FFIEC Information Technology Examination Handbook

Information Security

SEPTEMBER 2016

Contents

INTRODUCTION 1

I GOVERNANCE OF THE INFORMATION SECURITY PROGRAM 3

I.A Security Culture 3

I.B Responsibility and Accountability 3

I.C Resources 5

II INFORMATION SECURITY PROGRAM MANAGEMENT 6

II.A Risk Identification 7

II.A.1 Threats 8

II.A.2 Vulnerabilities 8

II.A.3 Supervision of Cybersecurity Risk and Resources for Cybersecurity Preparedness 9

II.B Risk Measurement 10

II.C Risk Mitigation 11

II.C.1 Policies, Standards, and Procedures 11

II.C.2 Technology Design 12

II.C.3 Control Types 12

II.C.4 Control Implementation 13

II.C.5 Inventory and Classification of Assets 14

II.C.6 Mitigating Interconnectivity Risk 14

II.C.7 User Security Controls 15

II.C.8 Physical Security 18

II.C.9 Network Controls 19

II.C.10 Change Management Within the IT Environment 21

II.C.11 End-of-Life Management 25

II.C.12 Malware Mitigation 25

II.C.13 Control of Information 26

II.C.14 Supply Chain 29

II.C.15 Logical Security 30

II.C.16 Customer Remote Access to Financial Services 35

II.C.17 Application Security 38

II.C.18 Database Security 40

II.C.19 Encryption 40

II.C.20 Oversight of Third-Party Service Providers 42

II.C.21 Business Continuity Considerations 43
II.C.22 Log Management 44
II.D Risk Monitoring and Reporting 45
II.D.1 Metrics 45
III SECURITY OPERATIONS 46
III.A Threat Identification and Assessment 47
III.B Threat Monitoring 48
III.C Incident Identification and Assessment 49
III.D Incident Response 50
IV INFORMATION SECURITY PROGRAM EFFECTIVENESS 52
IV.A Assurance and Testing 53
IV.A.1 Key Testing Factors 53
IV.A.2 Types of Tests and Evaluations 54
IV.A.3 Independence of Tests and Audits 56
IV.A.4 Assurance Reporting 56
APPENDIX A: EXAMINATION PROCEDURES 57
APPENDIX B: GLOSSARY 75
APPENDIX C: LAWS, REGULATIONS, AND GUIDANCE 89

Introduction

This "Information Security" booklet is an integral part of the *Federal Financial Institutions Examination Council (FFIEC)*[1] *Information Technology Examination Handbook (IT Handbook)* and should be read in conjunction with the other booklets in the *IT Handbook*. This booklet provides guidance to examiners and addresses factors necessary to assess the level of security risks to a financial institution's[2] information systems.[3] It also helps examiners evaluate the adequacy of the information security program's integration into overall risk management.[4]

Information security is the process by which a financial institution protects the creation, collection, storage, use, transmission, and disposal of sensitive information, including the protection of hardware and infrastructure used to store and transmit such information. Information security promotes the commonly accepted objectives of confidentiality, integrity, and availability of information and is essential to the overall safety and soundness of an institution. Information security exists to provide protection from malicious and non-malicious actions that increase the risk of adverse effects on earnings, capital, or enterprise value. The potential adverse effects can arise from the following:

- Disclosure of information to unauthorized individuals.
- Unavailability or degradation of services.
- Misappropriation or theft of information or services.
- Modification or destruction of systems or information.
- Records that are not timely, accurate, complete, or consistent.

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

[2] The term "financial institution" includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions. The term is used interchangeably with "institution" in this booklet.

[3] Examiners should also use this booklet to evaluate the performance by third-party service providers, including technology service providers, of services on behalf of financial institutions.

[4] This booklet addresses regulatory expectations regarding the security of all information systems and information maintained by or on behalf of a financial institution, including a financial institution's own information and that of all of its customers. An institution's overall information security program must also address the specific information security requirements applicable to "customer information" set forth in the "Interagency Guidelines Establishing Information Security Standards" implementing section 501(b) of the Gramm–Leach–Bliley Act and section 216 of the Fair and Accurate Credit Transactions Act of 2003. See 12 CFR 30, appendix B (OCC); 12 CFR 208, appendix D-2 and 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA) (collectively referenced in this booklet as the "Information Security Standards").

Institutions should maintain effective information security programs commensurate with their operational complexities.[5] Information security programs should have strong board and senior management support, promote integration of security activities and controls throughout the institution's business processes, and establish clear accountability for carrying out security responsibilities. In addition, because of the frequency and severity of cyber attacks, the institution should place an increasing focus on cybersecurity controls, a key component of information security.

Institutions should also assess and refine their controls on an ongoing basis. The condition of a financial institution's controls, however, is just one indicator of its overall security posture. Other indicators include the ability of the institution's board and management to continually review the institution's security posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions. Information security is far more effective when management does the following:

- Integrates processes, people, and technology to maintain a risk profile that is in accordance with the board's risk appetite.[6]
- Aligns the information security program with the enterprise risk management program and identifies, measures, mitigates, and monitors risk.

Because risk mitigation frequently depends on institution-specific factors, this booklet describes processes and controls that an institution can use to protect information and supporting systems from various threats. Management should be able to identify and characterize the threats, assess the risks, make decisions regarding the implementation of appropriate controls, and provide appropriate monitoring and reporting.

Financial institutions may outsource some or all of their IT-related functions. Although the use of outsourcing may change the location of certain activities from financial institutions to third-party service providers, outsourcing does not change the regulatory expectations for an effective information security program. Examiners should use this booklet when evaluating a financial institution's risk management process, including the duties, obligations, and responsibilities of the third-party service provider regarding information security and the oversight exercised by the financial institution.

[5] See also Information Security Standards, section II.A, requiring each financial institution to have a comprehensive written information security program, appropriate to its size and complexity, designed to (1) ensure the security and confidentiality of "customer information"; (2) protect against any anticipated threats or hazards to the security or integrity of such information; (3) protect against unauthorized access to or use of such information that could result in a substantial harm or inconvenience to any customer; and (4) ensure the proper disposal of both "customer information" and any "consumer information."

[6] Risk appetite can be defined as the amount of risk a financial institution is prepared to accept when trying to achieve its objectives.

I Governance of the Information Security Program

Action Summary

Management should promote effective IT governance by doing the following:

- Establishing an information security culture that promotes an effective information security program and the role of all employees in protecting the institution's information and systems.
- Clearly defining and communicating information security responsibilities and accountability throughout the institution.
- Providing adequate resources to effectively support the information security program.

While IT governance is generally addressed in the *IT Handbook's* "Management" booklet, this booklet addresses specific governance topics related to information security, including the following:

- Implementation and promotion of security culture.
- Assignment of responsibilities and accountability.
- Effective funding and use of resources.

I.A Security Culture

An institution's security culture contributes to the effectiveness of the information security program. The information security program is more effective when security processes are deeply embedded in the institution's culture.

The board and management should understand and support information security and provide appropriate resources for developing, implementing, and maintaining the information security program. The result of this understanding and support is a program in which management and employees are committed to integrating the program into the institution's lines of business, support functions, and third-party management program.

The introduction of new business initiatives (such as new service offerings or applications) can reveal the maturity of and degree to which information security is part of the institution's culture. An institution with a stronger security culture generally integrates information security into new initiatives from the outset and throughout the life cycles of services and applications. Another indicator of an effective culture is whether management and employees are held accountable for complying with the institution's information security program.

I.B Responsibility and Accountability

The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions. The board should reasonably

understand the business case for information security and the business implications of information security risks; provide management with direction; approve information security plans, policies, and programs; review assessments of the information security program's effectiveness; and, when appropriate, discuss management's recommendations for corrective action. The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program.

The board, or designated board committee, should approve the institution's written information security program; affirm responsibilities for the development, implementation, and maintenance of the program; and review a report on the overall status of the program at least annually.[7]

Management should provide a report to the board at least annually[8] that describes the overall status of the program and material matters related to the program, including the following:

- Risk assessment process, including threat identification and assessment.
- Risk management and control decisions, including risk acceptance and avoidance.
- Third-party service provider arrangements.
- Results of testing.
- Security breaches or violations of law or regulation and management's responses to such incidents.
- Recommendations for updates to the information security program.

When providing reports on information security, management should include the results of management assessments and reviews; internal and external audit activity related to information security; third-party reviews of the information security program and information security measures; and other internal or external reviews designed to assess the adequacy of the information security program, processes, policies, and controls.

Management also should do the following:

- Implement the board-approved information security program.
- Establish appropriate policies, standards, and procedures to support the information security program.
- Participate in assessing the effect of security threats or incidents on the institution and its lines of business and processes.
- Delineate clear lines of responsibility and communicate accountability for information security.

[7] See also Information Security Standards, section III.A, requiring the board of directors or an appropriate committee of the board of each financial institution to approve the institution's written information security program, and oversee the development, implementation, and maintenance of the program, including assigning specific responsibility for its implementation and reviewing management reports.

[8] See also Information Security Standards, section III.F, requiring each financial institution to report to its board or an appropriate committee of the board at least annually. The report should include a description of the institution's compliance with the Information Security Standards and discuss material matters related to its information security program.

- Adhere to board-approved risk thresholds relating to information security threats or incidents, including those relating to cybersecurity.
- Oversee risk mitigation activities that support the information security program.
- Implement a risk acceptance process that identifies the risk and when, how, to what extent, and who in management has accepted the risk associated with identified vulnerabilities.
- Establish segregation of duties.
- Coordinate information and physical security.
- Integrate security controls throughout the institution.
- Require that data with similar criticality and sensitivity be protected consistently throughout the institution.
- Establish and monitor the information security responsibilities of third parties, as further described in the "Oversight of Third-Party Service Providers" section of this booklet.
- Maintain job descriptions or employment contracts that include specific information security responsibilities.
- Provide information security and awareness training and ongoing security-related communications to employees, and ensure employees complete such training annually.

Management should designate at least one information security officer responsible and accountable for implementing and monitoring the information security program. Information security management responsibilities may be distributed across various lines of business depending on where the risk decisions are made and the institution's size, complexity, culture, nature of operations, or other factors.

Information security officers should report directly to the board or senior management and have sufficient authority, stature within the organization, knowledge, background, training, and independence to perform their assigned tasks. To ensure appropriate segregation of duties, the information security officers should be independent of the IT operations staff and should not report to IT operations management. Information security officers should be responsible for responding to security events by ordering emergency actions to protect the institution and its customers from imminent loss of information; managing the negative effects on the confidentiality, integrity, availability, or value of information; and minimizing the disruption or degradation of critical services.

Internal auditors should implement a risk-based audit program to ensure management maintains and the board oversees an effective information security program. Additionally, management should issue appropriate reports to the board. Refer to the *IT Handbook's* "Audit" booklet.

I.C Resources

Funding, along with technical and managerial talent, also contributes to the effectiveness of the information security program. Management should provide, and the board should oversee, adequate funding to develop, implement, and maintain a successful information security program. The program should be staffed by sufficient personnel who have skills that are aligned with the institution's technical and managerial needs and commensurate with its size, complexity, and risk profile. Knowledge of technology standards, practices, and risk methodologies is particularly important to the success of the information security program.

When third-party service providers supplement an institution's technical and managerial capabilities, management oversight should be commensurate with the sensitivity and criticality of the information and business processes supported by the third-party service provider. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

II Information Security Program Management

Action Summary

Management should develop and implement an information security program that does the following:

- Supports the institution's IT risk management (ITRM) process by identifying threats, measuring risk, defining information security requirements, and implementing controls.
- Integrates with lines of business and support functions in which risk decisions are made.
- Integrates third-party service provider activities with the information security program.

The institution should have a robust and effective information security program that supports the institution's ITRM process.[9] An effective information security program includes the following:

- Risk identification
- Risk measurement
- Risk mitigation
- Risk monitoring and reporting

Refer to the *IT Handbook's* "Management" booklet for more information. A comprehensive information security program should incorporate cybersecurity elements, and management should identify, measure, mitigate, monitor, and report cybersecurity-related risks in accordance with the information security program and the ITRM process. In addition, to determine the overall effectiveness of the information security program, management should have comprehensive assurance and testing processes.

Management should integrate the information security program with the institution's lines of business and support functions. An integrated program provides management the ability to assess the likelihood and potential damage to the institution from an incident, identify the root cause(s) of the incident, and implement controls to address identified issues.

Institutions that outsource technology, line of business activities, and support functions should ensure integration of these activities with the information security program through an effective

[9] See also Information Security Standards, section III.B, requiring each financial institution to assess risk including through the identification of reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of "customer information" or "customer information systems," and section III.C, requiring each financial institution to manage and control its risks by (1) designing an information security program to control risks it identifies commensurate with the sensitivity of the information and the complexity and scope of the institution's activities, and (2) adopting an enumerated list of controls, as appropriate.

third-party service provider management program.[10] Effective integration of these programs is evident when the institution creates and enforces expectations that align with the internal information security program in such a way that the combined activities of the institution and its third-party service providers result in an acceptable level of risk. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

II.A Risk Identification

Action Summary

Management should develop and implement a process to identify risk.

Risk is the potential that events, expected or unanticipated, may adversely affect the institution's earnings, capital, or reputation. Risk is considered in terms of categories, one of which is operational risk. Operational risk is the risk of failure or loss resulting from inadequate or failed processes, people, or systems. Internal and external events can affect operational risk. Internal events include human errors, misconduct, and insider attacks. External events affecting IT and the institution's ability to meet its operating objectives include natural disasters, cyber attacks, changes in market conditions, new competitors, new technologies, litigation, and new laws or regulations. These events pose risks and opportunities, and the institution should factor them into the risk identification process.

To be effective, an information security program should have documented processes to identify threats and vulnerabilities continuously. Risk identification should produce groupings of threats, including significant cybersecurity threats. A taxonomy[11] for categorizing threats, sources, and vulnerabilities can help support the risk identification process. Management should perform these risk identification activities to determine the institution's information security risk profile, including cybersecurity risk.

[10] See also Information Security Standards, section III.D, requiring each financial institution to oversee service provider arrangements by (1) exercising appropriate due diligence in selecting its service providers; (2) requiring its service providers by contract to implement appropriate measures designed to ensure the security and confidentiality of the institution's "customer information"; and (3) where indicated by the institution's risk assessment, monitoring its service providers to confirm that the service providers have satisfied their contractual obligations, including by reviewing audits, summaries of test results, or other equivalent evaluations of its service providers.

[11] A taxonomy is a method for classifying items into ordered categories. Institutions use taxonomies to find relevant information from a large collection of data and to better detect or understand the patterns and trends.

II.A.1 Threats

According to the National Institute of Standards and Technology (NIST), a threat is any circumstance or event with the potential to create loss.[12] A threat can be a natural occurrence, technology or physical failure, a person with intent to harm, or a person who unintentionally causes harm. Information about threats is available from public and private sources. Public sources include the news media, blogs, government publications and announcements, and various websites. Private sources include information security vendors and information-sharing organizations.

The threat identification process is a means to collect data on potential threats that can assist management in its identification of information security risks. Threat modeling is a structured approach that enables an institution to aggregate and quantify potential threats. Institutions should consider using threat modeling to better understand the nature, frequency, and sophistication of threats; evaluate the information security risks to the institution; and apply this knowledge to the institution's information security program. As threats evolve rapidly, however, it is understood that modeling may not account for attacks that have not previously been seen, such as zero-day attacks, but could have significant impacts.

II.A.2 Vulnerabilities

A vulnerability is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source.[13] A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation. These flaws provide opportunities for hackers to gain access to a computer system, execute commands as another user, or access data contrary to specified access restrictions. Institutions can use automated vulnerability scanners to scan their computer systems for known security exposures, as well as services available from third parties, such as the Mitre Corporation's Common Vulnerability and Exposures (CVE),[14] to track vulnerabilities.

In addition to technology-based vulnerabilities, weaknesses in business operational processes can create security vulnerabilities, exposing financial institutions to unwarranted risk. These vulnerabilities can include weaknesses in security procedures, administrative controls, physical layout, or internal controls that could be exploited to gain unauthorized access to information or to disrupt critical services. For example, an institution's systems architecture may be designed based on management's assumption that manual validation of wire transfers takes place before execution, when in practice the business process does not perform that validation until after transfers have taken place.

[12] NIST SP (Special Publication) 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments," September 2012.

[13] Ibid.

[14] CVE is a dictionary of publicly known information security vulnerabilities and exposures. The Mitre Corporation maintains the system. CVE is sponsored by the U.S. Computer Emergency Readiness Team in the Office of Cybersecurity and Communications at the U.S. Department of Homeland Security.

In addition to the vulnerabilities within a financial institution's system, vulnerabilities may also arise from interdependent and interconnected systems. Financial institutions connect their systems through mergers and acquisitions and through relationships with third parties. Over time, as these systems become increasingly interdependent and complex, new vulnerabilities may be introduced. Moreover, financial institutions are dependent on a vast array of hardware and services that may result in vulnerabilities from their supply chains, including those found in hardware and software products.

Management should assess whether the institution has processes and procedures in place to identify and maintain a catalogue of relevant vulnerabilities, determine which pose a significant risk to the institution, and effectively mitigate and monitor the risks posed by those vulnerabilities. When management cannot or chooses not to mitigate a vulnerability, management should document the decision to accept the risk, the level of risk associated with the vulnerability, and the person accountable for accepting the risk. Refer to the "Security Operations" section of this booklet for more information.

II.A.3 Supervision of Cybersecurity Risk and Resources for Cybersecurity Preparedness

II.A.3(a) *Supervision of Cybersecurity Risk*

Cybersecurity is the process of protecting consumer and bank information by preventing, detecting, and responding to attacks. As part of cybersecurity, institutions should consider management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks. In light of the increasing volume and sophistication of cybersecurity threats, examiners should focus on cybersecurity preparedness in assessing the effectiveness of an institution's overall information security program.

II.A.3(b) *Resources for Cybersecurity Preparedness*

The FFIEC members issued a voluntary Cybersecurity Assessment Tool[15] to help institution boards and management identify risks to their institutions and evaluate their institution's cybersecurity preparedness. In addition, there are other resources available to help management develop and evaluate information security and cyber resilience, such as the NIST Cybersecurity Framework, common approaches developed by the Mitre Corporation, and the U.S. Computer Emergency Readiness Team's (US-CERT)[16] National Cyber Awareness System. Institution management can select a single framework or use a combination of resources to help identify its risks and determine its cybersecurity preparedness. Regardless of the source, frameworks can help management identify a cybersecurity and resilience posture that is commensurate with the institution's risk and complexity.

[15] Refer to the Cybersecurity Assessment Tool on the FFIEC website.

[16] US-CERT, of the Department of Homeland Security, responds to major incidents, analyzes threats, and exchanges critical cybersecurity information with trusted partners around the world.

II.B Risk Measurement

Action Summary

Management should develop risk measurement processes that evaluate the inherent risk to the institution.

The risk measurement process should be used to understand the institution's inherent risk and determine the risk associated with different threats. Management should use its measurement of the risks to guide its recommendations for and use of mitigating controls.

Threat analysis tools assist in understanding and supporting the measurement of information security-related risks. Such tools can include event trees,[17] attack trees,[18] kill chains,[19] and other security-related schemata.[20] These tools help management deconstruct an event into stages, better understand the event, identify the most effective and efficient means of mitigating risk, and improve the information security program. Additionally, management could use a taxonomy for security-related events to help accomplish the following:

- Map threats and vulnerabilities.
- Incorporate legal and regulatory requirements.
- Improve consistency in risk measurement.
- Highlight potential areas for mitigation.
- Select proper controls to cover various attack stages, channels, and assets.
- Allow comparisons among different threats, events, and potential mitigating controls.

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

[17] An event tree is a diagram of a chronological series of events in a system or activity that displays sequence progression, end states, and dependencies across time.

[18] An attack tree is a diagram showing how an asset, or target, might be attacked through various attack scenarios. Using an attack tree helps describe threats on computer systems and possible attacks to realize those threats.

[19] A kill chain originally was used as a military concept related to the structure of an attack. In information security, a kill chain is a method for modeling intrusions on a computer network.

[20] Security-related schemata are lists of software vulnerabilities and include the Mitre Corporation's Common Attack Pattern Enumeration and Classification, CVE, Common Weakness Enumeration, "ATT&CK Matrix," and Malware Attribute Enumeration and Characterization, and Mandiant's Open Indicators of Compromise.

II.C Risk Mitigation

Action Summary

Management should develop and implement appropriate controls to mitigate identified risks.

Once management has identified and measured the risks, it should develop and implement an appropriate plan to mitigate those risks. This plan should include an understanding of the extent and quality of the current control environment. When conducting an evaluation of the strength of controls, or the ability to mitigate risk, the institution should consider the system of controls rather than any discrete control.

Management should also obtain, analyze, and respond to information from various sources (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC]) on cyber threats and vulnerabilities that may affect the institution. Management should incorporate available information on cyber events into the institution's information security program. Additionally, management should develop, maintain, and update a repository of cybersecurity threat and vulnerability information that may be used in conducting risk assessments and provide updates to senior management and the board on cyber risk trends.

II.C.1 Policies, Standards, and Procedures

Information security policies, standards, and procedures should define the institution's control environment through a governance structure and provide descriptions of required, expected, and prohibited activities. Policies, standards, and procedures guide decisions and activities of users, developers, administrators, and managers and inform those individuals of their information security responsibilities. Policies, standards, and procedures should also specify the mechanisms through which responsibilities can be met. In addition, they should provide guidance on acquiring, designing, implementing, configuring, operating, maintaining, and auditing information systems. Policies, standards, and procedures that address the information security program should describe the roles of the information security department, lines of business, and IT organization in administering the information security program. Information security policies, standards, and procedures form the means by which the objectives of the information security program are achieved. Key attributes that contribute to the success of information security policies, standards, and procedures include the following:

- Scope that describes the expectations for appropriate actions by affected parties.
- Sufficient details to guide behavior.
- Implementation through ordinary means, such as system administration procedures and acceptable use policies.
- Enforcement through security tools and restrictions.
- Delineation of the areas of responsibility for users, developers, administrators, and managers.
- Clear and easily understandable communications to all affected parties.
- Certification that employees have read and understand the policies.

- Flexibility to address changes in the environment.
- Annual board review and approval.

II.C.2 Technology Design

While technology can introduce risk, it can also serve as a mitigation tool. Management should understand the benefits and limitations of the technology that the institution uses and whether other types of controls are necessary to compensate for those limitations.

Information security issues arise when (a) the design of the technology and the policies governing its use do not effectively defend against identified and unidentified threats, (b) threats change in ways not envisioned by the designers, and (c) the controls are not operating as intended. Management should continually assess the capability of the institution's processes, people, and technologies to sustain the appropriate level of information security based on the institution's risk profile, size, complexity, and risk appetite.

II.C.3 Control Types

Management may mitigate information security risks by implementing controls. Controls may be categorized according to timing and nature.

Table 1: Examples of Timing- and Nature-Related Controls

Timing		
Control type	**Description**	**Example**
Preventive	Controls designed to prevent incidents from occurring	Access controls to applications and systems that prevent unauthorized individuals from performing transactions
Detective	Controls designed to alert management when incidents occur	Reports that show suspicious activity
Corrective	Controls that lessen impact to the institution when adverse incidents occur	Business continuity plans
Nature		
Control type	**Description**	**Example**
Administrative	Controls that align with the board-approved risk appetite and inform employees of management's expectations	Policies or procedures that guide implementation of the information security program
Technical	Software or hardware (or both) that prevents unauthorized activity	A firewall that prevents unauthorized logical access to or from a network
Physical	Devices to prevent unauthorized physical access to a facility or computer system	A deadbolt lock on a door

It is important to have a layered control system, which deploys different controls at different points of a business process and throughout an IT system so that the strength of one control can

compensate for weaknesses in or possible failure of another control. Therefore, layered controls function in an integrated fashion to more effectively mitigate risk.

Economic and technical considerations generally affect prevention and detection or response choices in system design. Compensating controls are controls that adjust for weaknesses within the system or process. An example of compensating controls would be a review of activity logs for applications that do not allow proper segregation of duties.

II.C.4 Control Implementation

Management should implement controls that align security with the nature of the institution's operations and strategic direction. Based on the institution's risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging and monitoring, and secure software development (including third-party software development). In implementing controls, management should ensure it has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls.

The level at which controls are implemented should depend on the institution's size, complexity, and risk profile, but all institutions should implement appropriate controls. In light of increasing cybersecurity risks, management should implement risk-based controls for managing cybersecurity threats and vulnerabilities, such as interconnectivity risk. Management should review and update the security controls as necessary depending on changes to the internal and external operating environment, technologies, business processes, and other factors.

The institution can reference one or more recognized technology frameworks and industry standards. Several organizations have published control listings in addition to implementation guidance, including the following:

- **NIST 800 series of publications.** These publications provide descriptions of some management processes and technical guidance on many individual controls.
- **Control Objectives for Information and Related Technology (COBIT).** COBIT provides a broad and deep framework for governance and management of enterprise IT.
- **IT Infrastructure Library (ITIL).** ITIL provides a list of recognized practices for IT service management.
- **International Organization for Standardization (ISO)[21] 27000 series.** The ISO 27000 series provides control standards specific to information security.
- **Industry publications and sources.[22]** Management and staff may find these useful for discrete controls and processes.

[21] ISO is an independent, non-governmental, international organization that brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards.

[22] Some industry publications or organizations that provide security-related information include the ISACA Journal, SANS Institute, the Financial Services Roundtable, the Council on Cybersecurity, and the Open Web Application Security Project.

- **Vendor-provided publications, bulletin boards, and user groups.** Vendors often publish recommendations for securing their products. Additionally, some offer bulletin boards and user groups for clients to interact among themselves.

II.C.5 Inventory and Classification of Assets

Action Summary

Management should inventory and classify assets, including hardware, software, information, and connections.

Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections. Management should have policies to govern the inventory and classification of assets both at inception and throughout their life cycle, and wherever the assets are stored, transmitted, or processed. Inventories enable management and staff to identify assets and their functions. Classification enables the institution to determine the sensitivity and criticality of assets. Management should use this classification to implement controls required to safeguard the institution's physical and information assets. Additionally, management can use the inventory to discover specific vulnerabilities, such as unauthorized software.

Inventories are important for management to identify assets that require additional protection, such as those that store, transmit, or process sensitive customer information, trade secrets, or other information or assets that could be a target of cyber criminals. Knowing what information assets the institution has and where they are stored, transmitted, or processed helps management comply with federal and state laws and regulations regarding privacy and security of sensitive customer information.

After inventorying the assets, management should classify the information according to the appropriate level of protection needed. For example, systems containing sensitive customer information may require access controls based on job responsibilities. These systems should have stronger controls than systems containing information meant for the general public. Some institutions classify information as public, non-public, or institution-confidential, while others use the classifications high, moderate, and low. Additional classifications, such as critical and noncritical, may be helpful to certain types of institutions.

II.C.6 Mitigating Interconnectivity Risk

Business processes often require institutions to share information with other institutions and third-party service providers that require connectivity. The extent of interconnectivity is a function of network architecture, network complexity, traffic volume, and number of connections. Interconnectivity risk arises from misuse, mismanagement, or compromise of these connections.

To mitigate interconnectivity risk, management should do the following:

- Identify connections with third parties, including other financial institutions, financial institution intermediaries, and third-party service providers.
- Identify all access points and connection types that pose risk, such as local area network (LAN) connections to other networks or Internet service providers (ISP), Wi-Fi, and cellular connections.
- Identify connections between and access across low-risk and high-risk systems.
- Assess all connections with third parties that provide remote access capability or control over internal systems.
- Implement and assess the adequacy of controls to ensure the security of connections regardless of criticality or sensitivity.

Management should maintain network and connectivity diagrams and data flow charts to ensure adequacy of layered controls and to facilitate more timely recovery and restoration of systems when incidents occur.

II.C.7 User Security Controls

Action Summary

Management should mitigate the risks posed by users by doing the following:

- Establishing and administering security screening in IT hiring practices.
- Establishing and administering a user access program for physical and logical access.
- Employing segregation of duties.
- Obtaining agreements covering confidentiality, nondisclosure, and authorized use.
- Providing training to support awareness and policy compliance.

Users should be granted access to systems, applications, and databases based on their job responsibilities. Access rights should be granted in accordance with the institution's physical and logical access control policies. Authorized users with elevated or administrator privileges can pose a potential threat to systems and data. Employees, contractors, or third-party service providers can exploit their legitimate computer access for unauthorized purposes. Additionally, the degree of internal access granted to some users increases the risk of damage or loss of information and systems. Risk exposures from internal users include the following:

- Alteration of data.
- Deletion of production and backup data.
- Misdirected data.
- Disruption of systems.
- Destruction of systems.
- Misuse of systems for personal gain or to damage the institution.
- Appropriation of strategic or customer data for espionage or fraud schemes.
- Extortion for stolen data.
- Misuse of data following the termination or change in job responsibility of an employee.

Management should understand the risks to the institution's information-processing environment and establish appropriate user access controls to mitigate these and other potential risks to the institution's assets. Users should understand and confirm their understanding of their roles and responsibilities in maintaining a sound security environment, which includes both physical and logical areas.

II.C.7(a) *Security Screening in Hiring Practices*

Management should have a process to verify job application information for all new employees. The sensitivity of a particular job or access level may warrant additional screening and recurring background and credit checks. Management should verify that contractors are subject to similar screening procedures. In addition to initial screening, management should remain alert to changes in personal circumstances of employees and contractors that could increase incentives for system misuse or fraud.

II.C.7(b) *User Access Program*

Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements:

- Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity.
- Alignment of employee job descriptions to the user access program.
- Requirements for business and application owners to define user profiles.
- Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel.
- Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations.
- Periodic independent reviews that ensure effective administration of user access, both physical and logical.

For more information, refer to the "Physical Security" and "Logical Security" sections of this booklet.

II.C.7(c) *Segregation of Duties*

Segregation of duties, or job designs that require more than one person to complete critical or sensitive tasks, can help mitigate risk. Employees and third parties with access to sensitive resources could cause substantial damage and potential loss. System administrators, for instance, have the most powerful role in the user access process and have unlimited access to an institution's information assets and technology. Given this extensive access, management should evaluate the process for determining which individuals should be granted system administrator privileges. Such access should be appropriately monitored for unauthorized or inappropriate activity. Management should incorporate independent reviews or approvals for individuals who

perform multiple functions to minimize the potential for fraud, irregularities, and errors. Examples of segregation of duties include the following:

- Independent monitoring of the activities performed by the users with increased privileges (e.g., system administrators and super users[23]).
- Distribution of system administration activities so no administrator can hide his or her activities or control an entire system.
- Additional levels of approval as the criticality and sensitivity of decisions increase.

If an activity is conducted without appropriate segregation of duties, management should require an independent review (e.g., audit) of that activity.

II.C.7(d) *Confidentiality Agreements*

The institution should protect the confidentiality of customer and institution information. A breach in confidentiality could disclose proprietary information, increase fraud risk, damage the institution's reputation, violate customer privacy and associated rights, and violate laws or regulations. Confidentiality agreements can be used to put all parties on notice that the financial institution owns its information, expects strict confidentiality, and prohibits information sharing outside of that required for legitimate business needs. Management should obtain signed confidentiality agreements before granting employees and contractors access to IT systems.

II.C.7(e) *Training*

Training ensures personnel have the necessary knowledge and skills to perform their job functions.[24] Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Management should educate users about their security roles and responsibilities and communicate them through acceptable use policies. Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected. Management should have the ability to impose sanctions for noncompliance.

Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. The institution should collect signed acknowledgments of the employee acceptable use policy as part of the annual training program.

[23] In computing, the super user is a special user account used for system administration. Depending on the operating system, the name of this account might be root, administrator, admin, or supervisor.

[24] See also Information Security Standards, section III.C.2, requiring each financial institution to train staff to implement its information security program.

II.C.8 Physical Security

Action Summary

Management should implement appropriate preventive, detective, and corrective controls for physical security.

Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Management should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones.

A data center houses an institution's most important information system components. When selecting a site for a data center, one major objective should be to limit the risk of exposure from internal and external threats, including, where possible, environmental threats inherent to physical locations (e.g., hurricanes, earthquakes, and blizzards). The selection process should include reviewing the surrounding area to determine whether it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Guards, fences, barriers, surveillance equipment, or other devices can deter intruders. Because access to key information systems' hardware and software should be limited, appropriate physical controls should be in place. Additionally, the location should not be identified or advertised by signage or other indicators.

Detection devices, when applicable, should be used to prevent theft and safeguard the equipment. The devices should provide continuous coverage. Detection devices have two purposes—to send alarms when responses are necessary and to support subsequent forensics. Alarms are useful only when response will occur. Some detection devices include the following:

- Switches that activate alarms when electrical circuits are broken.
- Light and laser beams, ultraviolet beams, sound, or vibration detectors that are invisible to intruders, and ultrasonic or radar devices that detect movement.
- Closed-circuit television (CCTV) that provides visual observation and records intrusions.

A combination of fire suppression, smoke alarms, raised flooring, and heat and moisture sensors should address risks from environmental threats (e.g., fire, flood, and excessive heat). Environmental threat monitoring should be continuous, and responses should occur when alarms activate.

Physical security devices frequently need preventive maintenance to function properly. The institution should be able to provide maintenance logs to demonstrate that physical security devices are regularly maintained. Periodic testing provides assurance that the devices are operating correctly.

The institution should have policies governing the duties and responsibilities of security guards. Employees who access secured areas should have proper identification and authorization to enter the areas. All non-employees should provide identification to a security guard before obtaining

access. Security guards should be trained to restrict the removal of technology assets from the premises and to record the identity of anyone attempting to remove those assets. Management should implement a specific and formal authorization process for the removal of hardware and software from the premises.

Access should be restricted to the following equipment or areas:

- Operations centers (e.g., data center operations, security operations center, and network operations center) or server rooms; uninterruptible power supplies and backup generators.
- Funds transfer and automated clearinghouse routers.
- Telecommunications equipment.
- Media libraries.
- Equipment removed from the network and awaiting disposal.
- Spare or backup devices.

II.C.9 Network Controls

Action Summary

Management should secure access to computer networks through multiple layers of access controls by doing the following:

- Establishing zones (e.g., trusted and untrusted) according to the risk profile and criticality of assets contained within the zones and appropriate access requirements within and between each security zone.
- Maintaining accurate network diagrams and data flow charts.
- Implementing appropriate controls over wired and wireless networks.

Networks should be protected by a secure boundary, identifying "trusted" and "untrusted" zones. Internal zones, typically trusted, should segregate various components into distinct areas, each with the level of controls appropriate to the content and function of the assets within the zone. The institution's trusted network should be protected through appropriate configuration and patch management, privileged access controls, segregation of duties, implementation of effective security policies, and use of perimeter devices and systems to prevent and detect unauthorized access. Tools used to enforce and detect perimeter protection include routers, firewalls, intrusion detection systems (IDS) and intrusion prevention systems, proxies, gateways, jump boxes,[25] demilitarized zones, virtual private networks (VPN), virtual LANs (VLAN), log monitoring and network traffic inspecting systems, data loss prevention (DLP) systems, and access control lists.

The trusted network should be further segregated into internal layers, including production, staging, and development environments. Within those environments, management should

[25] A jump box, or jump server, provides administrators with access to or control of other servers or devices in the network. Because of this capability, additional security measures should be implemented.

consider segregating sensitive traffic, by using Voice Over Internet Protocol[26] (VOIP) and network management (such as virtualization infrastructure that carries server boot images between storage devices and hosts). Each zone should have a security policy appropriate to its use, ensuring that zone restrictions are defined by risk, sensitivity of data, user roles, and appropriate access to application systems. Access to zones should be controlled according to the principle of least privilege and segregation of duties. To ensure appropriate network security, management should maintain accurate network and data flow diagrams, and store them securely, providing access only to essential personnel. These diagrams should identify hardware, software, and network components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture.

II.C.9(a) *Wireless Network Considerations*

A wireless LAN (WLAN) is a medium of network connectivity, supported by radio wave transmissions that provides more convenient network access to employees or devices that need flexibility to connect to multiple locations within the institution's facilities. Because the user is not physically connected to the network and the wireless signal is broadcast and available to others, wireless networks are inherently less secure than wired networks and require additional scrutiny, controls, and oversight. Wireless access points are the devices that broadcast the radio wave signals and should be physically secure to prevent compromise and securely configured to provide the same level of control as a wired connection. Wireless gateways can allow management to implement more complex access controls, including advanced identity management capabilities and services to detect and remediate malicious software.

Policies should prohibit installation of wireless access points and gateways without approval and formal inclusion in the hardware inventory. Network monitoring systems should be configured to detect the addition of new devices. Alternatively, network access control (NAC) systems could prevent the recognition of any unauthorized device.[27] Management should consider limiting the WLAN signal to authorized areas, within the boundaries of the institution, if feasible. Management should use an industry-accepted level of encryption with strength commensurate with the institution's risk profile on the institution's wireless networks.

Malicious insiders and attackers may also set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities. The institution should scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices.

[26] VOIP is the transmission of voice telephone conversations using the Internet or IP networks.

[27] A NAC system typically provides an IP address only after validating that the newly connected device is authorized, by means of some identification (such as a computer's physical address—MAC address—or certificate) or pre-installed client software.

The institution may provide guests with access to a wired or wireless network. The guest network generally is used to provide access to the Internet and should be configured to prevent access to any portion of the production network.

Institutions often provide remote network connectivity for employees or third-party service providers[28] who are not located within or around the institution's facilities. This connectivity presents operational advantages, but steps should be taken to ensure that the connection is encrypted and secured. VPN connections should be used for both broadband networks and wireless air card connections to isolate and encrypt remote traffic to institution networks. IP geolocation information may not always be available when using broadband networks, which can limit the effectiveness of monitoring. Therefore, management should consider implementing compensating controls, such as restricting access to network resources.

II.C.10 Change Management Within the IT Environment

Action Summary

Management should have a process to introduce changes to the environment in a controlled manner. Changes to the IT environment include the following:

- Configuration management of IT systems and applications.
- Hardening of systems and applications.
- Use of standard builds.
- Patch management.

The IT environment consists of operating systems,[29] middleware,[30] applications, file systems, and communications protocols. The institution should have an effective process to introduce application and system changes, including hardware, software, and network devices, into the IT environment. The process for introducing software should encompass securely developing, implementing, and testing changes to both internally developed and acquired software.

Application and system control considerations for introducing changes to the IT environment before implementation should include the following:

- Developing procedures to guide the process of introducing changes to the environment.
- Clearly defining requirements for changes.
- Restricting changes to authorized users.

[28] In some cases, the institution provides remote access via VPN to a third-party service provider. Controls over third-party access should be commensurate with the sensitivity and criticality of the system and information accessed.

[29] An operating system is fundamental software that supports and manages software applications, allocates system resources, provides access and security controls, maintains file systems, and manages communications between end users and hardware devices.

[30] Middleware is software that connects two or more software components or applications.

- Reviewing the impact that changes have on security controls.
- Identifying all system components affected by the changes.
- Developing test scripts and implementation plans.
- Performing necessary tests of all changes to the environment (e.g., systems testing, integration testing, functional testing, user acceptance testing, and security testing).
- Defining rollback procedures in the event of unintended or negative consequences with the introduced changes.
- Ensuring the application or system owner has authorized changes in advance.
- Maintaining strict version control of all software updates.
- Validating that new hardware complies with institution policies.
- Ensuring network devices are properly configured and function appropriately within the environment.
- Maintaining an audit trail of all changes.

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

II.C.10(a) *Configuration Management*

Configuration management is a process to securely maintain the institution's technology by developing expected baselines for tracking, controlling, and managing systems settings. To mitigate information security risk, management should control configurations of systems, applications, and other technology. Effective configuration management relies on policies and procedures to ensure compliance with minimally acceptable system configuration requirements. When information systems change, management should update baselines; confirm security settings; and track, verify, and report configuration items. Configurations should be monitored for unauthorized changes, and misconfigurations should be identified. Management can use automated solutions to help track, manage, and identify necessary corrections.

II.C.10(b) *Hardening*

Institutions typically use commercial off-the-shelf (COTS) software for operating systems and applications, on such diverse platforms as network infrastructure, servers, desktops, laptops, and mobile devices. COTS systems generally provide more functions than are required for the specific purposes for which they are employed. A default installation of a server operating system may include mail, web, and file-sharing services on a system that does not require those functions. Unnecessary software and services represent a potential security weakness. Their presence increases the potential number of discovered and undiscovered vulnerabilities in the system. Additionally, system administrators may not install patches or monitor the unused software and services to the same degree as they would operational software and services. Protection against those risks begins when the systems are constructed and software installed through a process that is referred to as hardening a system.

Management should consult operating system and software vendor-recommended security controls. When deploying COTS applications and systems, management should harden the resulting applications and systems. Hardening can include the following actions:

- Determining the purpose of the applications and systems and documenting minimum software and hardware requirements and services to be included.
- Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure.
- Installing necessary patches.
- Installing the most secure and up-to-date versions of applications.
- Configuring privilege and access controls by first denying all, then granting back the minimum necessary to each user (i.e., enforcing the principle of least privilege).
- Configuring security settings as appropriate, enabling allowed activity, and prohibiting non-approved activities.
- Enabling logging.
- Creating cryptographic hashes[31] of key files.
- Archiving the configuration and checksums[32] in secure storage before system deployment.
- Using secure replication procedures for additional, identically configured systems and making configuration changes on a case-by-case basis.
- Changing all default passwords.
- Testing the system to ensure a secure configuration.

Additionally, the systems should be audited periodically to ensure that the hardware, software, and services are authorized and properly configured.

II.C.10(c) *Standard Builds*

Consistency in system configuration makes security easier to implement and maintain. The institution should use standard builds, which allow one documented configuration to be applied to multiple computers in a controlled manner. Some institutions, depending on their size and complexity, may have many standard builds for the different system configurations needed to address various business functions. Through standard builds, an institution simplifies the following activities:

- Creating hardware and software inventories.
- Updating and patching systems.
- Restoring systems in the event of a disaster or outage.
- Investigating anomalous activity.
- Auditing configurations for conformance with the approved configuration.

The institution may not be able to meet all of its requirements from its standard builds. The use of nonstandard builds should be documented and approved by management, with appropriate changes made to patch management and disaster recovery plans.

[31] A hash is a fixed-length cryptographic output of variables, such as a message, being operated on by a formula or cryptographic algorithm.

[32] A checksum is a simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message, which allows the receiver to verify the accuracy of the message.

II.C.10(d) *Patch Management*

Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Hackers often will attempt to exploit these known vulnerabilities to try to gain access to the institution's systems. Third parties issue patches to address vulnerabilities found on institution systems and applications.[33] Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. In addition, management should use vulnerability scanners periodically to identify vulnerabilities in a timely manner.

As part of the institution's patch management process, management should establish and implement the following:

- A monitoring process that identifies the availability of software patches.
- A process to evaluate the patches against the threat and network environment.
- A prioritization process to determine which patches to apply across classes of computers and applications.
- A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments.
- An exception process, with appropriate documentation, for patches that management decides to delay or not apply.
- A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner.
- A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied.

The institution should have procedures that include how to implement patches to mitigate risks of changing systems and address systems with unique configurations. Before applying a patch, management should back up the production system. Additionally, management should define appropriate patch windows and, whenever possible, restrict the implementation of patches to defined time frames to minimize business impact or potential down time.

Patches make direct changes to the software and configuration of each system to which they are applied. While patches are necessary and useful, they may have unintended negative consequences, such as introducing new vulnerabilities, reintroducing old vulnerabilities, or degrading system performance. The following actions can help ensure patches do not compromise the security of the institution's systems:

- Obtain the patch from a known, trusted source.
- Verify the integrity of the patch through comparisons of cryptographic hashes to ensure the patch obtained is correct and unaltered.
- Protect and monitor the systems used to distribute patches to ensure only authorized patches are distributed.

[33] If an institution develops or maintains software in-house, management should have a process to update the software with appropriate patches.

- Apply the patch to an isolated test system before installing on the production system to ensure the patch is compatible with other software used on systems, does not alter the system's security posture in unexpected ways (such as altering log settings), and corrects the pertinent vulnerability.
- Test the resulting system to validate the effectiveness of the applied patch.

II.C.11 End-of-Life Management

Management should plan for a system's life cycle, eventual end of life, and any corresponding security and business impacts. The institution's strategy should incorporate planned changes to systems, including an evaluation of the current environment to identify potential vulnerabilities, upgrade opportunities, or new defense layers. Also included in this strategy should be considerations for the support provided by third-party system vendors and the risks related to operating unsupported legacy systems. Management should have policies to manage both the hardware and software life cycles. Security risks related to reaching a system's end of life include (a) the increased potential for vulnerabilities because the third party no longer provides patches or support, (b) incompatibility with other systems in the institution's environment, and (c) limitations in security features in older or obsolete systems.

Effective end-of-life management should include the following:

- Maintaining inventories of systems and applications.
- Adhering to an approved end-of-life or sunset policy for older systems.
- Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor.
- Conducting risk assessments on systems and applications to help determine end-of-life.
- Planning for the replacement of systems nearing obsolescence and complying with policy requirements for implementing new systems or applications.
- Developing specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information.

If an end-of-life system or application must remain in use, management should ensure appropriate mitigating controls are in place, which may include segregating the system or application from the network. Management should also have a plan to replace the system or application and implement compensating controls until replacement. Strategies for replacing and updating hardware and software should incorporate and align with overall information security and business strategies as appropriate.

II.C.12 Malware Mitigation

Attackers use malware to obtain access to an institution's environment and to execute an attack within the environment. Malware may enter through public or private networks and from devices

attached to the network. Although protective mechanisms may block most malware before it does damage, even a single malicious executable[34] may create a significant potential for loss.

Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. Methods or systems that management should consider include the following:

- Hardware-based roots of trust, which use cryptographic means to verify the integrity of software.
- Servers that run active content at the gateway and disallow content based on policy.
- Blacklists that disallow code execution based on code fragments, Internet locations, and other factors that correlate with malicious code.
- White lists of allowed programs.
- Port monitoring to identify unauthorized network connections.
- Network segregation.
- Computer configuration to permit the least amount of privileges necessary to perform the user's job.
- Application sandboxing[35] to limit the access and functionality of executed code.
- Monitoring for unauthorized software and disallowing the ability to install unauthorized software.
- Monitoring for anomalous activity for malware and polymorphic code.
- Monitoring of network traffic.
- User education in awareness, safe computing practices, indicators of malicious code, and response actions.

II.C.13 Control of Information

Action Summary

Management should control and protect access to and transmission of information to avoid loss or damage and do the following:

- Establish and supervise compliance with policies for storing and handling information, including storing data on mobile devices and cloud services.
- Define and implement appropriate controls over the electronic transmission of information.
- Facilitate safe and secure disposal of sensitive information.
- Secure physical media in transit.

[34] In computing, an executable is a file or a program that is able to be run by a computer.

[35] Sandboxing is the use of a restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

II.C.13(a) *Storage*

Management should implement policies to govern the secure storage of all types of sensitive information, whether on computer systems, on physical media, or in hard-copy documents. Management can achieve secure storage with physical controls,[36] logical controls (e.g., passwords, tokens, and biometrics), and environmental controls (e.g., fire and flood protection). In addition, stored information, in any form, should be classified and inventoried so that it can be retrieved when needed. Inventories should be updated periodically to remain current.

More sensitive information, such as system documentation, application source code, and production transaction data, should have more extensive controls to guard against alteration (e.g., integrity checkers and cryptographic hashes). Management should have appropriate logging and monitoring controls over stored information to ensure authorized access and appropriate use. Periodically, the security staff, audit staff, and data owners should review access rights to ensure the access rights remain appropriate and current.

Data storage in portable devices, such as laptops, smart phones, and tablets, poses unique problems. These devices may be lost, stolen, or subject to unauthorized and undetected use. Risk mitigation typically involves data encryption, host-provided access controls, homing beacons,[37] and remote deletion[38] capabilities. Management should implement appropriate controls (such as the use of a DLP program) over portable devices and the sensitive information contained on them.

Many institutions create or use a third-party cloud for storage. Cloud storage[39] provides unique issues and challenges. Management should understand the nature of the cloud technology being used; the physical location(s) where the data are stored and related legal jurisdiction; the access controls used and protection of the institution's data (e.g., how access is controlled and how that information is retrieved); and the frequency and method of backup used by the cloud provider. Management should verify that the cloud provider offers the capability for the institution to monitor its system activity, significant security incidents, performance and uptime, and success and failure of backups.

II.C.13(b) *Electronic Transmission of Information*

Electronic transmission of information can include e-mail, file transfer protocol (FTP), secure FTP (sFTP), secure shell, dedicated line, short message service/texting, and transmission via the Internet. Management should determine the type of transmission method, sensitivity of the

[36] Refer to the "Physical Security" section of this booklet.

[37] Homing beacons send messages to the institution when they connect to a network and enable recovery of the device.

[38] Remote deletion is a technology that enables the institution to remotely delete certain data from a portable device.

[39] Cloud storage is a model of data storage in which the digital data are stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.

information to be transmitted, and types of safeguards available to protect information. Management should implement appropriate controls or, if they are not available, restrict the type of information that can be transmitted. When transmitting sensitive information over a public network, information should be encrypted to protect it from interception or eavesdropping. Techniques include secure e-mail protocols, sFTP, and secure sockets layer (SSL) certificates.

II.C.13(c) *Disposal of Information*

The institution should have appropriate disposal procedures for paper-based and electronic information.[40] Designating a single individual, department, or function to be responsible for disposal facilitates accountability and promotes compliance with disposal policies.

Policies should prohibit employees from discarding paper-based information containing sensitive information by using the same disposal system as regular garbage to avoid accidental disclosure. Many institutions shred paper-based media on-site while others use collection and disposal services to ensure the media are rendered unreadable and unlikely to be reconstructed. Institutions that contract with third-party service providers should conduct due diligence to ensure those third parties conduct adequate employee background checks and employ appropriate controls. Contracts with third-party disposal firms should address acceptable disposal procedures.

Electronic information and computer-based media present distinct disposal challenges. In addition to disk drives and other forms of storage, information frequently is contained in or on the memory of other devices (e.g., printers, fax machines, and cellphones). Residual data frequently remain on media, even after deletion. Because the data can be recovered, additional disposal techniques should be applied to devices containing sensitive data. Overwriting destroys data by replacing it with new, random data. Overwriting may be preferable when the media will be reused. To be effective, overwriting may have to be performed many times.

Another disposal technique is degaussing, which scrambles the data recorded on the media with powerful, varying magnetic fields. Physical destruction of the media can make the data unrecoverable. Data can sometimes be destroyed after overwriting. Management should determine the most effective method of disposal based on the type of information. Policies and procedures should address making data non-recoverable. The institution should base its disposal policies on the sensitivity of the information. Policies, procedures, and training should inform employees about what actions should be taken to securely dispose of computer-based media and protect the data from the risks of reconstruction. Management should log the disposal of sensitive media. Logs should record the party responsible for disposal, as well as the date, media type, hardware serial number, and method of disposal. In cases when such devices are rented, rather than owned, by the institution, media sanitization should be addressed contractually so that sensitive information is disposed of properly before returning equipment at the end of the rental period.

[40] See also Information Security Standards, section III.C.4., requiring each financial institution to develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of "customer information" and "consumer information."

II.C.13(d) *Transit of Physical Media*

Management should implement policies for maintaining the security of physical media (including backup tapes) containing sensitive information while in transit, including to off-site storage, or when shared with third parties. Policies should include the following:

- Contractual requirements that incorporate necessary risk-based controls.
- Restrictions on the carriers used.
- Procedures to verify the identity of couriers.
- Requirements for appropriate packaging to protect the media from damage.
- Use of adequate encryption of sensitive information recorded on media that is being physically transported.
- Tracking of shipments to provide early indications of loss or damage.
- Security reviews or independent security reports of receiving companies.
- Use of nondisclosure agreements for couriers and third parties.

II.C.13(e) *Rogue or Shadow IT*

Management should have policies explaining that employees should not and are not authorized to use unsanctioned or unapproved IT resources (e.g., online storage services, unapproved mobile device applications, and unapproved devices). Security awareness or information security training should include procedures for identifying and reporting shadow IT.

II.C.14 Supply Chain

The typical institution purchases a wide variety of hardware and software, which often is manufactured or developed internationally. In a supply chain attack, a threat source incorporates unidentified and harmful features into the purchased items before delivery. During the risk identification process, management should identify factors that may increase risk from supply chain attacks and respond with appropriate risk mitigations. An effective information security program seeks to limit the potential for harm through techniques tailored to specific acquisitions and services. Examples of techniques to mitigate the risk from such attacks include the following:

- Only making purchases through reputable sellers who demonstrate an ability to control their own supply chains.
- Purchasing hardware and software through third parties to shield the institution’s identity.
- Reviewing hardware for anomalies.
- Using automated software testing and code reviews for software.
- Regularly reviewing the reliability of software and hardware items purchased through activity monitoring and evaluations by user groups.

II.C.15 Logical Security

Action Summary

Management should have an effective process to administer logical security access rights for the network, operating systems, applications, databases, and network devices, which should include the following:

- Assigning users and devices the access required to perform required functions.
- Updating access rights based on personnel or system changes.
- Reviewing users' access rights at an appropriate frequency based on the risk to the application or system.
- Designing appropriate acceptable-use policies and requiring users to agree to them.
- Controlling privileged access.
- Changing or disabling default user accounts and passwords.

System devices, programs, and data are system resources. Because users may access these resources through the institution's network, management should identify and restrict logical access to all system resources to the minimum required for legitimate and approved work activities, according to the principle of least privilege. Access beyond the minimum required for work to be performed exposes the institution's systems and information to a potential loss of confidentiality, integrity, and availability. The institution's logical security policy and procedures should address access rights and how those rights are to be administered. Management and system administrators should regularly evaluate information system access.

Logical user access rights administration consists of three processes:

- Enrolling new users to the system.
- Authorizing modifications to user access and deletions.
- Monitoring access rights granted to each user, including periodic review and validation of access rights.

The enrollment process establishes the user's identity and anticipated business needs for information and systems. Management should identify and evaluate all users, including new employees, IT outsourcing relationships, and contractors. The assignment of access rights is typically performed by the employee's manager and the application or data owners responsible for each accessed resource, with documented approval. The assignment of rights may also be established by the employee's role or group membership, which confers certain user access rights.

Management should have an authorization process to enable the employee's manager and the application or data owners to modify or delete existing user access rights to information and systems. The authorization process should include controls to verify that proper authorizations were granted or removed. Modifications to access rights should occur when an individual's business needs change. Job changes can result in an expansion, reduction, or deletion of needed

access rights. Job changes that could trigger a modification or deletion of access rights include transfers, mandatory leave, resignations, and terminations. The institution should promptly review, and modify as needed, access rights for all users who experience job changes, particularly those with privileged access, remote access privileges, and access to customer information.

As part of the user access rights monitoring process, management should perform regular reviews to validate user access. Reviews should test whether access rights continue to be appropriate or whether they should be modified or deleted. Management should review access rights on a schedule commensurate with risk.

Logical user access rights administration also constrains user activities through an acceptable use policy that details permitted system uses, user activities, and the consequences of noncompliance. Management should maintain an acceptable use policy, and employees should be required to acknowledge and agree in writing to the policy. When implemented correctly, an acceptable use policy is a key control for user awareness and administrative policing of system activities. Elements of an acceptable use policy can include the following:

- Specific access devices that can be used to access the network.
- Hardware and software changes the user can make to his or her access device.
- Purpose and scope of network activity.
- Permitted network services.
- Information that can or cannot be transmitted, and authorized transmission methods.
- Bans on attempts to break into accounts, crack passwords, or disrupt service.
- Responsibilities for secure operation.
- Consequences of noncompliance.

Authorization for privileged access should be tightly controlled. Privileged access refers to the ability to override system or application controls, and may include system administrator access. All individuals who are granted privileged access should have the appropriate training commensurate with the risk and complexity of the systems and information they access. Prudent practices for controlling privileged access include the following:

- Identifying each privilege associated with each system resource.
- Implementing a process to allocate privileges on a need-to-use or an event-by-event basis.
- Documenting the granting and extent of privileged access.
- Assigning privileges to a unique user ID apart from the one used for normal business use.
- Prohibiting shared privileged user accounts.
- Logging and independent monitoring of the use of privileged access.
- Reviewing, by an independent party, privileged access rights and allocations at appropriate intervals.

Access rights to new software and hardware present a different problem. Typically, hardware and software are shipped with default users and at least one default user has privileged access. Lists of default accounts and passwords are readily available and can enable anyone with access to the system to obtain privileged access. These passwords should be changed, and the accounts

should be disabled. Alternately, if these accounts are not disabled, access should be monitored closely.

II.C.15(a) *Operating System Access*

Access to the operating system and system utilities provide users with the authority to make fundamental changes to the system. System utilities are programs that perform repetitive functions, such as creating, deleting, changing, or copying files. System utilities also could include numerous types of system management software that can supplement operating system functionality by supporting common system tasks, such as security, system monitoring, or transaction processing.

Unauthorized access to the operating system and system utilities could result in significant financial and operational losses. System and security administrators should restrict and monitor privileged access to operating systems and system utilities. Many operating systems have integrated or third-party access control software, which is often essential to effective access control and can be used to integrate the security management of the operating system and applications. To prevent unauthorized access to or inappropriate activity on the operating system and system utilities, management should do the following:

- Implement effective user access to appropriately restrict system access for both users and applications and, depending on the sensitivity, extend protection at the program, file, record, or field level.
- Limit the number of employees with access to operating systems and grant only the minimum level of access required to perform job responsibilities.
- Restrict and log access to and activity on operating system parameters, system utilities (especially those with data-altering capabilities), and sensitive system resources (including files, programs, and processes), and supplement with additional security software, as necessary.
- Restrict operating system access to specific terminals in physically secure and monitored locations.
- Secure or remove external drives and portable media from system consoles, terminals, or personal computers (PC) running terminal emulations, residing outside of physically secure locations.
- Prohibit remote access to operating system and system utilities, where feasible, and, at a minimum, require strong authentication and encrypted sessions before allowing such remote access.
- Filter and review logs for potential security events and provide adequate reports and alerts.
- Independently monitor operating system access by user, terminal, date, and time of access.

II.C.15(b) *Application Access*

Sensitive or mission-critical applications should incorporate appropriate access controls that restrict which functions are available to users and other applications. These access controls allow authorized users and other applications to interface with related databases. Some security software programs integrate access control between the operating system and some applications.

Such software is useful when applications do not have their own access controls or when the institution uses security software instead of the application's native access controls. Management should understand the functionality and vulnerabilities of the application access control solutions and consider those issues in the risk management process.

Management should implement effective application access controls by doing the following:

- Implementing a robust authentication[41] method consistent with the criticality and sensitivity of the application.
- Easing the administrative burden of managing application access rights by using group profiles. Managing access rights individually can lead to inconsistent or inappropriate access levels.
- Periodically reviewing and approving the application access assigned to users for appropriateness.
- Communicating and enforcing the responsibilities of programmers, security administrators, and application owners for maintaining effective application access control.
- Setting time-of-day or terminal limitations for some applications or for more sensitive functions within an application.
- Logging access and events, defining alerts for significant events, and developing processes to monitor and respond to anomalies and alerts.

II.C.15(c) *Remote Access*

Management should develop policies to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner. Such policies and procedures should define how the institution provides remote access and the controls necessary to offer remote access securely. Management should employ the following measures:

- Disable remote communications if no business need exists.
- Tightly control remote access through management approvals and subsequent audits.
- Implement robust controls over configurations at both ends of the remote connection to prevent potential malicious use.
- Log and monitor all remote access communications.
- Secure remote access devices.
- Restrict remote access during specific times.
- Limit the applications available for remote access.
- Use robust authentication methods for access and encryption to secure communications.

There are several methods to provide remote access to employees. A prevalent form of remote access is through a VPN, which provides employees with a remote connection to the institution's network through a secure channel. The VPN connection uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure

[41] Stronger authentication and layered security methods, such as the use of tokens, public-key infrastructure-based systems, or out-of-band verification coupled with a robust identity and access management process, can reduce the potential for unauthorized access.

access to their organization's network. VPN provides an encrypted isolated “tunnel” or connection between a remote user’s computer and the internal network.

Because VPN connections provide access to sensitive internal networks, the connections require additional authentication from the remote user. Use of physical token devices is a common method that can provide one-time passwords to strongly authenticate remote users.

While VPNs effectively connect the remote computer to the internal network, other alternatives provide virtual desktop capability. In these cases, the remote computer connects to a special purpose software system (sometimes a website), authenticates the user, and establishes a secure connection to an internal network server. That server establishes a local internal network desktop session and connects it to the screen, keyboard, mouse, and speakers of the remote computer. This is an actual remote control environment, where the remote user’s actions have the same effect as if connected to an actual internal network desktop. The remote control configuration may permit file transfer between the remote and internal computers. If the remote access method allows users to store sensitive institution information, management should consider limiting this access to institution-owned devices.

Other methods of remote access are available, including remote control software and third-party services, file transfer software (e.g., FTP), conferencing/session sharing tools, and other remote desktop software. Management should conduct a risk assessment and implement appropriate controls before adopting any remote access solution.

If the institution allows employees to use authorized remote access methods with institution-owned devices, management should implement the following mitigating controls:

- Prevent users from installing software on the devices.
- Prohibit users from having administrative privileges on the devices.
- Use firewalls, host-based IDS, and packet content filtering to identify, monitor, and limit remote access activities.

II.C.15(d) *Use of Remote Devices*

Management may choose to allow employees to connect remotely to the institution’s network using either an institution-owned or a personally owned device (often referred to as BYOD or “bring your own device”). Institution-owned devices are easier to secure because the institution controls the devices’ configuration and often can implement remote wiping if the devices are lost or stolen. It may be more difficult to implement remote wiping or a similar measure on an employee’s personally owned device. BYOD is becoming more popular, however, with institutions and employees because it reduces costs to the institution and enables employees to carry one device instead of two.

For all remote devices, management should do the following to control employee remote access to the institution’s network:

- Disallow remote access unless a compelling business justification exists.

- Require management approval of employee remote access.
- Regularly review remote access approvals and rescind those that no longer have a compelling business justification.
- Restrict remote access to authorized network areas and applications by using VLANs, permissions, and other techniques.
- Log remote access communications (including date, time, user, user location, duration, and activity), analyze logs in a timely manner, and follow up on anomalies.
- Implement robust authentication methods for remote access.
- Use encryption to protect communications between the access device and the institution.
- Use application white-listing.[42]

For institution-owned devices, the institution should have the ability to manage the remote devices. The following controls should be implemented:

- Securely configure remote access devices.
- Protect remote access devices against malware.
- Patch, update, and maintain all software on remote access devices.
- Encrypt sensitive data residing on the access device.
- Implement secure containers with internal boundaries to store sensitive information, in a way that is not accessible to the device without permission.
- Periodically audit the access device configurations and patch levels.
- Remotely disable or wipe the device in the event of theft or loss.
- Use geolocation of the device to support device recovery efforts.

For personally owned devices, the institution may not have the ability to configure the devices; therefore, management should have an effective method or solution to ensure that such devices meet defined institution security standards, such as operating system version, patch levels, and anti-malware solutions, before such devices are allowed to log on to the network.

II.C.16 Customer Remote Access to Financial Services

Action Summary

Management should do the following:

- Develop and maintain policies and procedures to securely offer and strengthen the resilience of remote financial services, if the institution offers such services.
- Plan for actions that adversely affect the availability of remote banking services to customers.
- Coordinate appropriate responses with the institution's ISPs and third-party service providers.
- Regularly test the institution's response plans.

[42] Application white-listing is the maintenance and use of a list of applications and their components (e.g., libraries and configuration files) that are authorized to be present or active on a system according to a well-defined baseline.

Institutions increasingly offer services to customers through remotely accessible technology, such as the Internet and mobile financial services. If the institution offers such services, management should implement appropriate authentication techniques[43] commensurate with the risk from remote banking activities. Beyond authentication, remote access controls should include additional layered security controls and may include some combination of the following:

- Application time-outs with mandatory re-authentication.
- Fraud detection and monitoring systems that include consideration of customer history and behavior to alert management, and enable a timely and effective institution response.
- Dual customer authorization through different access devices.
- Out-of-band[44] verification for transactions.
- Positive pay,[45] debit blocks, and other techniques to appropriately limit the transactional use of the account.
- Supplementary controls over certain account activities, such as transaction value limits, restrictions on devices for adding payment recipients, limits on the number of transactions allowed per day, and allowable payment windows (e.g., days and times).
- Reputation-based tools to block connections to the institution's servers based on device or network indicators known or suspected to be associated with fraudulent activities.
- Device authentication with appropriate enrollment and de-enrollment processes.
- Policies for addressing customer devices identified as potentially compromised and identifying customers who may be facilitating fraud.
- Controls over changes to account maintenance activities (e.g., address or password changes) performed by customers either online or through customer service channels.
- Supplementary controls for system administrators who are granted privileges to set up or change system configurations of business accounts.[46]
- Customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

Institution customers may also use e-mail or other electronic means to transmit instructions. All instructions received through such channels should be authenticated and validated in accordance with institution policies.

An area of heightened concern when financial institutions offer remote financial services is the potential for malicious activity against the institution's mobile or online services. Malicious actors may restrict availability to those services through denial of service (DOS) attacks that target the institution's ISPs, third-party service providers, infrastructure, or applications.

[43] Techniques include multiple factor authentication, device authentication, location consistency, and additional authentication for sensitive functions.

[44] Out-of-band refers to activity outside of the primary means of interfacing with the customer. For example, if a user is performing activity online, he or she may be authenticated through a one-time password sent via text message.

[45] Positive pay is a technique that can reduce check fraud by requesting businesses to send electronic files of information to the financial institution on all checks the business has issued.

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

Additionally, attacks on organizations that share infrastructure with the institution, including domain name services, may adversely affect the availability of remote services. Management should develop and maintain policies and procedures to identify, measure, mitigate, monitor, and report on significant security incidents to ensure the resilience of remote financial services. Planning and coordination by the institution and its third-party service providers may improve the resilience of services in the face of those attacks. To prevent or minimize exposure to these incidents, management should do the following:

- Monitor threat alerts.
- Monitor service availability and diagnose causes of reduced availability.
- Monitor applications and network traffic for indicators of nefarious activity.
- Ensure traffic filtering by the institution's ISP or upstream ISP,[47] third-party service providers, and internal resources.
- Design and implement applications to withstand application-level DOS.
- Utilize distributed architecture.
- Limit traffic (e.g., allow valid traffic and block known bad traffic by port or IP address).
- Add bandwidth.
- Enable access to services through alternative channels.

The institution should develop and test an incident response plan in conjunction with the institution's ISPs and third-party service providers to mitigate the interruption of mobile or remote financial services. Refer to the "Incident Response" section of this booklet for more information.

Customers may be provided with a website disclosure with the institution's customer acceptable-use policy. Depending on the nature of the website, the institution may require customers to demonstrate knowledge of and agreement to abide by the terms of the acceptable use policy. That evidence can be paper-based or electronic.

Refer to appendix E[48] of the *IT Handbook's* "Retail Payment Systems" booklet for more information about mobile financial services.

II.C.16(a) *Customer Awareness*

The institution's customer awareness and education efforts should consider both retail and commercial account holders and include the following elements:

- An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts accessible online.

[47] An upstream ISP is usually a large ISP that provides Internet access to a local ISP.

[48] See the *IT Handbook's* "Retail Payment Systems" booklet, appendix E, "Mobile Financial Services."

- An explanation that while the institution may contact a customer regarding his or her account or suspicious activities related to his or her account, the institution should never ask the customer to provide his or her log-in credentials over the phone or via e-mail.
- A list of recommended controls and prudent practices that the customer should implement when using the institution's remote financial services.
- A suggestion that commercial online customers perform a related risk assessment and controls evaluation periodically.
- Recommendations of technical and business controls to commercial customers that can be implemented to mitigate the risks from fraud schemes such as Business Email Compromise.[49]
- A method to contact the institution if customers notice suspicious account activity.

II.C.17 Application Security

Action Summary

Management should use applications that have been developed following secure development practices and that meet a prudent level of security. Management should develop security control requirements for all applications, whether the institution acquires or develops them. Information security personnel should be involved in monitoring the application development process to verify that secure development practices are followed, security controls are implemented, and information security needs are met.

Institutions and their customers use a wide variety of applications. Such applications include core banking applications, web applications, and installable applications (e.g., downloadable mobile applications).

A secure software development life cycle ensures that Internet- and client-facing applications have the necessary security controls. The institution should ensure that all applications are securely developed. To verify the controls have been developed and implemented appropriately, management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications. Issues noted from tests should be remediated before launching applications or moving changes into production. At institutions that employ third parties to develop applications, management should ensure that the third parties meet the same controls.

Applications should provide the ability for management to do the following:

- Implement a prudent set of security controls (e.g., password and audit policies), audit trails of security and access changes, and user activity logs for all applications.
- Establish user and group profiles for applications if not part of a centralized identity access management system.

[49] See Federal Bureau of Investigation, Alert I-012215-PSA.

- Change and disable default application accounts upon installation.
- Review and install patches for applications in a timely manner.
- Implement validation controls for data entry[50] and data processing.[51]
- Integrate additional authentication and encryption controls, as necessary, to ensure integrity and confidentiality of data and non-repudiation of transactions.
- Protect web or Internet-facing applications through additional controls, including web application firewalls, regular scanning for new or recurring vulnerabilities, mitigation or remediation of common security weaknesses, and network segregation to limit inappropriate access or connections to the application or other areas of the network.
- Mitigate risks from potential flaws in applications allowing remote access by customers and others through network, host, and application layer architecture considerations.
- Obtain attestation or evidence from third-party developers that the application acquired by the institution meets the necessary security requirements and that noted vulnerabilities or flaws are remediated in a timely manner.
- Perform ongoing risk assessments to consider the adequacy of application-level controls in light of changing threat, network, and host environments.
- Implement minimum controls recommended by the third-party service provider and consider supplemental controls as appropriate.
- Review available audit reports, and consider and implement appropriate control recommendations
- Collect data to build metrics and reporting of configuration management compliance, vulnerability management, and other measurable items as determined by management.

Whether the institution acquires or develops applications, management should establish security control requirements for new systems, system revisions, or new system acquisitions. Management should define the security control requirements based on its risk assessment process and evaluate the value of the information at risk and the potential impact of unauthorized access or damage within existing software development and acquisition processes. Management should have a process to determine risks posed by the system and necessary security requirements. Management may also refer to published, widely recognized industry standards as a starting point for establishing the institution's security requirements.

Information security personnel should be involved from the outset in the application development process to determine whether security controls are designed, tested, and implemented and information security needs are being met. Monitoring the development environment can help ensure that the implemented controls are functioning properly. Institutions that purchase applications typically rely on third-party service providers to develop applications with appropriate security built-in; management, however, should perform its own verification to

[50] Data entry validation controls include access controls over entry and changes to data, error checks, review of suspicious or unusual data, and dual entry or additional review and authorization for highly sensitive transactions or data.

[51] Data processing controls include batch control totals, hash totals of data for comparison after processing, identification of any changes made to data outside the application (e.g., data-altering utilities), and job control checks to ensure programs run in correct sequence.

determine whether the application meets the institution's security requirements. Management should analyze the environment where the application will reside. As the environment changes, the security requirements and assurance needs for the application may also change. Management should leverage available resources[52] to assist in risk identification and improve the institution's application security practices.

II.C.18 Database Security

Action Summary

Management should implement effective controls for databases and restrict access appropriately.

Databases are collections of information organized to be easily accessed, managed, and updated. Databases can be developed in-house or purchased from third parties and have their own controls and protective mechanisms configured to provide varying levels of protection. Along with many other security features, encryption helps to protect the stored information from theft or unauthorized viewing. Management should implement or enable controls commensurate with the sensitivity of the data stored in or accessed by the database.

Database users may be people (e.g., employees, customers, and contractors) or other applications. Users have different levels of access and authorization. Some users may have extensive privileges, including the ability to change the database configuration and access controls. Other users may have restrictions in what they can view, manipulate, or store. When a person is the database user, authorizations can be tailored to that person, greatly limiting the amount of information that could be exposed in a security incident. When an application is the database user, the access granted to the application can be more extensive than a person would require. Accordingly, an attack on a database through an application could expose a larger and more damaging collection of data. For application accounts, management should strengthen authentication and monitoring requirements to minimize the potential for unauthorized use.

Management should appropriately control user access and apply the principle of least privilege in assigning authorizations. The use and overall configuration of a database's security features should be part of a well-designed, layered security program.

II.C.19 Encryption

Action Summary

Management should implement the type and level of encryption commensurate with the sensitivity of the information.

[52] Resources include software tools, industry resources, specific certifications, and education courses.

Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. Encryption can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols.

Encryption can be used as a preventive control, a detective control, or both. As a preventive control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow management to discover unauthorized changes to data. When prevention and detection are joined, encryption can be an important control in ensuring confidentiality, integrity, and availability.

Institution management should employ encryption strength sufficient to protect information from disclosure. Encryption methods should be reviewed periodically to ensure that the types and methods of encryption are still secure as technology and threats evolve. Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure and the costs of encryption. The need to encrypt data is determined by the institution's data classification and risk assessment.

Passwords should be hashed or encrypted in storage. Passwords that are hashed also should be salted.[53] Files containing encrypted or hashed passwords used by systems to authenticate users should be readable only with elevated (or administrator) privileges.

Key management[54] is crucial to the effective use of encryption. Effective key management systems rely on an agreed set of standards, procedures, and secure methods that address the following:[55]

- Generating keys for different cryptographic systems and different applications.
- Generating and obtaining public keys.
- Distributing keys to intended users, including how keys should be activated when received.
- Storing keys, including how authorized users obtain access to keys.
- Changing or updating keys, including rules on when and how keys should be changed.
- Addressing compromised keys.
- Archiving, revoking, and specifying how keys should be withdrawn or deactivated.
- Recovering keys that are lost or corrupted as part of business continuity management.
- Logging the auditing of key management-related activities.
- Instituting defined activation and deactivation dates, and limiting the usage period of keys.

[53] In password protection, salt is a random string of data used to modify a password hash.

[54] Key management is the management of cryptographic keys. This includes dealing with the generation, exchange, storage, use, and replacement of keys.

[55] Refer to ISO/IEC 11770-1:2010, "Key Management—Part 1: Framework"; ISO/IEC 11770-2:2008, "Key Management—Part 2: Mechanisms Using Symmetric Techniques"; and ISO/IEC 11770-3:2015, "Key Management—Part 3: Mechanisms Using Asymmetric Techniques."

II.C.20 Oversight of Third-Party Service Providers

Action Summary

Management should oversee outsourced operations through the following:

- Appropriate due diligence in third-party research, selection, and relationship management.
- Contractual assurances for security responsibilities, controls, and reporting.
- Nondisclosure agreements regarding the institution's systems and data.
- Independent review of the third party's security through appropriate reports from audits and tests.
- Coordination of incident response policies and contractual notification requirements.
- Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported.

Management should conduct appropriate due diligence in selecting and monitoring third-party service providers. Management should be responsible for ensuring that such third parties use suitable information security controls when providing services to the institution. When indicated by the institution's risk assessment, management should monitor third-party service providers to confirm that they are maintaining appropriate controls. If the third-party service provider stores, transmits, processes, or disposes of customer information, management should require third-party service providers by contract to implement appropriate measures designed to meet the Information Security Standards.

Management should evaluate information security considerations of potential third-party service providers during initial due diligence. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

Management should verify that third-party service providers implement and maintain controls sufficient to appropriately mitigate risks. The institution's contracts should do the following:

- Include minimum control and reporting standards.
- Provide for the right to require changes to standards as external and internal environments change.
- Specify that the institution or an independent auditor has access to the service provider to perform evaluations of the service provider's performance against the Information Security Standards.

Refer to the "Third-Party Reviews of Technology Service Providers" section of the *IT Handbook's* "Audit" booklet for more information.

Additionally, as part of the oversight of third-party service providers, management should determine whether cyber risks are identified, measured, mitigated, monitored, and reported by such third parties as third-party cyber threats can have an impact on the institution. Information security reporting by the institution should incorporate an assessment of these third-party risks to

facilitate a comprehensive understanding of the institution's exposure to third-party cyber threats.

II.C.20(a) *Outsourced Cloud Computing*

As with other forms of outsourcing, information security implications are key in the cloud computing model. Management may need to revise information security policies, standards, and procedures to incorporate the activities related to a cloud computing service provider. Refer to the FFIEC's "Outsourced Cloud Computing" statement for more information.[56]

II.C.20(b) *Managed Security Service Providers*

Management may rely on third parties to provide security services; management, however, remains responsible for ensuring the security of the institution's systems and information by overseeing the effectiveness of the services provided by the managed security services provider. Additional information is available in appendix D of the *IT Handbook's* "Outsourcing Technology Services" booklet.

II.C.21 Business Continuity Considerations

Action Summary

Management should do the following:

- Identify personnel who will have critical information security roles during a disaster, and train personnel in those roles.
- Define information security needs for backup sites and alternate communication networks.
- Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios.

Business continuity plans should be reviewed as an integral part of the security process. Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution if continuity plans must be implemented. Management should train personnel regarding their security roles during a disaster. Additionally, management should update technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of the business continuity plan.

Information security events may trigger activation of the business continuity plan. Therefore, the institution's plan should include steps that explicitly address information security incident response and resilience. Resilience testing should incorporate information security event scenarios identified by the institution.

Refer to the *IT Handbook's* "Business Continuity Planning" booklet for more information.

[56] See FFIEC, "Outsourced Cloud Computing," July 10, 2012.

II.C.22 Log Management

Network and host activities typically are recorded on the host and sent across the network to a central logging repository. The data that arrive at the repository are in the format of the software that recorded the activity. The logging repository may process the data and can enable timely and effective log analysis. Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs.

Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Intruders often attempt to conceal unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging repository. Considerations for securing the integrity of log files include the following:

- Encrypting log files that contain sensitive data or that are transmitted over the network.
- Ensuring adequate storage capacity to avoid gaps in data gathering.
- Securing backup and disposal of log files.
- Logging the data to a separate, isolated computer.
- Logging the data to read-only media.
- Setting logging parameters to disallow any modification to previously written data.
- Restricting access to log files to a limited number of authorized users.

Additionally, logging practices should be reviewed periodically by an independent party to ensure appropriate log management.

Logs are voluminous and challenging to read. They come from a variety of systems and can be difficult to manage and correlate. Security information and event management (SIEM) systems can provide a method for management to collect, aggregate, analyze, and correlate information from discrete systems and applications. Management can use SIEM systems to discern trends and identify potential information security incidents. SIEM systems can be used to gather information from the following:

- Network and security devices and systems.[57]
- Identity and access management applications.
- Vulnerability management and policy compliance tools.
- Operating system, database, and application logs.
- Physical and environmental monitoring systems.
- External threat data.

Regardless of the method of log management, management should develop processes to collect, aggregate, analyze, and correlate security information. Policies should define retention periods for security and operational logs. Institutions maintain event logs to understand an incident or cyber event after it occurs. Monitoring event logs for anomalies and relating that information

[57] These can include intrusion detection and prevention systems, DLP solutions, and firewalls.

with other sources of information broadens the institution's ability to understand trends, react to threats, and improve reports to management and the board.

II.D Risk Monitoring and Reporting

Risk monitoring is a process by which the institution tracks information about its inherent risk profile and identifies gaps in the effectiveness of risk mitigation activities. Risk monitoring should address changing threat conditions in both the institution and the greater financial industry. Threats change frequently, particularly in terms of the threat's capabilities and intentions, as well as the vulnerabilities they may exploit. Vulnerabilities in software are continually announced, and other vulnerabilities may emerge as the institution's systems are modified or updated. External requirements, including the use of new third-party service providers, also may change the institution's inherent risk profile.

Risk reporting is a process that produces information systems reports that address threats, capabilities, vulnerabilities, and inherent risk changes. Risk reporting should describe any information security events that the institution faces and the effectiveness of management's response and resilience to those events. The reporting process should provide a method of disseminating those reports to appropriate members of management. The contents of the reports should prompt action, if necessary, in a timely manner to maintain appropriate levels of risk.

II.D.1 Metrics

A mature and effective information security program uses metrics to improve the program's effectiveness and efficiency. Management should develop metrics that demonstrate the extent to which the security program is implemented and whether the program is effective. Metrics are used to measure security policy implementation, conformance with the information security program, the adequacy of security services delivery, and the impact of security events on business processes. The measurement of security characteristics can allow management to increase control and drive improvements to the security process. Metrics generally are formed to measure conformance to the standards and procedures that are used to implement policies.

Management should utilize metrics to quantify and report risks of the information security program. Metrics should be gathered from external sources and internal data. The scope of metrics should be comprehensive and commensurate with the complexity of the institution's operations. Reports should incorporate metrics tailored for different audiences and stakeholders. These metrics and other monitoring reports of the information security program should feed into ITRM reporting.

III Security Operations

Action Summary

Management should design policies and procedures to effectively manage security operations with the following characteristics:

- Broadly scoped to address all ongoing security-related functions.
- Guided by defined processes.
- Integrated with lines of business and third parties.
- Appropriately staffed and supplied with technology for continual incident detection and response activities.

Security operations involve a wide range of activities. Those activities may be centralized in a security operations center, distributed within the information security department and business lines, or outsourced in whole or in part. Security operations activities can include the following:

- Security software and device management (e.g., maintaining the signatures on signature-based devices and firewall rules).
- Forensics (e.g., analysis of potentially compromised systems).
- Threat identification and assessment.
- Vulnerability identification (e.g., operation or supervision of vulnerability scans, self-assessments, penetration tests, and analysis of audit results).
- Vulnerability cataloging and remediation tracking.
- Physical security management (e.g., CCTV, guards, and badge systems).
- Law enforcement interface (e.g., data retention and lawful intercepts).
- Third-party integration (e.g., managed security services and incident detection services).
- Network, host, and application activity monitoring.
- Analysis of threat intelligence from external sources.
- Engagement with information sharing groups.
- Incident detection and management.
- Enforcement of access controls.

Management should establish defined processes and appropriate governance to facilitate the performance of security operations. Policies should address the timing and extent of the security operations activities, reporting, escalation triggers, and response actions. Many institutions use an issue tracking system[58] to record and manage requests and events. An issue tracking system can be a source of evidence, contain a variety of security information, and serve as a valuable tool to assist management when taking actions to strengthen the information security environment.

[58] An issue tracking system (also ITS, trouble ticket system, ticketing management system, support ticket system, request management system, or incident ticket system) is a computer software package that manages and maintains lists of security issues.

Management should coordinate security operation activities with the institution's lines of business and with third-party service providers. Regardless of how extensive the coordination is, the goal should be to maintain a sufficient security operation capability across the entire environment.

Sufficient technology and staff should be available to support continual incident detection and response activities. Some institutions may rely on or supplement their activities with third parties to gain the necessary scope and depth of coverage. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for more information.

III.A Threat Identification and Assessment

Action Summary

Management should do the following:

- Identify and assess threats.
- Use threat knowledge to drive risk assessment and response.
- Design policies to allow immediate and consequential threats to be dealt with expeditiously.

Threat identification and assessment involves discovering knowledge about threat sources and vulnerabilities and analyzing the potential for exploitation. This is much more focused than the risk identification process described in the "Risk Identification" section of this booklet. Information gained from threat identification and assessment should be used in risk assessment and response to drive protective and detective strategies and tactics. Strategies involve the information security program's policies, standards, and procedures, and the implementing technologies. Examples of tactics include threat signatures used for incident identification and management of threat behaviors. NIST notes that types of threat sources include the following:

- Hostile cyber or physical attacks.
- Human errors of omission or commission.
- Structural failures of organization-controlled resources (e.g., hardware, software, and environmental controls).
- Natural and man-made disasters, accidents, and failures beyond the control of the organization.[59]

Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information. The identification of threats involves the sources of threats, their capabilities, and their objectives. Information about threats generally comes from government (e.g., US-CERT), information-sharing organizations (e.g., FS-ISAC), industry sources, the institution, and third parties. Third-party information may be from organizations that specifically track and report on threats or from third-party reports of past activity. Some of those

[59] NIST SP 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments," September 2012.

reports compile knowledge from incidents reported by many organizations worldwide. Different types of information supporting an assessment may be available through the following:

- Incident data from reports published by security providers and others.
- Attack data from sources including FS-ISAC and managed security service providers.
- Threat data through reports available either free or for a fee.

The availability of threat information is often ad hoc, although some providers present threat information within a defined framework that readily lends itself to analytical operations. By using a threat taxonomy, the institution may greatly reduce the complexity of threat assessment and enable efficient understanding of reasonable risk mitigations. Specific factors in the threat assessment may include a description, context for operation, capabilities and intent, and, from the threat-source perspectives, benefits and negative consequences associated with an attack.

Knowledge of threat sources is especially important to help identify vulnerabilities. Vulnerabilities can occur in many areas, such as the system design, the system operation, security procedures, business line controls, and the implementation of the system and controls. Self-assessments, audits, scans, penetration tests, and reviews of SIEM reports can identify vulnerabilities. Additionally, external individuals or groups can identify vulnerabilities.

Tools for analyzing vulnerabilities in a layered security environment include attack trees, event trees, and kill chains. These tools attempt to model an attacker's actions to enable identification of the most effective and efficient remediation options.

Once a threat is identified and potential vulnerabilities are assessed, the significance of the threat should trigger a response. The response should be commensurate with the risk posed by the threat and should include remediation options. Management should design policies to allow for immediate and consequential threats to be dealt with expeditiously, while less significant threats are addressed as part of a broader risk management process. When management receives vulnerability information from external individuals or groups, management should have appropriate processes and procedures to evaluate the credibility of the information to appropriately address it.

III.B Threat Monitoring

Threat monitoring policies should provide for continual and ad hoc monitoring of threat intelligence communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal procedures. Management should establish the responsibility and authority of security personnel and system administrators for monitoring. Additionally, management should review and approve the tools used and the conditions for use.

Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies. Monitoring should address incoming and outgoing network traffic, seeking to identify malicious activity and data exfiltration. Additionally, the monitoring process should be established and documented to independently monitor administrators and other users with higher privileges.

III.C Incident Identification and Assessment

Action Summary

Management should have a process to enable the following:

- Identify indicators of compromise.
- Analyze the event associated with the indicators.
- Classify the event.
- Escalate the event consistent with the classification.
- Report internally and externally as appropriate.

Incident identification involves indicators and analysis. External indicators may arise through contact with customers, law enforcement, card organizations (e.g., credit or payment cards), other financial institutions, media, or others. Internal indicators may arise when internal users contact the help desk, IT operations follows up on anomalies, or security operations follows up on anomalies identified through security devices and network and systems activity. Indicators may also arise through the use of "hunt teams," or dedicated analysts who actively search for indicators of compromise. Examples of technology-based intrusion identification systems and tools include the following:

- Threat intelligence data feeds (e.g., STIX/TAXII).[60]
- Intrusion detection and prevention systems for networks and hosts.
- End-point visibility tools (tools that can identify the function of end points and which end points contain or have access to sensitive information).
- DLP tools.
- Log correlation and analysis tools.
- File integrity tools.
- Malware detection tools.
- Network behavior analysis systems.
- "Big data" tools and analytics that aggregate and allow pre-formed and ad hoc analysis.

Technology-based indicators of compromise generally are anomalies in host state, host activity, and network traffic. A few examples are unexpected (1) processes, (2) changes to files, (3) packet source or destination, (4) protocols, (5) ports, (6) encryption, (7) log-ins, and (8) packet content. Other indicators include alerts triggered by black lists in anti-virus and network-monitoring products.

Management should have a process for identifying indicators of compromise and rapidly reporting those indicators for investigation. The report should instigate an analysis that seeks to

[60] There are efforts to automate and structure operational cybersecurity information-sharing techniques across the globe. Of these, STIX (the Structured Threat Information eXpression) and TAXII (the Trusted Automated eXchange of Indicator Information) are two of the technical specifications that allow an automated exchange of threat source data using standardized language.

confirm whether a compromise took place and how that compromise should be classified. Investigation may require additional information from outside and inside the institution, such as a forensic review. Management should perform due diligence to identify external assistance in advance of incidents to ensure available resources. Classification of a compromise may require information on the specific hosts affected, data lost, and business processes affected. Information developed in the analysis may be useful to guide response activities.

Analysis should result in a classification of the event, implementation of escalation procedures, and reporting. Analysis should be guided by the following:

- Classification policies should be sufficiently clear to enable timely classification of incidents by level of severity, enabling the use of response teams and responses depending on the type and severity of events.
- Escalation, response, and reporting should be commensurate with the level of severity.
- Escalation policies should address when different personnel within the organization will be contacted and the responsibility those personnel have in incident analysis and response.
- Escalation policies should include when to request or obtain external assistance, from both third parties and the federal government.
- Reporting policies should address internal and external reporting, including coordination with third parties and reporting to external organizations (e.g., FS-ISAC).

Additionally, a policy should address who is empowered to declare an incident. A defined process should guide responses to incidents. The institution should develop procedures to test the incident escalation, response, and reporting processes.

The sharing of attack data through organizations, such as FS-ISAC, also has the potential to benefit the industry at large by enabling other institutions to better assess and respond to current attacks. Management should consider whether to include such information sharing as a part of its strategy to protect the institution.

Management should determine whether the institution's or its managed security service provider's analysts are sufficiently trained to appropriately analyze network, host, and application activity and to use the monitoring and analysis tools made available to them. Additionally, security analysts should coordinate and collaborate with others in the institution with knowledge and authority for specific types of malicious activity, such as fraud.

III.D Incident Response

Management should have an incident response program.[61] The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate, containing the incident, coordinating with law

[61] See also "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," supplementing the Information Security Standards.

enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the institution.

The response involves a combination of people and technologies. The quality of incident response is attributable to the institution's culture, policies, procedures, and training. Incident response is also a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS-ISAC), and others. Management should prepare for potential incidents by developing an incident response plan that is comprehensive, coordinated, and integrated with existing institution policies, procedures, and training. To validate the effectiveness of the institution's incident response program, management should periodically test it through different test types, including scenario planning and tabletop testing, and perform the tests with appropriate internal and external parties.

Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort. Additionally, management should define thresholds for reporting significant security incidents, and consider developing processes for when the institution should notify its regulators of incidents that may affect the institution's operations, reputation, or sensitive customer information. These incidents may include those that could affect the financial system. Primary considerations for incident response include the following:

- How to balance concerns regarding confidentiality, integrity, and availability for devices and data. This consideration is a key driver for a containment strategy and may involve legal and liability considerations. Management may decide that some systems must be disconnected or shut down at the first sign of intrusion, while others must be left on line.
- When and under what circumstances to invoke the incident response activities, and how to ensure that the proper personnel are notified and available.
- When to involve outside experts and how to ensure the proper expertise will be available when needed. This consideration addresses both containment and restoration.
- Protocols to define when and under what circumstances to notify and involve regulators, customers, and law enforcement, including names and contact information for each group.
- Which personnel have authority to perform specific actions in the containment of the intrusion and restoration of the system. This consideration affects the internal communications strategy, the commitment of personnel, and procedures that escalate involvement and decisions within the organization.
- How, when, and what to communicate outside of the institution, whether to law enforcement, regulatory agencies, information-sharing organizations, customers, third-party service providers, potential victims, or others.
- How to document and maintain the evidence, the decisions made, and the actions taken.
- What criteria must be met before compromised services, equipment, and software are returned to the network.
- How to learn from the intrusion and use lessons learned to improve the institution's security.
- How and when to prepare and file a Suspicious Activities Report.

Successful implementation of any response policy or procedure requires the assignment of responsibilities, training, and testing. Some institutions formalize the response program with the creation of a security incident response team (SIRT). The SIRT typically is tasked with performing, coordinating, and supporting responses to security incidents and intrusions. Because of the wide range of technical and nontechnical issues posed by an intrusion, typical SIRT membership includes individuals with a wide range of backgrounds and expertise from different areas within the institution. Those areas include management, legal, and public relations, as well as IT staff. Other organizations may outsource some of the SIRT functions (e.g., forensic examinations). When SIRT functions are outsourced, management should require the third-party service provider to follow the institution's policies and maintain the confidentiality of data.

Institutions should assess the adequacy of their preparation through testing. There are a variety of testing methods; therefore, management should consider the most applicable tests for its IT environment. Institutions can also participate with outside entities that provide testing activities (e.g., FS-ISAC).

While containment strategies between institutions can vary, they typically include the following broad elements:

- Isolation of compromised systems or enhanced monitoring of intruder activities.
- Search for additional compromised systems.
- Collection and preservation of evidence.
- Communication with affected parties and often the primary regulator, information-sharing organizations (e.g., FS-ISAC), or law enforcement.

Restoration and follow-up strategies should address the following:

- Elimination of an intruder's means of access.
- Restoration of systems, programs, and data to a known good state.
- Initiation of customer notification and assistance activities consistent with laws, regulations, and interagency guidance.
- Monitoring to detect similar or further incidents.

Management should periodically review the actions taken in response to intrusions to identify improvements and implement those improvements through changes in policy, standards, procedures, training, and practices.

IV Information Security Program Effectiveness

The information security program should be subject to periodic review to ensure continual improvement in the program's effectiveness. The review should address the program in the context of the environment in which the program now operates, both within the institution and outside. Lessons learned from experience, audit findings, and other indicators of opportunities for improvement should be identified and the program changed as appropriate.

IV.A Assurance and Testing

Action Summary

Management should ascertain that the information security program is operating securely, as expected, and reaching intended goals by doing the following:

- Testing and evaluating through self-assessments, tests, and audits with appropriate coverage, depth, and independence.
- Aligning personnel skills and program needs.
- Establishing and implementing a reporting process that includes the assembly and distribution of assurance reports that are timely, complete, transparent, and relevant to management decisions.

Assurance relates to the confidence that the information security program is mitigating risk as expected. Assurance targets two parts of the process: (1) the IT system's design and (2) the IT system's operation. The institution should carefully distinguish between the two because the former relates to risk decisions that change the security controls and the latter relates to the operation of the controls. Flaws in control design typically are corrected by a redesign, and flaws in operation typically are corrected through a compliance program.

The institution should have a documented testing and evaluation plan that addresses the integration of security controls, level of assurance desired, and strategies and activities performed in obtaining that assurance. The plan should identify specific components of the system to address, methods by which the components are to be addressed, timing and frequency of the tests and evaluations, and criteria used to ascertain whether the test and evaluation results are acceptable and provide assurance.[62]

IV.A.1 Key Testing Factors

Management should consider the following key factors when developing and implementing independent tests:

- **Scope.** The tests and methods utilized, in the aggregate, should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling the risk from information security-related events.
- **Personnel.** Technical testing is only as good as the personnel performing and supervising the test. Management should review qualifications of testing personnel to verify testers' capabilities are adequate to support the test objectives.
- **Notifications.** Management should consider whom to inform within the institution about the timing and nature of the tests. The need for protection of institution systems and the potential for disruptive false alarms should be balanced against the need to test personnel reactions to unexpected activities.

[62] See also Information Security Standards, section III.C.3, requiring each financial institution to test the key controls, systems, and procedures of its information security program using independent third parties or staff independent of those that develop or maintain the program.

- **Confidentiality, integrity, and availability.** Management should carefully control information security tests to limit the risks to confidentiality, integrity, and system availability. Because testing may uncover sensitive customer information, management should use appropriate safeguards to protect such information. Management should ensure that employee and contract personnel who perform the tests or have access to the test results have passed appropriate background checks and that contract personnel are appropriately bonded. Because certain tests may pose more risk to system availability than other tests, management should have personnel who perform those tests maintain logs of testing actions. Those logs are helpful if the systems react unexpectedly.
- **Confidentiality of test plans and data.** Because knowledge of test planning and results may facilitate a security breach, the institution should carefully limit the distribution of testing information. Management should restrict test plans and data only to those individuals involved in the testing. Results should be made available in a usable form only to those responsible for following up on tests. Additionally, management should require contractors to sign nondisclosure agreements and to return information they obtained in their testing to the institution.
- **Frequency.** The institution's ITRM process should determine the frequency of independent testing. Factors that may increase testing frequency include changes to network configurations, changes to or additions of systems and applications, significant changes in potential attacker profiles and techniques, and results of other testing. For instance, management should have a testing process for security and usability over the life cycle of testing (during development, before placing a new or modified system into production, and periodic testing of the production system or application).
- **Proxy testing.** Proxy testing refers to testing that is conducted on like systems and with like interfaces, rather than the actual system, to avoid disruptions on a system that may be too critical for a comprehensive continuity test. Proxy tests are conducted using the same hardware and operating software, are sometimes used as a replacement for actual tests, and should provide similar results. Independent testing of a proxy system is generally not effective in validating the effectiveness of a security process. Proxy testing, by its nature, does not test the operational system's policies and procedures or its integration with other systems. It also does not test the reaction of personnel to unusual events. Proxy testing may be the best choice, however, when management is unable to test the operational system without creating excessive risk.

IV.A.2 Types of Tests and Evaluations

Information security management may use several tools to gain confidence that the information security program is operating as expected and reaching the intended goals. The primary tools include self-assessments, penetration tests, vulnerability assessments, and audits. The coverage and depth of the various tools directly relates to the confidence gained in the information security program.

IV.A.2(a) *Self-Assessments*

Periodic self-assessments typically should be performed by the organizational unit being assessed. Self-assessments capture subjective opinions on the achievement of objectives.

Although they may provide valuable information related to perceived changes in the level of risk and effectiveness of controls, they are affected by the breadth and depth of the assessor's knowledge, the completeness and reliability of information used to complete the assessment, and the assessor's biases. Self-assessment frequency should be a function of the level of assurance needed by the institution, determined by the risk management process. Results from self-assessments can be informative to the overall test and evaluation process. Management should use the results to help strengthen the organizational unit's information security.

IV.A.2(b) *Penetration Tests*

A penetration test subjects a system to real-world attacks selected and conducted by the testers. A penetration test targets systems and users to identify weaknesses in business processes and technical controls. The test mimics a threat source's search for and exploitation of vulnerabilities to demonstrate a potential for loss. Some tests focus on only a subset of the institution's systems and may not accurately simulate a determined threat actor. There are many types of penetration tests (e.g., network, client-side, web application, and social engineering), and management should determine the level and types of tests employed to ensure effective and comprehensive coverage.

The frequency and scope of a penetration test should be a function of the level of assurance needed by the institution and determined by the risk assessment process. The test can be performed internally by independent groups, internally by the organizational unit, or by an independent third party. Management should determine the level of independence required of the test.

IV.A.2(c) *Vulnerability Assessments*

A vulnerability assessment is a process that defines, identifies, and classifies the vulnerabilities in a computer, network, or communications infrastructure. Technical vulnerabilities can be identified through the use of scanners and other tools. Scanners search for known vulnerabilities (e.g., Mitre's CVE) or for known vulnerability classes (e.g., Structured Query Language [SQL] injection and cross-site scripting). They also can search for compliance with approved configurations. Scanners identify vulnerabilities by inspecting network traffic or hosts. When inspecting hosts, they may require agents to be placed on the hosts with high-level access. If host agents are required, the security over the use of credentials in the scan should be a prime consideration for management.

Similar to penetration testing, the frequency of the performance of vulnerability assessments should be determined by the risk management process. Scanners and other tools can be run continuously, generating metrics that are reported and acted upon continuously. Alternatively, they can be run periodically. Vulnerability assessments can be performed internally or by external testers, but they are often run as part of internal testing processes.

IV.A.2(d) *Audits*

Independent internal departments or third parties typically perform audits. Audits should review every aspect of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the reasonableness and appropriateness of, and compliance with, policies, standards, and procedures; report on information security activity and control deficiencies to decision makers; identify root causes and recommendations to address deficiencies; and test the effectiveness of controls within the program. Internal audit should track the results and the remediation of control deficiencies reported in audits and additional technical reviews, such as penetration tests and vulnerability assessments.

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

IV.A.3 Independence of Tests and Audits

Institutions frequently use independent organizations to test aspects of their information security programs. Independent tests have the potential to reduce bias, increase capabilities, and increase knowledge about threats and technologies. Independence gives credibility to the test results. To be considered independent, testing personnel should not be responsible for the design, installation, maintenance, and operation of the tested system, or the policies and procedures that guide its operation. The reports generated from the tests should be prepared by individuals who similarly are independent.

IV.A.4 Assurance Reporting

Reporting of self-assessments, penetration tests, vulnerability assessments, and audits supports management decision making. Those decisions may support a range of ITRM activities, including the prioritization and funding of resource allocations and improvement to existing information security policies and procedures.

Management should provide reports that are timely, complete, transparent, and relevant to management decisions. The reports should prioritize risk and findings in the order of importance, suggest options for remediation, and highlight repeat issues. Additionally, reports should address root causes. The reporting should be to individuals with authority and responsibility to act on the reports and to those accountable for the outcomes, as well as those responsible for advising or influencing risk decisions. Reporting should trigger appropriate, timely, and reliable escalation and response procedures. Summary reports should be made available to the board as appropriate.

Appendix A: Examination Procedures

Examination Objective

Determine the quality and effectiveness of the institution's information security. Examiners should use these procedures to measure the adequacy of the institution's culture, governance, information security program, security operations, and assurance processes. In addition, controls should be evaluated as additional evidence of program quality and effectiveness. Controls also should be evaluated for conformance with contracts, indicators of legal liability, and conformance with regulatory policy and guidance. Failure of management to implement appropriate controls may expose the institution to potential loss from fines, penalties, and customer litigation.

These examination procedures (commonly referred to as the work program) are intended to help examiners determine the effectiveness of the institution's information security process. Examiners may choose, however, to use only particular components of the work program based on the size, complexity, and nature of the institution's business. Examiners should also use these procedures to measure the adequacy of the institution's cybersecurity risk management processes.

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

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

    a. Regulatory reports of examination.
    b. Internal and external audit reports.
    c. Independent security tests.
    d. Regulatory, audit, and security reports on service providers.

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

    a. Adequacy and timing of corrective action.
    b. Resolution of root causes rather than just specific issues.
    c. Existence of any outstanding issues.

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

    a. Products or services delivered to either internal or external users.
    b. Network topology or diagram including changes to configuration or components and all internal and external connections.
    c. Hardware and software inventories.
    d. Loss, addition, or change in duties of key personnel.
    e. Technology service providers and software vendor listings.

f. Communication lines with other business units (e.g., loan review, credit risk management, line of business quality assurance, and internal audit).
g. Credit or operating losses primarily attributable (or thought to be attributable) to IT (e.g., system problems, fraud occurring due to poor controls, and improperly implemented changes to systems).
h. Changes to internal business processes.
i. Internal reorganizations.

4. Determine the complexity of the institution's information security environment.

    a. Determine the degree of reliance on service providers for information processing and technology support, including security operation management.
    b. Identify unique products and services and any required third-party access requirements.
    c. Determine the extent of network connectivity internally and externally and the boundaries and functions of security domains.
    d. Identify the systems that have recently undergone significant change, such as new hardware, software, configuration, and connectivity. Correlate the changed systems with the business processes they support, the extent of customer data available to those processes, and the effect of those changes on institution operations.

Objective 2: Determine whether management promotes effective governance of the information security program through a strong information security culture, defined information security responsibilities and accountability, and adequate resources to support the program.

1. Determine whether the institution has a culture that contributes to the effectiveness of the information security program.

    a. Determine whether the institution's board and management understand and support information security and provide appropriate resources for the implementation of an effective security program.
    b. Determine whether the information security program is integrated with the institution's lines of business, support functions, and management of third parties.
    c. Review for indicators of an effective information security culture (e.g., method of introducing new business initiatives and manner in which the institution holds lines of business and employees accountable for promoting information security).

2. Determine whether the board, or a committee of the board, is responsible for overseeing the development, implementation, and maintenance of the institution's information security program.

3. Determine whether the board holds management accountable for the following:

    a. Central oversight and coordination.
    b. Assignment of responsibility.
    c. Support of the information security program.

d. Effectiveness of the information security program.

4. Determine whether the board approves a written information security program and receives a report on the effectiveness of the information security program at least annually. Determine whether the report to the board describes the overall status of the information security program and discusses material matters related to the program such as the following:

    a. Risk assessment process, including threat identification and assessment.
    b. Risk management and control decisions.
    c. Service provider arrangements.
    d. Results of security operations activities and summaries of assurance reports.
    e. Security breaches or violations and management's responses.
    f. Recommendations for changes or updates to the information security program.

5. Determine whether management responsibilities are appropriate and include the following:

    a. Implementation of the information security program by clearly communicating responsibilities and holding appropriate individuals accountable for carrying out these responsibilities.
    b. Establishment of appropriate policies, standards, and procedures to support the information security program.
    c. Participation in assessing the effect of security threats or incidents on the institution and its business lines and processes.
    d. Delineation of clear lines of responsibility and communication of accountability for information security.
    e. Adherence to risk thresholds established by the board relating to information security threats or incidents, including those relating to cybersecurity.
    f. Oversight of risk mitigation activities that support the information security program.
    g. Establishment of appropriate segregation of duties.
    h. Coordination of both information and physical security.
    i. Integration of security controls throughout the institution.
    j. Protection of data consistently throughout the institution.
    k. Definition of the information security responsibilities of third parties.
    l. Facilitation of annual information security and awareness training and ongoing security-related communications to employees.

6. Determine whether management has designated one or more individuals as an information security officer and determine appropriateness of the reporting line.

7. Determine whether security officers and employees know, understand, and are accountable for fulfilling their security responsibilities.

8. Determine the adequacy of audit coverage and reporting of the information security program by reviewing appropriate audit reports and board or audit committee minutes. (For further questions, refer to the *IT Handbook's* "Audit" booklet examination procedures.)[63]

9. Determine whether the board provides adequate funding to develop and implement a successful information security function. Review whether the institution has the following:

    a. Appropriate staff with the necessary skills to meet the institution's technical and managerial needs.
    b. Personnel with knowledge of technology standards, practices, and risk methodologies.
    c. Training to prepare staff for their short- and long-term security responsibilities.
    d. Oversight of third parties when they supplement an institution's technical and managerial capabilities.

10. Determine whether management has adequately incorporated information security into its overall ITRM process. (For further questions, refer to the *IT Handbook's* "Management" booklet examination procedures.)[64]

Objective 3: Determine whether management of the information security program is appropriate and supports the institution's ITRM process, integrates with lines of business and support functions, and integrates third-party service provider activities with the information security program.

1. Determine whether the institution has an effective information security program that supports the ITRM process. Review whether the program includes the following:

    a. Identification of threats and risks.
    b. Measurement of risks.
    c. Implementation of risk mitigation.
    d. Monitoring and reporting of risks.
    e. Methods to assess the program's effectiveness.

2. Determine whether management appropriately integrates the information security program across the institution's lines of business and support functions. Review whether management has the following:

    a. Security policies, standards, and procedures that are designed to support and to align with the policies in the lines of business.
    b. Incident response programs that include all affected lines of business and support units.
    c. Common awareness and enforcement mechanisms between lines of business and information security.
    d. Visibility to assess the likelihood of threats and potential damage to the institution.
    e. The ability to identify and implement controls over the root causes of an incident.

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

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

3. If the institution outsources activities to a third-party service provider, determine whether management integrates those activities with the information security program. Verify that the third-party management program evidences expectations that align with the institution's information security program.

Objective 4: As part of the information security program, determine whether management has established risk identification processes.

1. Determine whether management effectively identifies threats and vulnerabilities continuously.

2. Determine whether the risk identification process produces manageable groupings of information security threats, including cybersecurity threats. Review whether management has the following:

    a. A threat assessment to help focus the risk identification efforts.
    b. A method or taxonomy for categorizing threats, sources, and vulnerabilities.
    c. A process to determine the institution's information security risk profile.
    d. A validation of the risk identification process through audits, self-assessments, penetration tests, and vulnerability assessments.
    e. A validation though audits, self-assessments, penetration tests, and vulnerability assessments that risk decisions are informed by appropriate identification and analysis of threats and other potential causes of loss.

3. Determine whether management has a means to collect data on potential threats to identify information security risks. Determine whether management uses threat modeling (e.g., development of attack trees) to assist in identifying and quantifying risk and in better understanding the nature, frequency, and sophistication of threats.

4. Determine whether management has continuous, established routines to identify and assess vulnerabilities. Determine whether management has processes to receive vulnerability information disclosed by external individuals or groups, such as security or vulnerability researchers.

5. Determine whether management adjusts the information security program for institutional changes and changes in legislation, regulation, regulatory policy, guidance, and industry practices. Review whether management has processes to do the following:

    a. Maintain awareness of new legal and regulatory requirements or changes to industry practices.
    b. Update the information security program to reflect changes.
    c. Report changes of the information security program to the board.

Objective 5: Determine whether management measures the risk to guide its recommendations for and use of mitigating controls.

1. Determine whether management uses tools to perform threat analysis and analyzes information security events to help do the following:

    a. Map threats and vulnerabilities.
    b. Incorporate legal and regulatory requirements.
    c. Improve consistency in risk measurement.
    d. Highlight potential areas for mitigation.
    e. Allow comparisons among different threats, events, and potential mitigating controls.

Objective 6: Determine whether management effectively implements controls to mitigate identified risk.

1. Determine whether policies, standards, and procedures are of sufficient scope and depth to guide information security-related decisions. Review whether policies, standards, and procedures have the following characteristics:

    a. Are appropriately implemented and enforced.
    b. Delineate areas of responsibility.
    c. Are communicated in a clear and understandable manner.
    d. Are reviewed and agreed to by employees.
    e. Are appropriately flexible to address changes in the environment.

2. Determine whether the information security policy is annually reviewed and approved by the board.

3. Determine whether the institution continually assesses the capability of technology needed to sustain an appropriate level of information security based on the size, complexity, and risk appetite of the institution.

4. Determine whether management implements an integrated control system characterized by the use of different control types that mitigates identified risks. Review whether management does the following:

    a. Implements a layered control system using different controls at different points in a transaction process.
    b. Uses controls of different classifications, including preventive, detective, and corrective.
    c. Verifies that compensating controls are used appropriately to compensate for weaknesses with the system or process.

5. Determine whether management implements controls that appropriately align security with the nature of the institution’s operations and strategic direction. Specifically, review whether management does the following:

a. Implements controls based on the institution's risk assessment to mitigate risk from information security threats and vulnerabilities, such as interconnectivity risk.
b. Evaluates whether the institution has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls.
c. Reviews and improves or updates the security controls, where necessary.

6. Determine whether management effectively maintains an inventory(ies) of hardware, software, information, and connections. Review whether management does the following:

   a. Identifies assets that require protection, such as those that store, transmit, or process sensitive customer information, or trade secrets.
   b. Classifies assets appropriately.
   c. Uses the classification to determine the sensitivity and criticality of assets.
   d. Uses the classification to implement controls required to safeguard the institution's assets.
   e. Updates the inventory(ies) appropriately.

7. Determine whether management comprehensively and effectively identifies, measures, mitigates, monitors, and reports interconnectivity risk. Review whether management does the following:

   a. Identifies connections with third parties.
   b. Identifies access points and connection types that pose risk.
   c. Identifies connections between and access across low-risk and high-risk systems.
   d. Measures the risk associated with connections with third parties with remote access.
   e. Implements and assesses the adequacy of appropriate controls to ensure the security of connections.
   f. Monitors and reports on the institution's interconnectivity risk.

8. Determine whether management effectively mitigates risks posed by users. Review whether management does the following:

   a. Develops and maintains a culture that fosters responsible and controlled access for users.
   b. Establishes and effectively administers appropriate security screening in IT hiring practices.
   c. Establishes and appropriately administers a user access program for physical and logical access.
   d. Employs appropriate segregation of duties.
   e. Obtains agreements from employees, contractors, and service providers covering confidentiality, nondisclosure, and authorized use.
   f. Provides training to support awareness and policy compliance.

9. Determine whether management applies appropriate physical security controls to protect its premises and more sensitive areas, such as its data center(s).

10. Determine whether management secures access to its computer networks through multiple layers of access controls. Review whether management does the following:

    a. Establishes zones (e.g., trusted and untrusted) according to risk with appropriate access requirements within and between each zone.
    b. Maintains accurate network diagrams and data flow charts.
    c. Implements appropriate controls over wired and wireless networks.

11. Determine whether management has a process to introduce changes to the environment (e.g., configuration management of IT systems and applications, hardening of systems and applications, use of standard builds, and patch management) in a controlled manner. Determine whether management does the following:

    a. Maintains procedures to guide the process of introducing changes to the environment.
    b. Defines change requirements.
    c. Restricts changes to authorized users.
    d. Reviews the potential impact changes have on security controls.
    e. Identifies all system components affected by the changes.
    f. Develops test scripts and implementation plans.
    g. Performs necessary tests of all changes to the environment (e.g., systems testing, integration testing, functional testing, user acceptance testing, and security testing).
    h. Defines rollback procedures in the event of unintended or negative consequences with the introduced changes.
    i. Verifies the application or system owner has authorized changes in advance.
    j. Maintains strict version control of all software updates.
    k. Validates that new hardware complies with institution policies and guidelines.
    l. Verifies network devices are properly configured and function appropriately within the environment
    m. Maintains an audit trail of all changes.

12. Determine whether appropriate processes exist for configuration management (managing and controlling configurations of systems, applications, and other technology).

13. Determine whether management has processes to harden applications and systems (e.g., installing minimum services, installing necessary patches, configuring appropriate security settings, enforcing principle of least privilege, changing default passwords, and enabling logging).

14. Determine whether management uses standard builds, allowing one documented configuration to be applied to multiple computers in a controlled manner, to create hardware and software inventories, update or patch systems, restore systems, investigate anomalies, and audit configurations.

15. Determine whether management has a process to update and patch operating systems, network devices, and software applications, including internally developed software provided

to customers, for newly discovered vulnerabilities. Review whether patch management processes include the following:

a. An effective monitoring process that identifies the availability of software patches.
b. A process to evaluate the patches against the threat and network environment.
c. A prioritization process to determine which patches to apply across classes of computers and applications.
d. A process for obtaining, testing, and securely installing the patches.
e. An exception process, with appropriate documentation, for patches that an institution decides to delay or not apply.
f. A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment.
g. A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied.
h. Actions to ensure that patches do not compromise the security of the institution's systems.

16. Determine whether management plans for the life cycles of the institution's systems, eventual end of life, and any corresponding business impacts. Review whether the institution's life cycle management includes the following:

a. Maintaining inventories of systems and applications.
b. Adhering to an approved end-of-life or sunset policy for older systems.
c. Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor.
d. Planning for the update or replacement of systems nearing obsolescence.
e. Outlining procedures for the secure destruction or wiping of hard drives being returned to vendors or donated to prevent the inadvertent disclosure of sensitive information.

17. Determine whether management has implemented defense-in-depth to protect, detect, and respond to malware.

18. Determine whether management maintains policies and effectively controls and protects access to and transmission of information to avoid loss or damage. Review whether management does the following:

a. Requires secure storage of all types of sensitive information, whether on computer systems, portable devices, physical media, or hard-copy documents.
b. Establishes controls to limit access to data.
c. Requires appropriate controls over data stored in a cloud environment.
d. Implements appropriate controls over the electronic transmission of information or, if appropriate safeguards are unavailable, restricts the type of information that can be transmitted.
e. Has appropriate disposal procedures for both paper-based and electronic information.

f. Maintains the security of physical media, including backup tapes, containing sensitive information while in transit, including to off-site storage, or when shared with third parties.
g. Has policies restricting the use of unsanctioned or unapproved IT resources (e.g., online storage services, unapproved mobile device applications, and unapproved devices).

19. Determine whether management identifies factors that may increase risk from supply chain attacks and responds with appropriate risk mitigation. Review whether management implements the following as appropriate:

    a. Purchases are made only through reputable sellers.
    b. Purchases are made through a third party to shield the institution's identity.
    c. Hardware is reviewed for anomalies.
    d. Software is reviewed through both automated software testing and code reviews.
    e. Reliability of the items purchased is regularly reviewed post-implementation.

20. Determine whether management has an effective process to administer logical security access rights for the network, operating systems, applications, databases, and network devices. Review whether management has the following:

    a. An enrollment process to add new users to the system.
    b. An authorization process to add, delete, or modify authorized user access to operating systems, applications, directories, files, and specific types of information.
    c. A monitoring process to oversee and manage the access rights granted to each user on the system.
    d. A process to control privileged access.
    e. A process to change or disable default user accounts and passwords.

21. As part of management's process to secure the operating system and all system components, determine whether management does the following:

    a. Limits the number of employees with access to operating system and system utilities and grants only the minimum level of access required to perform job responsibilities.
    b. Restricts and logs access to and activity on operating system parameters, system utilities (especially those with data-altering capabilities), and sensitive system resources (including files, programs, and processes), and supplements with additional security software, as necessary.
    c. Restricts operating system access to specific terminals in physically secure and monitored locations.
    d. Secures or removes external drives and portable media from system consoles, terminals, or PCs running terminal emulations, residing outside of physically secure locations.
    e. Prohibits remote access to operating system and system utilities, where feasible, and, at a minimum, requires strong authentication and encrypted sessions before allowing such remote access.
    f. Filters and reviews logs for potential security events and provides adequate reports and alerts.

g. Independently monitors operating system access by user, terminal, date, and time of access.

22. Determine whether management controls access to applications. Review whether management does the following:

    a. Implements a robust authentication method consistent with the criticality and sensitivity of the application.
    b. Manages application access rights by using group profiles.
    c. Periodically reviews and approves the application access assigned to users for appropriateness.
    d. Communicates and enforces the responsibilities of programmers, security administrators, and application owners in maintaining effective application access control.
    e. Sets time-of-day or terminal limitations for some applications or for more sensitive functions within an application.
    f. Logs access and events, defines alerts for significant events, and develops processes to monitor and respond to anomalies and alerts.

23. Determine whether management has policies and procedures to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner. Review whether management does the following:

    a. Provides remote access in a safe and sound manner.
    b. Implements the controls necessary to offer remote access securely (e.g., disables unnecessary remote access, obtains approvals for and performs audits of remote access, maintains robust configurations, enables logging and monitoring, secures devices, restricts remote access during specific times, controls applications, enables strong authentication, and uses encryption).

24. Determine whether management effectively controls employees' use of remote devices. Review whether management does the following:

    a. Implements controls over institution owned and personally owned devices used by employees to access the network (e.g., disallows remote access without business justification, requires management approval, reviews remote access approvals, restricts access to authorized network areas, logs remote access, implements robust authentication, uses encryption, and uses application white-listing).
    b. Implements controls over remote devices provided by the institution (e.g., securely configures remote access devices, protects devices against malware, patches and updates software, encrypts sensitive data, implements secure containers, audits device access, uses remote disable and wipe capabilities, and uses geolocation).
    c. Uses an effective method to ensure personally owned devices meet defined institution security standards (e.g., such as operating system version, patch levels, and anti-malware solutions).

25. Determine whether management effectively provides secure customer access to financial services and plans for potential interruptions in service. Review whether management does the following:

    a. Develops and maintains policies and procedures to securely offer and ensure the resilience of remote financial services (e.g., using appropriate authentication, layered security controls, and fraud detection monitoring). (For additional questions, refer to the "Mobile Financial Services" examination procedures.)[65]
    b. Plans and coordinates with ISPs and third parties to minimize exposure to incidents and continue services when faced with an incident (e.g., monitors threat alerts, service availability, applications, and network traffic for indicators of nefarious activity, and ensures traffic filtering).
    c. Develops and tests a response plan in conjunction with the institution's ISPs and third-party service providers to mitigate the interruption of mobile or remote financial services.

26. Determine whether management develops customer awareness and education efforts that address both retail (consumer) and commercial account holders.

27. Determine whether management uses applications that were developed by following secure development practices and that meet a prudent level of security. Determine whether management develops security control requirements for applications, whether they are developed in-house or externally. Determine whether information security personnel are involved in monitoring the application development process to verify secure development practices. Review whether applications in use provide the following capabilities:

    a. Provide a prudent level of security (e.g., password and audit policies), audit trails of security and access changes, and user activity logs.
    b. Have user and group profiles to manage user access for applications if they are not part of a centralized identity access management system.
    c. Provide the ability to change and disable default application accounts upon installation.
    d. Allow administrators to review and install patches for applications in a timely manner.
    e. Use validation controls for data entry and data processing.
    f. Integrate additional authentication and encryption controls, as necessary.
    g. Protect web or Internet-facing applications through additional controls, including web application firewalls, regular scanning for new or recurring vulnerabilities, mitigation or remediation of common security weaknesses, and network segregation.

28. With respect to developed software, determine whether institution management does the following:

    a. Reviews mitigation of potential flaws in applications.
    b. Obtains attestation or evidence from third-party developers that the applications acquired by the institution meet the necessary security requirements and that noted vulnerabilities or flaws are remediated in a timely manner.

[65] Refer to appendix E of the *IT Handbook's* "Retail Payment Systems" booklet.

c. Performs ongoing risk assessments to consider the adequacy of application-level controls in light of changing threat, network, and host environments.
d. Implements minimum controls recommended by third-party service providers and considers supplemental controls as appropriate.
e. Reviews available audit reports, and considers and implements appropriate control recommendations.
f. Collects data to build metrics and reporting of configuration management compliance, and vulnerability management.

29. For database security, determine whether management implemented or enabled controls commensurate with the sensitivity of the data stored in or accessed by the database(s). Determine whether management appropriately restricts access and applies the rule of least privilege in assigning authorizations.

30. Determine how and where management uses encryption and if the type and strength are sufficient to protect information appropriately. Additionally, determine whether management has effective controls over encryption key management.

31. Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. Review the due diligence involved, security controls to mitigate risk, and monitoring capabilities over the institution's third parties. Review the institution's policies, standards, and procedures related to the use of the following:

    a. Third-party service providers that facilitate operational activities (e.g., core processing, mobile financial services, cloud storage and computing, and managed security services).
    b. Due diligence in research and selection of third-party service providers.
    c. Contractual assurances from third-party service providers for security responsibilities, controls, and reporting.
    d. Nondisclosure agreements with third-party service providers with access to the institution's systems and data (including before, during, and following termination of the contract).
    e. Independent review of the third-party service provider's security through appropriate reports from audits and tests.
    f. Coordination of incident response policies and contractual notification requirements.
    g. Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported.

32. If the institution outsources cloud computing or storage to a third-party service provider, refer to the FFIEC's "Outsourced Cloud Computing" statement.[66]

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

33. If the institution outsources the management of security services to a third-party service provider, refer to the information available in appendix D of the *IT Handbook's* "Outsourcing Technology Services" booklet and the related examination procedures.[67]

34. Determine whether management effectively manages the following information security considerations related to business continuity planning. Review management's ability to do the following:

    a. Identify personnel with key information security roles during a disaster and training of personnel in those roles.
    b. Define information security needs for backup sites and alternate communication networks.
    c. Develop policies that address the concepts of information security incident response and resilience and test information security incident scenarios.

35. Determine whether management has an effective log management process that involves a central logging repository, timely transmission of log files, and effective log analysis. Review whether management has the following:

    a. Log retention policies that meet incident response and analysis needs.
    b. Processes for the security and integrity of log files (e.g., encryption of log files, adequate storage capacity, secure backup and disposal of logs, logging to a separate computer, use of read-only media, controlled log parameters, and restricted access to log files).
    c. Independent review of logging practices.
    d. Processes to effectively collect, aggregate, analyze, and correlate security event information from discrete systems and applications.

Objective 7: Determine whether management has effective risk monitoring and reporting processes.

1. Determine whether the institution has risk monitoring and reporting processes that address changing threat conditions in both the institution and the greater financial industry. Determine whether these processes address information security events faced by the institution, the effectiveness of management's response, and the institution's resilience to those events. Review whether the reporting process includes a method of disseminating those reports to appropriate members of management.

2. Determine whether the risk monitoring and reporting process is regular and prompts action, when necessary, in a timely manner.

3. Determine whether program monitoring and reporting instigate appropriate changes that are effective in maintaining an acceptable level of risk.

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

4. Determine whether management develops and effectively uses metrics as part of the risk monitoring and reporting processes for the information security program. Review whether management does the following:

    a. Uses metrics that are timely, comprehensive, and actionable to improve the program's effectiveness and efficiency.
    b. Develops metrics that demonstrate the extent to which the information security program is implemented and whether the program is effective.
    c. Uses metrics to measure security policy implementation, the adequacy of security services delivery, and the impact of security events on business processes.
    d. Establishes metrics to measure conformance to the standards and procedures that are used to implement policies.
    e. Uses metrics to quantify and report risks in the information security program.

Objective 8: Determine whether management has security operations that encompass necessary security-related functions, are guided by defined processes, are integrated with lines of business and activities outsourced to third-party service providers, and have adequate resources (e.g., staff and technology).

1. Determine whether the institution's security operations activities include the following:

    a. Security software and device management (e.g., maintaining the signatures on signature-based devices and firewall rules).
    b. Forensics (e.g., analysis of potentially compromised systems).
    c. Vulnerability identification (e.g., operation or supervision of vulnerability scans, self-assessments, penetration tests, and analysis of audit results).
    d. Vulnerability cataloging and remediation tracking.
    e. Physical security management (e.g., CCTV, guards, and badge systems).
    f. Law enforcement interface (e.g., data retention and lawful intercepts).
    g. Third-party integration (e.g., managed security services and incident detection services).
    h. Monitoring of network, host, and application activity.
    i. Threat identification and assessment.
    j. Incident detection and management.
    k. Enforcement of access controls.

2. Determine whether management establishes defined processes and appropriate governance to facilitate the performance of security operations. Determine whether management coordinates security operations activities with the institution's lines of business and with the institution's third-party service providers.

3. Determine whether management has effective threat identification and assessment processes, including the following:

    a. Maintaining procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information.

b. Identifying and assessing threats (e.g., threat information is often ad hoc, although some providers present threat information within a defined framework that readily lends itself to analytical operations).
c. Using tools to assist in the analysis of vulnerabilities (e.g., design of system, operation of the system, security procedures, business line controls, and implementation of the system and controls).
d. Using threat knowledge to drive risk assessment and response.
e. Designing policies to allow immediate and consequential threats to be dealt with expeditiously.
f. Developing appropriate processes to evaluate and respond to vulnerability information from external groups or individuals.

4. Determine whether management has effective threat monitoring processes, including the following:

a. Defining threat monitoring policies that provide for both continual and ad hoc monitoring of communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal proceedings.
b. Establishing responsibility and accountability for security personnel and system administrators for monitoring.
c. Appropriately reviewing and providing approval of the monitoring tools used.
d. Monitoring of indicators, including vulnerabilities, attacks, compromised systems, and suspicious users.
e. Monitoring both incoming and outgoing network traffic to identify malicious activity and data exfiltration.
f. Establishing and documenting a process to independently monitor administrators and other users with higher privileges.

5. Determine whether management has effective incident identification and assessment processes to do the following:

a. Identify indicators of compromise.
b. Analyze the event associated with the indicators.
c. Classify the event.
d. Enable the use of response teams and responses depending on the type of event.
e. Escalate the event consistent with the classification.
f. Report internally and externally as appropriate.
g. Identify personnel empowered to declare an incident.
h. Develop procedures to test the incident escalation, response, and reporting processes.

6. Determine whether management has effective incident response processes, including the following:

a. Protocols defined in the incident response policy to declare and respond to an incident once identified.

b. Procedures to minimize damage through the containment of the incident, restoration of systems, preservation of data and evidence, and notification, as appropriate, to customers and others as needed.
c. Appropriate balance of adequate people and technologies in the response.
d. A plan that is comprehensive, coordinated, integrated, and periodically tested with appropriate internal and external parties.
e. Policies and procedures to guide the response, assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort.
f. Thresholds for reporting significant security incidents and processes to notify, as appropriate, the institution's regulators of those incidents that may affect the institution or the financial system.
g. Assignment of responsibilities, training, and testing.
h. Containment strategies.
i. Restoration and follow-up strategies.

Objective 9: Determine whether management has an effective information security program.

1. Determine whether the information security program is subject to periodic review and whether management provides for continual improvement in the program's effectiveness. Verify whether that review does the following:

    a. Addresses the program in its current environment.
    b. Demonstrates that lessons learned from experience, audit findings, and other opportunities for improvement are identified and applied.

Objective 10: Determine whether assurance activities provide sufficient confidence that the security program is operating as expected and reaching intended goals.

1. Review whether management ascertains assurance through the following:

    a. Testing and evaluations through a combination of self-assessments, penetration tests, vulnerability assessments, and audits with appropriate coverage, depth, and independence.
    b. Alignment of personnel skills and program needs.
    c. Reporting that is timely, complete, transparent, and relevant to management decisions.

2. Determine whether management considers the following key testing factors when developing and implementing independent tests:

    a. Scope.
    b. Personnel.
    c. Notifications.
    d. Confidentiality, integrity, and availability of the institution's information.
    e. Confidentiality of test plans and data.
    f. Frequency.

g. Proxy testing.

3. Determine whether management uses the following types of tests and evaluations to determine the effectiveness of the information security program. Verify whether management ensures the following are done:

   a. Periodic self-assessments performed by the organizational unit being assessed.
   b. Penetration tests that subject a system to real-world attacks and identify weaknesses.
   c. Vulnerability assessments that define, identify, and classify the security holes found in the system.
   d. Audits performed by independent internal departments or third parties.

4. Determine whether management uses independent organizations to test aspects of its information security programs.

5. Determine whether management uses reporting of the results of self-assessments, penetration tests, vulnerability assessments, and audits to support management decision making.

6. Determine whether the annual information security report is timely and contains adequate information.

Objective 11: Discuss corrective action and communicate findings.

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

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

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

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

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

Appendix B: Glossary

Acceptable use policy: A document that establishes an agreement between users and the enterprise and defines for all parties the ranges of use that are approved before users can gain access to a network or the Internet.

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

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

Air-gapped environment: Security measure that isolates a secure network from unsecure networks physically, electrically, and electromagnetically.

Anomalous activity: Activity that deviates from normal. The result of the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.

Antivirus/anti-malware software: A program that monitors a computer or network to identify all types of malware and prevent or contain malware incidents.

Asset: In computer security, a major application, a general-support system, a high-impact program, a physical plant, a mission-critical system, personnel, equipment, or a logically related group of systems.

Attack signature: A specific sequence of events indicative of an unauthorized access attempt.

Authentication: The process of verifying the identity of an individual user, machine, software component, or any other entity.

Availability: Whether or how often a system is available for use by its intended users. Because downtime is usually costly, availability is an integral component of security.

Baseline configuration: A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time and that can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, or changes.

Black holing: A method typically used by ISPs to stop a distributed denial-of-service (DDoS) attack on one of its customers. This approach to blocking DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic.

Border router: A device located at the organization’s boundary to an external network.

Change management: The broad processes for managing organizational change. Change management encompasses planning, oversight or governance, project management, testing, and implementation.

Checksum: A mathematical value that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously or erroneously changed.

Classification: Categorization (e.g., "confidential," "sensitive," or "public") of the information processed by the service provider on behalf of the receiver company.

Cloud computing: Generally a migration from owned resources to shared resources in which client users receive IT services on demand from third-party service providers via the Internet "cloud." In cloud environments, a client or customer relocates its resources—such as data, applications, and services—to computing facilities outside the corporate firewall, which the end user then accesses via the Internet.

Cloud storage: A model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.

Compensating control: A management, operational, and/or technical control (e.g., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

Computer security: Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

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

Configuration management: The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, testing, test fixtures, and test documentation throughout the development and operational life of the system.

Consumer information: For purposes of the Information Security Standards, "consumer information" means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report that is maintained by or on behalf of a financial institution for a business purpose, such as information that an institution obtains about a loan applicant or a prospective employee from a consumer report.

Control: The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature.

Control requirements: Process used to document and/or track internal processes to determine that those established procedures and/or physical security policies are being followed.

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

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

Crisis management: The process of managing an institution's operations in response to an emergency or event that threatens business continuity. An institution's ability to communicate with employees, customers, and the media, using various communications devices and methods, is a key component of crisis management.

Critical system (infrastructure): The systems and assets, whether physical or virtual, that are so vital that the incapacity or destruction of them may have a debilitating impact.

Customer: For purposes of the Information Security Standards, "customer" means a consumer with whom a financial institution has a continuing relationship under which the institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes. In the case of a credit union, a customer relationship will exist between a credit union and certain consumers that are not the credit union's members.

Customer information: A term used in the Information Security Standards to mean any record containing non-public personal information about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of a financial institution.

Customer information systems: For purposes of the Information Security Standards, "customer information systems" means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

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

Cyber event: A cybersecurity change or occurrence that may have an impact on organizational operations (including mission, capabilities, or reputation).

Cyber incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

Cyber resilience: The ability of a system or domain to withstand cyber attacks or failures and, in such events, to reestablish itself quickly.

Cyber threat: An internal or external circumstance, event, action, occurrence, or person with the potential to exploit technology-based vulnerabilities and to adversely affect (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

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

Data classification program: A program that categorizes data to convey required safeguards for information confidentiality, integrity, and availability, and establishes required controls based on value and level of sensitivity.

Data corruption: Errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data.

Data integrity: The property that data have not been destroyed or corrupted in an unauthorized manner; maintaining and assuring the accuracy and consistency of data over their entire life cycle.

Data loss prevention (DLP) program: A comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data while it is stored, used, or in transit over the network and at the perimeter.

Database: A collection of data that is stored on any type of computer storage medium and may be used for more than one purpose.

Defense-in-depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

Demilitarized zone (DMZ): A computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

Detection device: A device designed to recognize an event and alert management when events occur.

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

Device: A generic term for any machine or component that attaches to a computer or connects to a network.

Distributed denial of service (DDoS): A type of attack that makes a computer resource or resources unavailable to its intended users. Although the means to carry out, motives for, and

targets of a DDoS attack may vary, it generally consists of the concerted efforts of a group that intends to affect an institution's reputation by preventing an Internet site, service, or application from functioning efficiently.

Due diligence for service provider selection: Technical, functional, and financial review to verify a third-party service provider's ability to deliver the requirements specified in its proposal. The intent is to verify that the service provider has a well-developed plan and adequate resources and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

End-of-life: All software products have life cycles. End-of-life refers to the date when a software development company no longer provides automatic fixes, updates, or online technical assistance for the product.

End-point security: Refers to a methodology of protecting the corporate network when accessed with remote devices, such as laptops, or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry (or exit) point for security threats.

End-to-end process flow: Document that details the flow of the processes, considering automated and manual control points, hardware, databases, network protocols, and real-time versus periodic processing characteristics.

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

Exploit: A technique or code that uses a vulnerability to provide system access to the attacker. An exploit is an intentional attack to affect an operating system or application program.

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

File transfer protocol (FTP): A standard high-level protocol for transferring files from one computer to another, usually implemented as an application-level program.

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

Firewall: A hardware or software link in a network that relays only data packets clearly intended and authorized to reach the other side.

Frame relay: A high-performance wide area network protocol that operates at the physical and data link layers of the Open Systems Interconnection reference model. Frame relay is an example

of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth.

Governance: In computer security, governance means setting clear expectations for the conduct (behaviors and actions) of the entity being governed and directing, controlling, and strongly influencing the entity to achieve these expectations. Governance includes specifying a framework for decision making, with assigned decision rights and accountability, intended to consistently produce desired behaviors and actions.

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

Hardening: The process of securing a computer's administrative functions or inactivating those features not needed for the computer's intended business purpose.

Hardware: The physical elements of a computer system; the computer equipment as opposed to the programs or information stored in a machine.

Hash: A fixed-length cryptographic output of variables, such as a message, being operated on by a formula or cryptographic algorithm.

Hijacking: An attacker's use of an authenticated user's communication session to communicate with system components.

Homing beacons: Devices that send messages to the institution when they connect to a network and that enable recovery of the device.

Host: A computer that is accessed by a user from a remote location.

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

Incident response plan: A plan that defines the action steps, involved resources, and communication strategy upon identification of a threat or potential threat event, such as a breach in security protocol, power or telecommunications outage, severe weather, or workplace violence.

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

Information systems: Electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information systems can include networks (computer systems, connections to business partners and the Internet, and the

interconnections between internal and external systems). Other examples are backup tapes, mobile devices, and other media.

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

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

Integrity: Assurance that information is trustworthy and accurate; ensuring that information will not be accidentally or maliciously altered or destroyed (see "Data integrity").

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

Interdependencies: When two or more departments, processes, functions, or third-party service providers support one another in some fashion.

Internal "trusted" zone: A channel in which the end points are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include SSLIP security and a secure physical connection.

International Organization for Standardization (ISO): An independent, non-governmental, international organization that brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards.

Internet: The global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide.

Internet service provider (ISP): A company that provides its customers with access to the Internet (e.g., AT&T, Verizon, and CenturyLink).

Intrusion detection: Techniques that attempt to detect unauthorized entry or access into a computer or network by observation of actions, security logs, or audit data; detection of break-ins or attempts, either manually or via software expert systems that operate on logs or other information available on the network.

Intrusion detection system (IDS): Software or hardware product that detects and logs inappropriate, incorrect, or anomalous activity. It gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations). IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

Intrusion prevention system (IPS): A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its target.

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

Life-cycle process: The multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system.

Log: A record of information or events in an organized system, usually sequenced in the order in which the events occurred.

Logical access: Ability to interact with computer resources granted using identification, authentication, and authorization.

Logical access controls: The policies, procedures, organizational structure, and electronic access controls designed to restrict access to computer software and data files.

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

Media: Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks.

Metric: A quantitative measurement.

Middleware: Software that connects two or more software components or applications. It is another term for an application programmer interface or API, and it allows programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services.

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

Multi-factor authentication: The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number); something you have (e.g., cryptographic identification device or token); and something you are (e.g., biometric).

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

Network: Two or more computer systems grouped together to share information, software, and hardware.

Network activity baseline: A base for determining typical utilization patterns so that significant deviations can be detected.

Network administrator: The individual responsible for the installation, management, and control of a network.

Network diagram: A description of any kind of locality in terms of its physical layout. In the context of communication networks, a topology describes pictorially the configuration or arrangement of a network, including its nodes and connecting communication lines.

Network security: The protection of computer networks and their services from unauthorized entry, modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and that there are no harmful side effects. Network security includes providing for data integrity.

Non-public personal information: For purposes of the Information Security Standards, non-public personal information means (i) “personally identifiable financial information”; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any “personally identifiable financial information” that is not publicly available.

Non-repudiation: Ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

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

Out-of-band: Activity outside of the primary means of interfacing with the customer. For example, if a user is performing activity online, he or she may be authenticated through a one-time password sent via text message.

Outsourcing: The practice of contracting with another entity to perform services that might otherwise be conducted in-house; a contractual relationship with a third party to provide services, systems, or support.

Packet: The data unit that is routed from source to destination in a packet-switched network.

Patch: Software code that replaces or updates other code. Patches frequently are used to correct security flaws.

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

Personally identifiable financial information: For purposes of the Information Security Standards, personally identifiable financial information means information (i) a consumer provides to a financial institution to obtain a financial product or service; (ii) about a consumer resulting from any transaction involving a financial product or service between the financial institution and a consumer; or (iii) that a financial institution otherwise obtains about a consumer in connection with providing a financial product or service, such as account balance information, payment history, overdraft history, and credit or debit card purchase information; or the fact that an individual is one of the financial institution's customers.

Phishing: A digital form of social engineering that uses authentic-looking—but bogus—e-mail to request information from users or direct them to fake websites that request information.

Policy: A document that records a high-level principle or an agreed-upon course of action; overall intention and direction as formally expressed by management.

Port: Either an end point to a logical connection or a physical connection to a computer.

Positive pay: A technique that can reduce check fraud by requesting businesses to send electronic files of information to the financial institution on all checks the business has issued.

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

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

Privilege: The level of trust with which a system object is imbued.

Privileged access: Individuals with the ability to override system or application controls.

Protocol: A format for transmitting data between devices.

Real-time network monitoring: Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.

Remote access: The ability to obtain access to a computer or network from a remote location.

Remote deletions: Use of a technology to remove data from a portable device without touching the device.

Removable media: Portable electronic storage media, such as magnetic, optical, and solid-state devices that can be inserted into and removed from a computing device and that are used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, pen drives, and similar storage devices.

Resource: Any enterprise asset that can help the organization achieve its objectives.

Retention requirement: Requirement established by a company or by regulation for the length of time and/or for the amount of information that should be retained.

Risk analysis: The process of identifying risks, determining their probability and impact, and identifying areas needing safeguards.

Risk assessment: A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.

Rogue wireless access: An unauthorized wireless node on a network.

Routing: The process of moving information from its source to the destination.

Sandbox: A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

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

Secure shell: Network protocol that uses cryptography to secure communication, remote command line log-in, and remote command execution between two networked computers.

Secure Sockets Layer (SSL): A protocol that is used to transmit private documents through the Internet.

Security architecture: A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

Security audit: An independent review and examination of system records and activities to test for adequacy of system controls, ensure compliance with established policy and operational procedures, and recommend any indicated changes in control, policy, and procedures.

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

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

Security log: A record that contains log-in and logout activity and other security-related events and that is used to track security-related information on a computer system.

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

Security violation: An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information or system resources.

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

Server: A computer or other device that manages a network service. An example is a print server, which is a device that manages network printing.

Service level agreement (SLA): Formal documents between an institution and its third-party service provider that outline an institution's predetermined requirements for a service and establish incentives to meet, or penalties for failure to meet, the requirements. SLAs should specify and clarify performance expectations, establish accountability, and detail remedies or consequences if performance or service quality standards are not met.

Service provider: For purposes of the Information Security Standards, service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through its provision of services directly to a financial institution.

Shadow IT: A term used to describe IT systems or applications used inside institutions without explicit approval.

Sniffing: The passive interception of data transmissions.

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

Spear phishing: An attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into the targeted network.

Spoofing: A form of masquerading in which a trusted IP address is used instead of the true IP address as a means of gaining access to a computer system.

SQL Injection Attack: An exploit of target software that constructs structured query language (SQL) statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended. SQL injection enables an attacker to talk directly to the database, thus bypassing the application completely. Successful injection can cause information disclosure as well as the ability to add or modify data in the database.

Stateful inspection: A firewall inspection technique that examines the claimed purpose of a communication for validity. For example, a communication claiming to respond to a request is compared to a table of outstanding requests.

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

System resources: Capabilities that can be accessed by a user or program either on the user's machine or across the network. Capabilities can be services, such as file or print services, or devices, such as routers.

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

Third-party service provider: Any third party to whom a financial institution outsources activities that the institution itself is authorized to perform, including a technology service provider.

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

Trojan horse: Malicious code hidden in software that has an apparently beneficial or harmless use.

Tunnel: The path that encapsulated packets follow in an Internet VPN.

U.S. Computer Emergency Readiness Team (US-CERT): US-CERT is part of the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center in the Office of Cybersecurity and Communications. US-CERT is a partnership between the Department of Homeland Security and the public and private sectors, established to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation.

User identification: The process, control, or information by which a user identifies himself or herself to the system as a valid user (as opposed to authentication).

Utility: A program used to configure or maintain systems, or to make changes to stored or transmitted data.

Virtual local area network (VLAN): Logical segmentation of a LAN into different broadcast domains.

Virtual machine: A software emulation of a physical computing environment.

Virtual private network (VPN): A computer network that uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Virus: Malicious code that replicates itself within a computer.

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

Vulnerability assessment: Systematic examination of systems to identify, quantify, and prioritize the security deficiencies of the systems.

Worm: A self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network), possibly without any user intervention. This occurs primarily because of security vulnerabilities on the target computers.

Zero-day attack: An attack on a piece of software that has a vulnerability for which there is no known patch.

Appendix C: Laws, Regulations, and Guidance

Laws

12 USC 1861–1867, “Bank Service Company Act”
12 USC 1882, “Bank Protection Act”
15 USC 1681w, “Fair and Accurate Credit Transactions Act”
15 USC 6801 and 6805(b), “Gramm–Leach–Bliley Act”
18 USC 1030, “Fraud and Related Activity in Connection With Computers”

Consumer Financial Protection Bureau

Regulations

12 CFR 1005, “Electronic Fund Transfers (Regulation E)”
12 CFR 1016, “Privacy of Consumer Financial Information (Regulation P)”

Federal Deposit Insurance Corporation

Regulations

12 CFR 326, subpart A, “Minimum Security Procedures”
12 CFR 326, subpart B, “Procedures for Monitoring Bank Secrecy Act Compliance”
12 CFR 332, “Privacy of Consumer Financial Information”
12 CFR 353, “Suspicious Activity Reports”
12 CFR 364, appendix A, “Interagency Guidelines Establishing Standards for Safety and Soundness”
12 CFR 364, appendix B, “Interagency Guidelines Establishing Information Security Standards”

Guidance

FIL-28-2015, “Cybersecurity Assessment Tool” (July 2, 2015)
FIL-13-2015, “FFIEC Joint Statements on Destructive Malware and Compromised Credentials” (March 30, 2015)
FIL-9-2015, “Business Continuity Planning Booklet Appendix J Update to FFIEC IT Examination Handbook Series” (February 23, 2015)
FIL-49-2014, “Technology Alert GNU Bourne-Again Shell (Bash) Vulnerability” (September 29, 2014)
FIL-16-2014, “Technology Alert OpenSSL Heartbleed Vulnerability” (April 11, 2014)
FIL-11-2014, “Distributed Denial of Service (DDoS) Attacks” (April 2, 2014)
FIL-10-2014, “ATM and Card Authorization Systems” (April 2, 2014)
FIL-50-2011, “FFIEC Supplement to Authentication in an Internet Banking Environment” (June 29, 2011)

FIL-56-2010, “Guidance on Mitigating Risk Posed by Information Stored on Photocopiers, Fax Machines and Printers” (September 15, 2010)
FIL-6-2010, “Retail Payment Systems Booklet” (February 25, 2010)
FIL-30-2009, “Identity Theft Red Flags, Address Discrepancies, and Change of Address Regulations Frequently Asked Questions” (June 11, 2009)
FIL-105-2008, “Identity Theft Red Flags, Address Discrepancies, and Change of Address Regulations Examination Procedures” (October 16, 2008)
FIL-100-2007, “Identity Theft Red Flags—Interagency Final Regulation and Guidelines” (November 15, 2007)
FIL-32-2007, “FDIC’s Supervisory Policy on Identity Theft” (April 11, 2007)
FIL-77-2006, “Authentication in an Internet Banking Environment Frequently Asked Questions” (August 21, 2006)
FIL-103-2005, “FFIEC Guidance Authentication in an Internet Banking Environment” (October 12, 2005)
FIL-69-2005, “Guidance on the Security Risks of Voice Over Internet Protocol (VoIP)” (July 27, 2005)
FIL-66-2005, “Spyware—Guidance on Mitigating Risks From Spyware” (July 22, 2005)
FIL-64-2005, “Pharming”—Guidance on How Financial Institutions Can Protect Against Pharming Attacks” (July 18, 2005)
FIL-59-2005, “Identity Theft Study Supplement on ‘Account Hijacking Identity Theft’” (July 5, 2005)
FIL-27-2005, “Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice” (April 1, 2005)
FIL-7-2005, “Fair and Accurate Credit Transactions Act of 2003 Guidelines Requiring the Proper Disposal of Customer Information” (February 2, 2005)
FIL-132-2004, “Identity Theft Study on ‘Account Hijacking’ Identity Theft and Suggestions for Reducing Online Fraud” (December 14, 2004)
FIL-121-2004, “Computer Software Due Diligence—Guidance on Developing an Effective Software Evaluation Program to Assure Quality and Regulatory Compliance” (November 16, 2004)
FIL-114-2004, “Risk Management of Free and Open Source Software FFIEC Guidance” (October 21, 2004)
FIL-103-2004, “Interagency Informational Brochure on Internet ‘‘Phishing’ Scams” (September 13, 2004)
FIL-84-2004, “Guidance on Instant Messaging” (July 21, 2004)
FIL-62-2004, “Guidance on Developing an Effective Computer Virus Protection Program” (June 7, 2004)
FIL-27-2004, “Guidance on Safeguarding Customers Against E-Mail and Internet Related Fraud Schemes” (March 12, 2004)
FIL-63-2003, “Guidance on Identity Theft Response Programs” (August 13, 2003)
FIL-43-2003, “Guidance on Developing an Effective Software Patch Management Program” (May 29, 2003)
FIL-30-2003, “Federal Bank and Credit Union Regulatory Agencies Jointly Issue Guidance on the Risks Associated With Weblinking” (April 23, 2003)
FIL-8-2002, “Wireless Networks and Customer Access” (February 1, 2002)
FIL-69-2001, “Authentication in an Electronic Banking Environment” (August 24, 2001)

FIL-68-2001, “501(b) Examination Guidance” (August 24, 2001)
FIL-39-2001, “Guidance on Identity Theft and Pretext Calling” (May 9, 2001)
FIL-22-2001, “Security Standards for Customer Information” (March 14, 2001)
FIL-77-2000, “Bank Technology Bulletin: Protecting Internet Domain Names” (November 9, 2000)
FIL-67-2000, “Security Monitoring of Computer Networks” (October 3, 2000)
FIL-68-99, “Risk Assessment Tools and Practices” (July 7, 1999)
FIL-98-98, “Pretext Phone Calling” (September 2, 1998)
FIL-131-97, “Security Risks Associated With the Internet” (December 18, 1997)
FIL-124-97, “Suspicious Activity Reporting” (December 5, 1997)
FIL-82-96, “Risks Involving Client/Server Computer Systems” (October 8, 1996)

Federal Reserve

Regulations

12 CFR 208.61, “Minimum Security Devices and Procedures”
12 CFR 208.62, “Reports of Suspicious Activities”
12 CFR 208.63, “Procedures for Monitoring Bank Secrecy Act Compliance”
12 CFR 208, appendix D-1, “Interagency Guidelines Establishing Standards for Safety and Soundness”
12 CFR 208, appendix D-2, “Interagency Guidelines Establishing Information Security Standards”
12 CFR 211.5(l), “Interagency Guidelines Establishing Information Security Standards”
12 CFR 211.9, “Interagency Guidelines Establishing Standards for Safeguarding Customer Information”
12 CFR 211.24(i), “Interagency Guidelines Establishing Information Security Standards”
12 CFR 225, appendix F, “Interagency Guidelines Establishing Information Security Standards”

Guidance

SR Letter 15-9, “FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors”
SR Letter 05-19, “Interagency Guidance on Authentication in an Internet Banking Environment”
SR Letter 04-17, “FFIEC Guidance on the Use of Free and Open Source Software”
SR Letter 04-14, “FFIEC Brochure With Information on Internet ‘Phishing’”
SR Letter 02-18, “Section 312 of the USA Patriot Act—Due Diligence for Correspondent and Private Banking Accounts”
SR Letter 02-6, “Information Sharing Pursuant to Section 314(b) of the USA Patriot Act”
SR Letter 01-15, “Safeguarding Customer Information”
SR Letter 01-11, “Identity Theft and Pretext Calling”
SR Letter 00-17, “Guidance on the Risk Management of Outsourced Technology Services”
SR Letter 00-04, “Outsourcing of Information and Transaction Processing”
SR Letter 99-08, “Uniform Rating System for Information Technology”

SR Letter 97-32, “Sound Practices Guidance for Information Security for Networks”

National Credit Union Administration

Regulations

12 CFR 716, “Privacy of Consumer Financial Information & Appendix”
12 CFR 721, “Federal Credit Union Incidental Powers Activities”
12 CFR 741, “Requirements for Insurance”
12 CFR 748, “Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance & Appendices”

Guidance

NCUA Letter to Credit Unions 05-CU-20, “Phishing Guidance for Credit Unions and Their Members”
NCUA Letter to Credit Unions 05-CU-18, “Guidance on Authentication in Internet Banking Environment” (November 2005)
NCUA Letter to Credit Unions 04-CU-12, “Phishing Guidance for Credit Union Members” (September 2004)
NCUA Letter to Credit Unions 04-CU-06, “E-Mail and Internet Related Fraudulent Schemes Guidance” (May 2004)
NCUA Letter to Credit Unions 04-CU-05, “Fraudulent E-Mail Schemes” (May 2004)
NCUA Letter to Credit Unions 03-CU-14, “Computer Software Patch Management” (September 2003)
NCUA Letter to Credit Unions 03-CU-12, “Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to Be Credit Unions” (August 2003)
NCUA Letter to Credit Unions 03-CU-08, “Weblinking: Identifying Risks & Risk Management Techniques” (April 2003)
NCUA Letter to Credit Unions 03-CU-03, “Wireless Technology” (March 2003)
NCUA Letter to Credit Unions 02-CU-13, “Vendor Information Systems & Technology Reviews—Summary Results” (July 2002)
NCUA Letter to Federal Credit Unions 02-FCU-11, “Tips to Safely Conduct Financial Transactions Over the Internet—An NCUA Brochure for Credit Union Members” (July 2002)
NCUA Letter to Credit Unions 02-CU-08, “Account Aggregation Services” (April 2002)
NCUA Letter to Federal Credit Unions 02-FCU-04, “Weblinking Relationship” (March 2002)
NCUA Letter to Credit Unions 01-CU-21, “Disaster Recovery and Business Resumption Contingency Plans” (December 2001)
NCUA Letter to Credit Unions 01-CU-20, “Due Diligence Over Third-Party Service Providers” (November 2001)
NCUA Letter to Credit Unions 01-CU-12, “E-Commerce Insurance Considerations” (October 2001)

NCUA Letter to Credit Unions 01-CU-11, “Electronic Data Security Overview” (August 2001)
NCUA Letter to Credit Unions 01-CU-10, “Authentication in an Electronic Banking Environment” (August 2001)
NCUA Letter to Credit Unions 01-CU-09, “Identity Theft and Pretext Calling” (September 2001)
NCUA Regulatory Alert 01-RA-03, “Electronic Signatures in Global and National Commerce Act (E-Sign Act)” (March 2001)
NCUA Letter to Credit Unions 01-CU-04, “Integrating Financial Services and Emerging Technology” (March 2001)
NCUA Letter to Credit Unions 01-CU-02, “Privacy of Consumer Financial Information” (February 2001)
NCUA Letter to Credit Unions 00-CU-11, “Risk Management of Outsourced Technology Services (With Enclosure)” (December 2000)
NCUA Letter to Credit Unions 00-CU-07, “NCUA’s Information Systems & Technology Examination Program” (October 2000)
NCUA Letter to Credit Unions 00-CU-04, “Suspicious Activity Reporting” (June 2000)
NCUA Letter to Credit Unions 00-CU-02, “Identity Theft Prevention” (May 2000)
NCUA Regulatory Alert 99-RA-3, “Pretext Phone Calling by Account Information Brokers” (February 1999)
NCUA Regulatory Alert 98-RA-4, “Interagency Guidance on Electronic Financial Services and Consumer Compliance” (July 1998)
NCUA Letter to Credit Unions 97-CU-05, “Interagency Statement on Retail On-Line PC Banking” (April 1997)
NCUA Letter to Credit Unions 97-CU-01, “Automated Response System Controls” (January 1997)
NCUA Letter to Credit Unions 109, “Information Processing Issues” (September 1989)

Office of the Comptroller of the Currency

Regulations

12 CFR 21, subpart A, “Minimum Security Devices and Procedures”
12 CFR 21, subpart B, “Reports of Suspicious Activities”
12 CFR 21, subpart C, “Procedures for Monitoring Bank Secrecy Act Compliance”
12 CFR 30, appendix A, “Interagency Guidelines Establishing Standards for Safety and Soundness”
12 CFR 30, appendix B, “Interagency Guidelines Establishing Information Security Standards”
12 CFR 41.83, “Proper Disposal of Records Containing Customer Information”

Guidance

OCC Bulletin 2016-18, “Cybersecurity of Interbank Messaging and Wholesale Payment Networks: FFIEC Statement” (June 7, 2016)

OCC Bulletin 2016-14, “FFIEC Information Technology Examination Handbook: Mobile Financial Services, New Appendix to the Retail Payment Systems Booklet” (April 29, 2016)
OCC Bulletin 2015-44, “FFIEC Information Technology Examination Handbook: Revised Management Booklet” (November 10, 2015)
OCC Bulletin 2015-40, “Cybersecurity: Joint Statement on Cyber Attacks Involving Extortion” (November 3, 2015)
OCC Bulletin 2015-31, “FFIEC Cybersecurity Assessment Tool” (June 30, 2015)
OCC Bulletin 2015-20, “Cybersecurity: Destructive Malware Joint Statement” (March 30, 2015)
OCC Bulletin 2015-19, “Cybersecurity: Cyber Attacks Compromising Credentials Joint Statement” (March 30, 2015)
OCC Bulletin 2015–9, “FFIEC Information Technology Examination Handbook: Strengthening the Resilience of Outsourced Technology Services, New Appendix for Business Continuity Planning Booklet” (February 6, 2015)
OCC Bulletin 2014-53, “Cybersecurity Assessment General Observations and Statement” (November 3, 2014)
OCC Bulletin 2014-17, “Information Security Vulnerability in OpenSSL Encryption Tool (Heartbleed): Joint Statement” (April 25, 2014)
OCC Bulletin 2014-14, “Distributed Denial-of-Service Cyber Attacks, Risk Mitigation, and Additional Resources: Joint Statement” (April 3, 2014)
OCC Bulletin 2014-13, “Cyber Attacks on Financial Institutions’ Automated Teller Machine and Card Authorization Systems: Joint Statement” (April 2, 2014)
OCC Bulletin 2013-29, “Third-Party Relationships: Risk Management Guidance” (October 30, 2013)
OCC Bulletin 2013-22, “Windows XP Operating System: Joint Statement” (October 7, 2013)
OCC Bulletin 2011-26, “Authentication in an Internet Banking Environment: Supplement” (June 28, 2011)
OCC Bulletin 2008-16, “Information Security: Application Security” (May 8, 2008)
OCC Bulletin 2007-45, “Identity Theft Red Flags and Address Discrepancies: Final Rulemaking” (November 14, 2007)
OCC Bulletin 2005-35, “Authentication in an Internet Banking Environment: Interagency Guidance” (October 12, 2005)
OCC Bulletin 2005-24, “Threats From Fraudulent Bank Web Sites: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents” (July 1, 2005)
OCC Bulletin 2005-13, “Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance: Interagency Guidance” (April 14, 2005)
OCC Bulletin 2005-1, “Proper Disposal of Consumer Information: Final Rule” (January 12, 2005)
OCC Bulletin 2001-35, “Examination Procedures to Evaluate Compliance With the Guidelines to Safeguard Customer Information: Examination Procedures” (July 18, 2001)
OCC Bulletin 2001-8, “Guidelines Establishing Standards for Safeguarding Customer Information: Final Guidelines” (February 15, 2001)
OCC Bulletin 2000-14, “Infrastructure Threats—Intrusion Risks: Message to Bankers and Examiners” (May 15, 2000)

OCC Bulletin 1999-20, “Certificate Authority Systems: Guidance for Bankers and Examiners” (May 4, 1999)
OCC Bulletin 1998-3, “Technology Risk Management: Guidance for Bankers and Examiners” (February 4, 1998)
OCC Alert 2001-4, “Network Security Vulnerabilities” (April 24, 2001)
OCC Alert 2000-9, “Protecting Internet Addresses of National Banks” (July 19, 2000)

Other References

Basel Committee on Banking Supervision, “Sound Practices for the Management and Supervision of Operational Risk” (February 2003)
ISACA Control Objectives for Enterprise IT Governance