectiveness of Controls

Control testing should include the effectiveness of control design and implementation and take into account the changing nature of the threats and the enforcement of control functions. Management should monitor risk mitigation activities and controls to ensure that identified risks are appropriately mitigated. Monitoring of the effectiveness of controls should be ongoing, and departments should provide periodic progress reports to management. Ongoing monitoring ensures that the risk management process is not a one-time or annual event.

III.D.6 Quality Assurance and Quality Control

Quality assurance (QA) is a process intended to ensure that a product or service under development meets specified requirements. Management should oversee the establishment of a QA process and update future planning with the results. QA may include internal performance measures, focus groups, and customer surveys. Management should assess whether QA testing is conducted on new or updated systems before implementation. Testing should be independent of any programming function and should incorporate user acceptance testing programs. The thorough QA testing of a new system can identify vulnerabilities or poor functionality.

Quality control (QC) is a procedure intended to ensure that a product or application adheres to a defined set of quality criteria that meet the requirements of the end user. QC includes activities that can be used to identify weaknesses or vulnerabilities in work products and to avoid the resource drain and expense of repeating a task. The traditional goal of QC activities is to ensure that a product conforms to specifications and is fit to use. QC helps to determine the following about a product:

- Whether the product works.
- Whether the product does what it is designed to do.
- Whether the product is fit for use.

QA and QC reports are valuable tools for management and help document the control process for the production environment.

III.D.7 Reporting

Management should develop an IT risk reporting process that assembles and reports IT risk information in a manner that is timely, complete, transparent, and relevant to management decisions. IT management should provide periodic reports based on risk to senior management or the board as well as to necessary stakeholders. Recipients of IT risk reports should have the authority and responsibility to act on the reported information, provide a credible challenge for information contained in the reports, and be held accountable for the outcomes. The reporting

should be appropriate to the decisions the individual reviewing the report is responsible for influencing. This reporting should be defined in accordance with the institution's enterprise-wide risk management program. Additionally, reporting should trigger appropriate, timely, and reliable escalation procedures.

Appendix A: Examination Procedures

Examination Objective

Examiners should use these procedures to determine the quality and effectiveness of the institution's management of IT. Examiners should also use these procedures to measure the adequacy of the institution's ITRM process, including management awareness and participation, risk assessment, policies and procedures, reporting, ongoing monitoring, and follow-up.

These examination procedures (also known as the work program) are intended to assist examiners in determining the effectiveness of the institution's IT management process. Examiners may choose, however, to use only particular work steps of the following examination procedures based on the size, complexity, and nature of the institution's business. Examiners should use these procedures to measure the adequacy of the institution's cybersecurity risk management processes.

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

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

    a. Regulatory reports of examination.
    b. Internal and external audit reports.
    c. Internal or independent tests or reviews of controls (e.g., penetration tests, business continuity reviews, and third-party management reviews).
    d. Regulatory and audit reports on service providers.

2. Review management's response to issues raised during, or since, the last examination. Consider the following:

    a. Adequacy and timing of corrective action.
    b. Resolution of root causes rather than just specific issues.
    c. Existence of any outstanding issues.
    d. Whether management has taken positive action toward correcting exceptions reported in audit and examination reports.
    e. Independent review of resolution and reporting of resolution to the audit committee.

3. Interview management and review responses to pre-examination information requests to identify changes to the technology infrastructure or new products and services that might increase the institution's risk. Consider the following:

    a. Products or services delivered to either internal or external users.
    b. Current network diagrams and data flow diagrams, including changes to configuration or components.
    c. Hardware and software inventories.
    d. Loss or addition of key personnel.
    e. Inventories of third-party providers and software vendors.

f. Organizational charts that include reporting relationships between business units and control functions (e.g., enterprise risk management, ITRM, and internal audit).
g. Credit or operating losses primarily attributable (or thought to be attributable) to IT (e.g., system problems, inadequate controls, improperly implemented changes to systems, and fraud resulting from cybersecurity attacks, such as account takeover).
h. Changes to internal business processes.
i. Internal reorganizations.

Objective 2: Determine whether the board of directors oversees and senior management appropriately establishes an effective governance structure that includes oversight of IT activities.

1. Review the institution's governance structure to determine the oversight of IT activities and verify that it includes the following:

   a. Board sets the tone and direction for the institution's use of technology.
   b. IT risks are adequately identified, measured, and mitigated.
   c. Board approval of the information security program and other IT-related policies.
   d. Board members are familiar with IT activities.

2. Review the activities performed by the board or a committee of the board to determine the effectiveness of IT oversight. Specifically, review whether the board or a committee of the board appropriately does the following:

   a. Reviews and approves an IT strategic plan that aligns with the overall business strategy and includes an information security strategy to safeguard against ongoing and emerging threats, including cybersecurity threats.
   b. Oversees the institution's adoption of effective IT governance processes.
   c. Oversees management processes for approving third-party providers that include an assessment of financial condition and IT security posture of the third party, including on cybersecurity.
   d. Has an oversight process that includes receiving updates on major projects, IT budgets, IT priorities, and overall IT performance; and has an approval process for critical projects and activities.
   e. Reviews the adequacy and allocation of IT resources in terms of funding and personnel.
   f. Approves a policy to escalate and report significant security incidents to the board, steering committee, government agencies, and law enforcement, as appropriate.
   g. Holds management accountable for the identification, measurement, and mitigation of IT risks.
   h. Provides for independent, comprehensive, and effective audit coverage of the IT program.

3. Determine whether the board does the following:

   a. Delegates monitoring for specific IT activities, as appropriate, to a steering committee.
   b. Provides a credible challenge to management decisions.

c. Receives regular reports regarding operations.
d. Directs management to maintain an institution-wide view of technology and the business processes supported by technology.

4. Review the membership list of board, steering committee, and/or relevant management committees established to review IT activities. Determine whether board, senior management, lines of business, audit, and IT personnel are represented appropriately, and whether regular meetings are held and minutes are maintained.

5. Review the minutes of the board of directors and relevant committee meetings for evidence of board support and supervision of IT activities.

6. If the board delegates certain activities regarding the oversight of IT to a committee, review the membership, responsibilities, and activities of the committee. Specifically, determine whether the committee does the following:

   a. Maintains a charter that defines its responsibilities.
   b. Has a defined mission to assist the board in IT oversight.
   c. Has decision-making authority.
   d. Receives appropriate management information from IT, lines of business, and external sources.
   e. Coordinates and monitors IT resources.
   f. Determines whether there is adequate training, including cybersecurity training, for institution staff.
   g. Reports to the board on the status of IT activities to enable the board to make decisions.
   h. Receives reports on IT to remain informed on risk.
   i. Is responsible for effective strategic IT planning, oversight of IT performance, and aligning IT with business needs.

7. Review the board of directors and management oversight program for IT. Determine whether the board has effective oversight of IT. Determine whether the board oversees and management implements the following:

   a. Processes and procedures that meet objectives of governing IT policies.
   b. Appropriate policies for information security, including cybersecurity risk management processes, and other relevant IT policies.
   c. Policies that result in compliance with applicable regulatory requirements.
   d. Controls over risks associated with system development and acquisition.
   e. Process for business continuity planning.

8. Review IT management and determine whether management performs the following:

   a. Implements effective IT governance and IT risk management processes, including those that relate to cybersecurity.
   b. Reviews, understands, approves, and provides for at least annual reviews of ITRM processes.

c. Assesses the institution's inherent IT risks across lines of business and ensures IT risks are included in enterprise-wide risk assessments.
d. Provides regular reports to the board on IT risks, IT strategies, and IT changes.
e. Coordinates priorities between the IT department and lines of business.
f. Establishes a formal process to obtain, analyze, and respond to information on threats and vulnerabilities by developing a repeatable threat intelligence and collaboration program.
g. Ensures that hiring and training practices are governed by appropriate policies to maintain competent and trained staff.

9. Review the roles and responsibilities of all levels of management, including executive management, CIO or CTO, CISO, IT line management, and IT business unit management, to ensure that there is a clear delineation between management and oversight functions and operational duties.

10. Review the corporate and IT departmental organization charts to determine whether they show the following:

    a. IT management reports directly to senior management, with appropriate reporting directly to the board, as needed.
    b. The IT department's responsibilities are appropriately segregated from business processing activities.

11. Review the institution's structure to determine whether the board established the following:

    a. The organizational structure provides for effective IT support throughout the institution, from IT management up through senior management and the board.
    b. Defined roles and responsibilities for key IT positions, including executive management (CEO and COO, and often CIO or CTO), and CISO.
    c. An appropriate and effective executive management team or positions, such as CEO and COO, to assist in the oversight and management of IT.
    d. A defined and functioning role for the CIO or CTO to focus on strategic IT issues and the overall effectiveness of the IT function.
    e. A CISO or information security officer position responsible for the management and mitigation of information security risks.
    f. Involvement of frontline management in the IT oversight process.
    g. Integration of business line managers into the IT oversight process.

12. Determine whether the reporting structure ensures that the CISO has the appropriate authority to carry out its responsibilities and that there are no conflicts of interest in the ability of the CISO to make decisions in line with the risk appetite.

13. Determine management's need for, or effectiveness in, selecting and implementing appropriate EA and assess whether the EA program serves the institution's needs, complexity, and future technology plans.

Objective 3: As part of the ITRM structure, determine whether financial institution management has defined IT responsibilities and functions. Verify the existence of well-defined responsibilities and expectations between risk management and IT functional areas, such as information security, project management, business continuity, and information systems reporting.

1. Review the institution's established lines of authority for enforcing and monitoring controls.

2. Determine whether management has a board-approved written information security program and verify that it is maintained and updated according to regulatory requirements.

3. Determine whether the institution has a project management function appropriate for the complexity of the institution, and verify that this function contains the appropriate elements.

4. Determine whether the institution maintains an adequate and up-to-date enterprise-wide business continuity plan. Determine whether the board oversees implementation and approves policies related to business continuity planning.

5. Determine whether the institution has a well-defined role for the implementation and use of information systems reporting and that it produces accurate and useful reports. Determine the effectiveness of the reports used by senior management or relevant management committees to supervise and monitor the following IT functions:

    a. Management reports that provide the status of software development and maintenance activities.
    b. Performance and problem reports prepared by internal user groups.
    c. System use and planning reports prepared by operating managers.
    d. Internal and external audit reports of IT activities.

6. Review information systems reports for management, and determine whether they provide the information necessary to help manage the institution effectively. Determine the following:

    a. The information systems reports facilitate the management of the business.
    b. The process and results are effective.
    c. Data and information provided to the board and senior management allow them to make strategic decisions.
    d. The information systems reports provide key risk and performance trends, indicators, and performance against risk tolerances.
    e. The institution has effective controls procedures in place to ensure that information is correct and relevant.
    f. The systems and reporting meet the five elements of effective reporting: timeliness, accuracy, consistency, completeness, and relevance.
    g. The information systems reports are appropriate for the size and complexity of the institution.

Objective 4: Determine the adequacy of the institution's IT operations planning and investment. Assess the adequacy of the risk assessment and the overall alignment with the institution's business strategy, including planning for IT resources and budgeting.

1. Determine whether the board oversees and management considers the following when formulating the institution's overall business strategy:

    a. Risk assessment, priority, and mitigation across the institution.
    b. IT strategic plans.
    c. Major projects in process or planned.
    d. Third-party relationships, including the third party's current and future plans (e.g., changes in strategy and products offered) and service or security issues that may affect the institution.
    e. Staffing levels sufficient to complete tasks as scheduled.
    f. IT operating costs.
    g. IT contingency planning and business recovery.

2. Review the strategic plan for IT activities. Determine whether the goals and objectives are consistent with the institution's overall business strategy. Document significant changes made since the previous examination that affect (or any planned changes that may affect) the institution's organizational structure, hardware or software configuration, and overall operational goals. Determine the following:

    a. Business needs are realistic.
    b. IT has the ability to meet business needs.
    c. The plan addresses long-term (three- to five-year horizon) goals and allocation of resources.
    d. The plan incorporates the entire IT environment.
    e. The plan lists strategic initiatives and considers all necessary factors around those initiatives.
    f. The plan includes tactical plans to achieve strategic goals.
    g. The plan explains trends and issues of potential impact.
    h. The plan incorporates clearly defined goals and metrics.
    i. The planning process adjusts for new or changing risks.
    j. IT Management participates in the development of the IT strategic plan.
    k. There is review of and credible challenge to the plan.

3. Determine whether the institution has adequate tactical and operational IT plans to support the larger IT strategic plan.

4. Determine whether the board or board committee reviews and approves the following:

    a. Information security risk assessment, including cybersecurity.
    b. Short- and long-term IT tactical, operational, and strategic plans.
    c. Resource allocation (e.g., major hardware or software acquisition and project priorities).
    d. Reported status of major projects.

e. IT budgets and current operating cost and the allocation of IT resources.

5. Determine the effectiveness of management's process to fund IT resources to meet the current operational needs of the institution. Assess whether management considers the following IT resources:

   a. Infrastructure.
   b. Hardware.
   c. Operating software.
   d. Application software.
   e. Personnel.

6. Determine whether the board reviews management's budget plans. Determine the effectiveness of the budget process to estimate and control the institution's activities.

7. If the institution uses third-party providers, determine whether management:

   a. Verifies that the third-party providers can continue to support current contract requirements and future changes (e.g., that the third party has a satisfactory financial condition).
   b. Has a process to assess whether a third party's actions may negatively affect the institution (e.g., a review of the third-party plans to continue offering the necessary products or services contracted by the institution).
   c. Has an effective ongoing monitoring process of its third-party providers.

Objective 5: Along with the IT audit and compliance departments, the HR department can serve as an influencing function for IT. Determine the adequacy of the institution's HR function to ensure its ability to attract and retain a competent workforce.

1. Determine the institution's ability to attract and retain a competent workforce and the ability of HR management to effectively meet the requirements for IT and the lines of business that IT supports.

2. Identify key IT positions, review biographical data (e.g., résumés and training and development records), and determine the following:

   a. Job descriptions are reasonable and represent actual practice.
   b. Employees have appropriate qualifications.
   c. Staffing levels are appropriate.
   a. There are provisions for management succession that provide for an acceptable transition in the event of the loss of a key IT manager or staff member.
   b. Backup personnel are identified and trained.

3. Review and evaluate written job descriptions to ensure that management performs the following:

a. Clearly defines the authority, responsibility, and technical skills required.
b. Maintains updated job descriptions in writing.

4. Determine whether the HR function has processes for compensation planning, performance reviews, knowledge transfer mechanisms, training, and mentoring.

5. Determine whether the financial institution has a process to ensure that staff has the requisite expertise to fulfill its roles. Review the adequacy of the process.

6. Determine the adequacy of the institution's training programs. Determine whether the institution has or supports the following:

   a. Internal or external training programs.
   b. Certification programs.
   c. Training processes that support the goals and objectives of the institution.

7. Review turnover rates of IT staff and discuss staffing and retention issues with IT management, or review turnover rates of IT management and discuss with senior management. Identify root causes of any staffing or expertise shortages, including compensation plans or other retention practices.

8. If IT staff members have duties in other departments, determine the following:

   a. Management is aware of the potential conflicts such duties may cause.
   b. Conflicting duties are subject to appropriate supervision and compensating controls.

Objective 6: Evaluate management's review and oversight of IT controls, including the other influencing functions of IT audit and compliance.

1. Consult with the examiner reviewing audit or IT audit to determine the adequacy of IT audit coverage and management's responsiveness to identified weaknesses.

2. Determine whether the board provides for the necessary expertise in the audit department and that audit coverage is comprehensive, timely, and independent. Assess whether the board requires audit reporting directly to the board or a designated committee.

3. Determine whether the board, or its committee, has appropriate oversight of audit through the following:

   a. Audit risk assessment and audit plan.
   b. Audit review activities.
   c. Audit reports with identified weaknesses.
   d. Management's responses and corrective actions to audit issues.
   e. Updates on any audit concerns and the status of issues.

4. Determine whether the board, or a board committee, is responsible for overseeing performance and compensation for the audit department.

5. Determine whether the compliance function has involvement in the institution's review oversight process, and assess the adequacy of its involvement.

6. Determine whether compliance staff reviews new products, systems, applications, or changes to evaluate compliance with applicable laws and regulations.

Objective 7: Determine whether the institution's risk management program facilitates effective risk identification and measurement and provides support for risk decisions within ITRM.

1. Determine whether the institution has a risk management program and whether the program includes an integrated approach for enterprise-wide risk management, including identification, measurement, mitigation, monitoring, and reporting of risk. If applicable, determine whether the structure conforms to regulatory requirements.

2. Determine the effectiveness of the risk management program by reviewing whether it receives appropriate direction and support from the board and senior management.

3. Determine the following:

    a. The board of directors has defined its risk appetite and the institution's risk tolerance levels.
    b. The board of directors has applied sufficient resources to achieve its risk appetite and remain within the institution's risk tolerance levels.
    c. Management has committed to support the board's risk decisions.

4. Determine whether the institution maintains a risk assessment process to perform the following:

    a. Identify risks and threats from both internal and external sources.
    b. Develop or update policies within the risk management function to guide risk measurement activities.
    c. Ensure the existence of a process to promote sound understanding and analysis of threats, events, assets, and controls.
    d. Maintain processes within the risk management function to help make risk mitigation decisions.
    e. Determine the entities that should have involvement in that decision-making process.
    f. Ensure that the board and management understand the risk categories.

Objective 8: Determine whether the board of directors oversees and senior management proactively mitigates operational risk.

1. Review the institution's management of operational risk, and verify that the risk management process includes aspects of operational risk across the institution, including the following:

    a. Back-office operations and transaction processing.
    b. Customer service.
    c. Systems development and support.
    d. Internal controls and processes.
    e. Capacity planning.

2. Determine whether the institution's management of operational risk incorporates an enterprise-wide view of IT and business processes that are supported by technology.

3. Assess whether IT management maintains an active role in the institution's strategic planning to align IT with established business goals and strategies. Assess whether effective IT controls exist throughout the institution, either through direct oversight or by holding lines of business accountable for IT-related controls.

4. Determine whether IT management participates in the enterprise-wide risk management process to identify and measure risk from the use of IT, support decisions on how to mitigate the risks, implement the mitigation decisions, and monitor and report on the resulting outcomes.

Objective 9: Determine whether management implements an ITRM process that supports the overall enterprise-wide risk management process.

1. Review the role of IT management in the risk management process and identify whether it is supportive and collaborative to the overall process.

2. Determine whether the ITRM process includes the following:

    a. A risk identification process to identify risks to information assets within the institution and information assets controlled by third-party providers.
    b. A risk measurement process using an evidence-based approach to measure the level of risk and determine if it is in line with the board's risk appetite.
    c. A risk mitigation process to ensure that management mitigates the risks to an acceptable residual risk level.
    d. A risk monitoring and reporting process to monitor changing risk levels and report the results of the process to the board and senior management.

3. Determine whether the ITRM process includes the following:

    a. Is regularly updated with a frequency appropriate for the pace of change.
    b. Aligns IT and business objectives.

c. Has formality appropriate to the complexity of the institution.
d. Considers the overall IT environment, regardless of the design and management of the IT environment.

Objective 10: Determine whether the institution maintains a risk identification process that is coordinated and consistent across the enterprise.

1. Determine whether the institution has a comprehensive IT risk identification process that includes the identification of cybersecurity risks. Specifically, determine whether management performs the following:

   a. Maintains an inventory of assets, event classes, threats, and existing controls.
   b. Participates in an information sharing forum (such as FS-ISAC).
   c. Has a process to identify internal and external threats.
   d. Considers existing controls—including governance of controls, their limitations, and their effectiveness—in a comprehensive control assessment.
   e. Has a risk identification process that is formal yet flexible enough to adapt to changes in the IT environment.
   f. Incorporates a measurement and assessment of outsourced relationships in the risk identification process.
   g. Considers the information security risk assessments completed in accordance with the Information Security Standards in management oversight of IT operations.

2. Determine whether the institution's risk identification process includes the ongoing collection of information on the IT environment, including the following:

   a. IT systems inventories.
   b. IT strategic plans.
   c. Interconnectivity documentation.
   d. Information flow diagrams.
   e. Business continuity and disaster recovery plans.
   f. Third-party management program.
   g. Call center data.
   h. Department self-assessments.
   i. IT audit findings.
   j. Threat intelligence information.

Objective 11: Determine whether institution management maintains a risk measurement process that is coordinated and consistent across the enterprise.

1. Determine whether management's risk measurement process includes the determination of risk factors (such as adverse events, threats, and controls) and the affected assets. Determine whether management develops inventories of those risk factors. Specifically, determine whether management does the following in the risk measurement process:

   a. Identifies reasonable threats to financial institution assets.

b. Performs a threat analysis.
c. Estimates the probability of occurrence of adverse events.
d. Determines the potential impacts of events and threats, internal and external.
e. Analyzes the institution's technical and organizational vulnerabilities.
f. Measures risk through qualitative, quantitative, or hybrid measurement approaches.
g. Measures and assesses risks posed by third-party relationships.
h. Considers the information security risk assessments completed in accordance with the Information Security Standards in management oversight of IT operations.
i. Risk ranks information assets according to a rigorous and consistent methodology.

2. Determine whether the risk measurement process is comprehensive and includes the following types of risks that affect the institution:

   a. Security breaches.
   b. System failures.
   c. External or insider events.
   d. Development and acquisition issues.
   e. Capacity planning issues.
   f. Third-party provider issues.

3. Identify whether the institution has a proactive process in place to effectively update its measurement of risk before implementing system changes, rolling out new products or services, or confronting new external conditions.

Objective 12: Determine whether financial institution management effectively implements satisfactory risk mitigation practices.

1. Determine whether the institution has processes within enterprise-wide risk management to assist IT management in making risk mitigation decisions, and determine which entities should be involved in the decision-making process.

2. Determine whether management has adequate methods and tools, including control self-assessments and scenario analysis, to evaluate controls for effectiveness against identified threats.

3. Determine whether the ITRM process addresses risks with an effective IT control structure in the institution's IT environment and through conformance with external legal and regulatory requirements.

4. Determine whether IT management has developed adequate policies, standards, and procedures to manage the risk from technology and that they are current, documented, and appropriately communicated. Policies, standards, and procedures should address the following:

   a. Risk assessment.
   b. Personnel administration.

c. Development and acquisition, including secure development.
d. Computer operations.
e. Third-party risk management.
f. Computer and information security, including cybersecurity.
g. Business continuity and resilience planning.
h. IT audit.

5. Determine whether management has effective hiring and training practices that include the following:

   a. Performing appropriate background checks on new staff, contractors, and third-party provider personnel, as necessary.
   b. Confirming identity.
   c. Obtaining character references.
   d. Requiring periodic acknowledgement of acceptable-use policies.
   e. Obtaining signed confidentiality and nondisclosure agreements.
   f. Providing information security awareness and training programs.

6. Determine whether the board has appropriate oversight and management has appropriate responsibility for the implementation of the institution's information security program.

7. For the information security program, verify that the board is responsible for the following:

   a. Overseeing the development, implementation, and maintenance of the program.
   b. Assigning specific responsibility for its implementation.
   c. Providing management with guidance and reviewing the effectiveness of management's actions.
   d. Annually reviewing and approving a formal, written information security program.
   e. Overseeing management steps to safeguard the information assets of the bank and its customers.
   f. Annually reviewing management's report on the status of the bank's actions to achieve or maintain compliance with the Information Security Standards.

8. Determine whether, as part of the institution's information security program, the board of directors oversees and management establishes a control structure that is intended to specifically address cybersecurity risks and includes the following:

   a. Developing and implementing processes to identify, protect against, detect, respond to, and recover from security events and incidents.
   b. Developing, implementing, and periodically testing incident response procedures.
   c. Using a threat intelligence and collaboration process to identify and respond to information on threats and vulnerabilities.
   d. Including information security risks when developing, implementing, or updating products.
   e. Assigning "business owner" responsibility in product development or update processes.

f. Performing penetration tests before launching new or making significant changes to existing Internet- and client-facing applications and remediating findings from the tests.
g. Conducting initial due diligence and ongoing monitoring to fully understand the connections and mitigating controls in place between the financial institution and its third-party providers.
h. Implementing a governance process to establish, monitor, maintain, and test controls to mitigate interconnectivity risk.
i. Developing a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulators based on thresholds defined by the financial institution.

9. Determine whether the board of directors approved policies and management established and implemented policies, procedures, and responsibilities for an enterprise-wide business continuity program, including the following:

   a. Annual review and approval of the business continuity program by the board of directors.
   b. Management responsibility to document, maintain, and test the plan and backup systems periodically according to risk.
   c. Annual reports by management of the results of the business continuity and disaster recovery tests to the board of directors.

10. Determine whether management assesses and mitigates the operational risks associated with the development or acquisition of software. Appropriate management of the risks should include the following:

    a. Policies documenting risk management controls for the development and acquisition of systems.
    b. System development life cycle or similar methodology based on the complexity and type of development performed.
    c. Tests of new technology, systems, and products before deployment to validate functionality, controls, and interoperability.
    d. Penetration tests of new or updated applications, particularly for Internet- or client-facing applications, to detect and correct security flaws.

11. Review major acquisitions of hardware and software to determine if the acquisitions are within the limits approved by the board of directors.

12. Determine whether management is aware of and mitigates operational risks associated with IT operations, including the following:

    a. Data center or computer operations.
    b. Network services.
    c. Distributed computing.
    d. Desktop computing.
    e. Change management.
    f. Project management.

g. Security.
h. Resource management.
i. Contingency and resiliency planning.

13. Review the financial institution's insurance program and determine whether it is commensurate with the size, complexity, risks, and mitigation strategy of the institution. Determine the adequacy of insurance coverage (if applicable) for the following:

    a. Employee fidelity.
    b. IT equipment and facilities.
    c. Media reconstruction.
    d. Extra expenses, including backup site expenses.
    e. E-banking activities.
    f. Business interruption.
    g. Valuable papers and records.
    h. Errors and omissions.
    i. Items in transit.
    j. Other probable risks (unique or specific risks for a particular institution).

14. Review the financial institution's third-party management program to ascertain the extent and effectiveness of the oversight by the board of directors and management of risks involved in the financial institution's outsourced relationships. An effective third-party management program should incorporate the following:

    a. A framework for management to identify, measure, mitigate, and monitor the risks associated with third-party relationships.
    b. Board oversight and senior management development and implementation of enterprise-wide policies to govern the third-party management program.
    c. A review process of third-party providers to ensure that each relationship supports the institution's overall business objectives and strategic plans.
    d. Evaluation of prospective third-party providers based on the scope and criticality of services provided.
    e. Tailoring of the monitoring program based on the initial and ongoing risk assessment of the third party and the services provided.

15. As part of the examiner's review of the institution's third-party management program, analyze the third party's financial condition and note any potential weaknesses, including measures to improve those weaknesses.

16. When reviewing information provided by the institution's third-party providers, determine whether the third-party provider enables adequate financial institution client access to relevant information. Consider the following:

    a. The third party's method of communication with financial institution clients.
    b. Timeliness of third-party reporting to financial institution clients.
    c. Quality of financial information, as determined by internal or external auditor reports.

17. When reviewing information provided by the institution's third-party providers, determine the adequacy of third-party provider audit reports in terms of scope, independence, expertise, frequency, and corrective actions taken on identified issues. Work with the examiner reviewing the third-party management program to determine its adequacy.

18. When reviewing information provided by the institution's third-party providers, determine the quality of management's follow-up and resolution of customer concerns and problems with its third-party providers.

Objective 13: Determine whether IT management develops satisfactory measures for defining and monitoring metrics, performance benchmarks, service level agreements, compliance with policies, effectiveness of controls, and quality assurance and control. Determine whether management developed satisfactory reporting of ITRM activities.

1. Determine whether management develops and uses metrics to help assess the overall IT environment. Determine whether the metrics used and the frequency and monitoring of those metrics are useful to direct management's attention to emerging issues. Additionally, determine whether necessary metrics or summary reports of metrics are provided to the board.

2. Determine whether there are established performance benchmarks and standards for the IT function and whether they serve to help management identify problem areas, particularly in system or data center availability, operating conditions, response times, and error rates.

3. Review whether the institution has formal service level agreements with all of its third-party providers. Determine whether the agreements provide the institution with assurance of continued service.

4. Determine the effectiveness of management's communication and monitoring of IT policy compliance across the institution.

5. Determine whether management has an adequate method of testing the effectiveness of control design and implementation and whether management and the board appropriately monitor risk mitigation activities. Determine whether management considers all forms of controls, including governance of controls, their limitations, and their effectiveness in a comprehensive control assessment.

6. Determine whether management has QA and QC procedures defined for significant IT activities and whether those procedures are performed internally or externally. Specifically, review whether management:

    a. Has a process to assist it in determining whether products or services meet specified requirements (QA).
    b. Has procedures to ensure that a product or application adheres to a defined set of quality criteria to meet end-user requirements (QC),

c. Performs tests associated with QA and QC independent of the programming function, and whether the QA and QC procedures incorporate user acceptance testing programs.
d. Receives effective reports on the results of QA and QC testing.

7. Review the monitoring and reporting specific to the institution's ITRM activities. Specifically, determine whether the institution has developed the following:

a. A process to adequately identify and monitor relevant external threats and vulnerabilities.
b. Effective risk monitoring that provides tangible feedback on the quality of the implementation of controls and risk mitigation strategies.
c. A reporting process that assembles and reports IT risk-related information in a timely, complete, transparent, and relevant manner.
d. Appropriate escalation procedures in place depending on the content of the reporting.

Objective 14: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the examiner-in-charge (EIC) regarding:

a. Violations of laws and regulations.
b. Significant issues warranting inclusion as matters requiring attention or recommendations in the report of examination.
c. Proposed Uniform Rating System for Information Technology management component rating and the potential impact of the examiner's conclusions on composite or other component IT ratings.
d. Potential impact of the examiner's conclusions on the institution's risk assessment.

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

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

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

Appendix B: Glossary

Access: The ability to physically or logically enter or make use of an IT system or area (secured or unsecured). The process of interacting with a system.

Administrator privileges: Computer system access to resources that are unavailable to most users. Administrator privileges permit execution of actions that would otherwise be restricted.

Agility: In IT systems, the ability to rapidly incorporate new technologies or changes to technologies allowing an organization to adapt to changing business needs.

Application development: The process of designing and building code to create a computer program (software) used for a particular type of job.

Benchmark: A standard, or point of reference, against which things may be compared or assessed.

Confidentiality: Assuring that information will be kept secret, with access limited to appropriate persons.

Control self-assessment: A technique used to internally assess the effectiveness of risk management and control processes.

Corrective control: A mitigating technique designed to lessen the impact to the institution when adverse events occur.

Cyber attack: An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an institution for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cybersecurity: The process of protecting consumer and bank information by preventing, detecting, and responding to attacks.

Data center: A facility that houses an institution's most important information systems components, including computer systems, telecommunications components, and storage systems.

Detective control: A mitigating technique designed to recognize an event and alert management when events occur.

Disaster recovery: The process of recovering from major processing interruptions.

Due diligence: Technical, functional, and financial review to verify a service provider's ability to deliver the requirements specified in its proposal. The intent is to verify that the service

provider has a well-developed plan and adequate resources and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

Enterprise Architecture: The overall design and high-level plan that describes an institution's operational framework and includes the institution's mission, stakeholders, business and customers, work flow and processes, data processing, access, security, and availability.

Enterprise-wide: Across an entire organization, rather than a single business department or function.

External connections: An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

Financial Services Information Sharing and Analysis Center (FS-ISAC): A nonprofit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information.

Gramm–Leach–Bliley Act: The Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999 (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999), required the Federal banking agencies to establish information security standards for financial institutions.

Incident management: The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible.

Information security: The process by which an organization protects the creation, collection, storage, use, transmission, and disposal of information.

Information systems: Electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information systems can include networks (computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems). Other examples are backup tapes, mobile devices, and other media.

Information technology: Any services or equipment, or interconnected system(s) or subsystem(s) of equipment that comprise the institution's IT architecture or infrastructure. It can include computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources.

Infrastructure: Describes what has been implemented by IT architecture and often include support facilities such as power, cooling, ventilation, server and data redundancy and resilience, and telecommunications lines. Specific architecture types may exist for the following: enterprise, data (information), technology, security, and application.

Interconnectivity: The state or quality of being connected together. The interaction of a financial institution's internal and external systems and applications and the entities with which they are linked.

Interdependencies: Where two or more departments, processes, functions, and/or third parties affect or support one another.

Internet: A worldwide network of computer networks, governed by standards and protocols developed by the Internet Engineering Task Force (IETF).

Interoperability: The ability of a system to work with or use the parts or equipment of another system.

IT architecture: A subset of enterprise architecture, with detail to support data processing and access, including fundamental requirements for centralized or distributed computing, real or virtual servers, devices and workstations, and networking design. Architecture plans may also exist for data (information), security, and applications.

IT governance: An integral part of governance that consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

IT strategic plan: A comprehensive blueprint that guides the organization's technology management and contains high-level goals and plans for all areas of information technology that affect the business, not just the infrastructure. The plan should include areas that impact technology management, including cost management, human capital management, hardware and software management, third-party management, risk management, and all other considerations in the enterprise IT environment.

IT system inventory: A list containing information about the information resources owned or operated by an organization.

Malware: Software designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs.

Metric: A quantitative measurement.

Milestone: Major project event.

Mobile device: A portable computing and communications device with information-storage capability. Examples include notebook and laptop computers, cellular telephones and smart phones, tablets, digital cameras, and audio recording devices.

Mobile financial services: A financial institution's use of mobile devices to provide products and services to its customers.

National Institute of Standards and Technology (NIST): An agency of the U.S. Department of Commerce that works to develop and apply technology, measurements, and standards. NIST developed a voluntary cybersecurity framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructures.

Network: Two or more computer systems that are connected to share information, software, and hardware.

Operating system: A system that supports and manages software applications. Operating systems allocate system resources, provide access and security controls, maintain file systems, and manage communications between end users and hardware devices.

Operational IT plan: Typically, the plans that are made by front-line, or low-level, IT managers. Operational IT plans are focused on the specific procedures and processes that implement the larger strategic plan.

Operational risk: The risk of failure or loss resulting from inadequate or failed processes, people, or systems.

Penetration test: The process of using approved, qualified personnel to conduct real-world attacks against a system to identify and correct security weaknesses before they are discovered and exploited by others.

Preventive control: A mitigating technique designed to prevent an event from occurring.

Principle of least privilege: The security objective of granting users only the access needed to perform official duties.

Project: A task involving the acquisition, development, or maintenance of a technology product.

Project management: Planning, monitoring, and controlling an activity.

Residual risk: The amount of risk remaining after the implementation of controls.

Resilience: The ability of an institution to recover from a significant disruption and resume critical operations.

Risk: The potential that events, expected or unanticipated, may have an adverse effect on a financial institution's earnings, capital, or reputation.

Risk identification: The process of determining risks and existing safeguards. It generally includes inventories of systems and information necessary to operations and defines the potential threats to systems and operations.

Risk management: The total process required to identify, control, and minimize the impact of uncertain events. The objective of a risk management program is to reduce risk and obtain and maintain appropriate management approval at pre-defined stages in the life cycle.

Risk measurement: A process of determining the likelihood of an adverse event or threat occurring and the potential impact of such an event on the institution. The result of risk measurement is the prioritization of potential risks based on severity and likelihood of occurrence.

Risk mitigation: The process of reducing risks through the introduction of specific controls and risk transfer. It includes the implementation of appropriate controls to reduce the potential for risk and bring the level of risk in line with the board's risk appetite.

Scenario analysis: The process of analyzing possible future events by considering alternative possible outcomes.

Scorecard: A dashboard of performance measures.

Security breach: A security event that results in unauthorized access of data, applications, services, networks, or devices by bypassing underlying security mechanisms.

Security event: An event that potentially compromises the confidentiality, integrity, availability, or accountability of an information system.

Security posture: The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, and policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

Sensitive customer information: A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as user name and password or password and account number.

Service level agreement (SLA): Formal documents between an institution and its third-party provider that outline an institution's predetermined requirements for a service and establish

incentives to meet, or penalties for failure to meet, the requirements. SLAs should specify and clarify performance expectations, establish accountability, and detail remedies or consequences if performance or service quality standards are not met.

Social engineering: A general term for trying to trick people into revealing confidential information or performing certain actions.

Systems administration: The process of maintaining, configuring, and operating computer systems.

Tactical plan: Typically, a short-term plan that establishes the specific steps needed to implement a company's strategic plan.

Telecommunications: The exchange of information over significant distances by electronic means.

Third-party provider: Any type of company, including affiliated entities, nonaffiliated entities, and alliances of companies providing products and services to a financial institution. Other terms used to describe service providers include subcontractors, external service providers, application service providers, and outsourcers. Also called a third-party service provider.

Third-party relationship: Any business arrangement between a financial institution and another entity, by contract or otherwise.

Threat intelligence: The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision-making.

Total cost of ownership (TCO): The true cost of ownership of a computer or other technology system that includes: original cost of the computer and software; hardware and software upgrades; maintenance; technical support; and training.

Virus: Malicious code that replicates itself within a computer.

Vulnerability: A hardware, firmware, or software flaw that leaves an information system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to information or to disrupt critical processing.

Appendix C: References

Laws

12 USC 1464(d), Home Owners' Loan Act
12 USC 1867(c), Bank Service Company Act
12 USC 1882, Bank Protection Act
15 USC 6801 and 6805(b), Gramm–Leach–Bliley Act
18 USC 1030, Computer Fraud and Abuse Act

Federal Reserve

Regulations

12 CFR 208, appendix D-2, "Interagency Guidelines Establishing Information Security Standards"
12 CFR 211.5 and 211.24 (i), Protection of Customer and Consumer Information
12 CFR 225, appendix F, "Interagency Guidelines Establishing Information Security Standards"

Guidance

SR Letter 13-19, "Guidance on Managing Outsourcing Risk" (December 5, 2013)
SR Letter 11-9, "Interagency Supplement to Authentication in an Internet Banking Environment" (June 29, 2011)
SR Letter 05-23, "Unauthorized Access to Customer Information" (December 1, 2005)
SR Letter 05-19, "Interagency Guidance on Authentication in an Internet Banking Environment" (October 13, 2005)
SR Letter 01-15, "Standards for Safeguarding Customer Information" (May 31, 2001)
SR Letter 00-17, "Guidance on the Risk Management of Outsourced Technology Services" (November 30, 2000)
SR Letter 99-8, "Uniform Rating System for Information Technology" (March 31, 1999)
SR Letter 98-9, "Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations" (April 20, 1998)

Federal Deposit Insurance Corporation

Regulations

12 CFR 364, appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness"
12 CFR 364, appendix B, "Interagency Guidelines Establishing Information Security Standards"

Guidance

FIL-13-2015, "FFIEC Joint Statements on Destructive Malware and Compromised Credentials" (March 30, 2015)
FIL-21-2014, "Webinar on Senior Management's Role in Cybersecurity" (April 25, 2014)
FIL-11-2014, "Distributed Denial of Service Attacks" (April 2, 2014)
FIL-13-2014, "Technology Outsourcing Information Tools for Community Bankers" (April 7, 2014)
FIL-46-2012, "Supervision of Technology Service Providers and Outsourcing Technology Services" (November 6, 2012)
FIL-44-2008, "Third Party Risk: Guidance for Managing Third Party Risk" (June 6, 2008)
FIL-6-2008, "Interagency Statement on Pandemic Planning: Guidance for Minimizing a Pandemic's Potential Adverse Effect" (February 6, 2008)
FIL-52-2006, "Foreign-Based Third Party Service Providers: Guidance on Managing Risks in These Outsourcing Relationships" (June 21, 2006)
FIL-25-2006, "Influenza Pandemic: Interagency Advisory" (March 15, 2006)
FIL-121-2004, "Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance" (November 16, 2004)
FIL-103-2004, "Interagency Information Brochure on Internet Phishing Scams" (Sept 13, 2004)
FIL-43-2003, "Computer Software Patch Management" (May 29, 2003)
FIL-50-2001, "Bank Technology Bulletin on Outsourcing" (June 4, 2001)
FIL-49-99, "Required Notification for Compliance with the Bank Service Company Act" (June 3, 1999)

National Credit Union Administration

Regulations

12 CFR 721, "Federal Credit Union Incidental Powers Activities"
12 CFR 748, "Security Program, Report of Crime and Catastrophic Act, Bank Secrecy Act Compliance," and appendix A, "Guidelines for Safeguarding Member Information"
12 CFR 741, "Requirements for Insurance"
12 CFR 740, "Advertising"

Guidance

NCUA Letter to Credit Unions 02–CU–17, "E-Commerce Guide for Credit Unions" (December 2002)
NCUA Letter to Credit Unions 01–CU–20, "Due Diligence Over Third–Party Service Providers" (November 2001)
NCUA Letter to Credit Unions 00–CU–11, "Risk Management of Outsourced Technology Services (with Enclosure)" (December 2000)

Office of the Comptroller of the Currency

Regulations

12 CFR 30, appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness"
12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards"

Guidance

OCC Bulletin 2015–20, "Cybersecurity: Destructive Malware Joint Statement" (March 30, 2015)
OCC Bulletin 2015–19, "Cybersecurity: Cyber Attacks Compromising Credentials Joint Statement" (March 30, 2015)
OCC Bulletin 2015–9, "FFIEC Information Technology Examination Handbook: Strengthening the Resilience of Outsourced Technology Services, New Appendix for Business Continuity Planning Booklet" (February 6, 2015)
OCC Bulletin 2014-45, "Heightened Standards for Large Banks; Integration of 12 CFR 30 and 12 CFR 170: Final Rules and Guidelines"
OCC Bulletin 2014–53, "Cybersecurity: Cybersecurity Assessment General Observations and Statement" (November 3, 2014)
OCC Bulletin 2013–29, "Third-Party Relationships: Risk Management Guidance" (October 30, 2013)
OCC Bulletin 2006–26, "Disaster Planning: Hurricane Katrina—Lessons Learned" (June 15, 2006)
OCC Bulletin 2006–12, "Influenza Pandemic: Interagency Advisory" (March 15, 2006)
OCC Bulletin 2004–47, "FFIEC Guidance: Risk Management for the Use of Free and Open Source Software" (October 27, 2004)
OCC Bulletin 2003–14, "Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" (April 8, 2003)
OCC Bulletin 1998–3, "Technology Risk Management: Guidance for Bankers and Examiners" (February 4, 1998)

Other References

FDIC FIL-28-2015 "Cybersecurity Assessment Tool" (July 2, 2015)
SR Letter 15-9, "FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors" (July 2, 2015)
OCC Bulletin 2015-31, "FFIEC Cybersecurity Assessment Tool" (June 30, 2015)
Basel Committee on Banking Supervision, "Sound Practices for the Management and Supervision of Operational Risk" (February 2003)
ISACA Control Objectives for Enterprise IT Governance (CoBIT)