EM-31.7

Category: **Board & Management Operations**
Topic: **Information Technology & Security**
Published: 1/17/2025

Overview

The *Information Technology & Security* topic provides guidance on evaluating the effectiveness of a Farm Credit System (System) institution's information technology (IT) and security processes to determine if sufficient internal controls are in place to support critical business functions and protect information assets. IT operations are the use of computers, networks, applications, databases, and other electronic devices to create, process, store, and use various forms of electronic data to support critical business functions. 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. Cybersecurity is the process of protecting information assets and data by preventing, detecting, and responding to cyberattacks. Development and acquisition include creating, procuring, or changing software, hardware, and tools that support critical business functions. Payment systems are the mechanism, rules, institutions, people, markets, and agreements that make the exchange of payments possible. Electronic commerce (e-commerce) is the use of technology for business purposes. Adequate governance, risk management, and controls over IT operations and security is imperative.

FCA's procedures and processes for examining IT and security in System institutions incorporate the guidance published by the Federal Financial Institutions Examination Council (FFIEC) in the IT Examination Handbook InfoBase (IT Handbook). The IT Handbook is a series of booklets that cover various IT subject areas. The FFIEC maintains the IT Handbook, and it revises the individual booklets periodically to reflect changes in the IT industry and federal regulatory guidance. FCA's guidance below includes content, references, and links to the applicable FFIEC IT booklets and is applicable to all banks, associations, and service corporations. The formality and complexity of an institution's IT and security program depends on the institution's size, staffing, complexity of operations, scope of IT activities, and business risk profile. Additionally, System institutions often outsource various IT activities and services. Examiner application of this guidance should be differentiated based on these factors. Examiners can also refer to the National Institute of Standards and Technology for additional guidance and as an example of industry standards.

Examination Procedures and Guidance

General

1. Governance & Management:

Evaluate the adequacy of overall governance and management of IT operations and security activities.

Guidance:

Governance and management refer to how an institution directs and controls its operations and performance. IT governance refers to how an institution directs and controls its IT operations and security services, infrastructure, and environment to support the institution and help achieve its strategic goals and objectives. IT management refers to the day-to-day direction and control of IT operations and security assets and processes. This includes basic management functions, such as staffing (including outsourcing), training, budgeting, and reporting related to IT operations and security.

As part of IT governance, the board and management need to establish and maintain an effective internal control culture and framework. The governance structure specifies the responsibilities of the board, executive and IT management, audit, and other staff. It also specifies the level of authority and accountability for decision-making, and it includes mechanisms for monitoring actions and decisions across the institution. Ultimately, the board sets the tone and direction for an institution's use of technology (see the *Governing IT activities* section in The Director's Role). The board and management should create an IT governance framework by integrating technology into the institution's strategic plan, developing applicable policies and procedures, and establishing an internal control system to safeguard data and other critical assets. Since IT supports most aspects of an institution's business, effective IT risk management practices are necessary no matter the institution's size or complexity. As part of IT risk management, management should complete a risk assessment to identify potential risks to institution information and information systems, the probability that these risks will occur, and the expected loss if these potential risks become reality. Based on the risk assessment, management can determine how best to mitigate known risks, formulate appropriate policies and procedures, and implement controls. The formality of the IT plan, policies, and risk management practices should be commensurate with the institution's business model, size, risk profile, and complexity.

Refer to the FFIEC Management booklet for additional background and examination guidance on IT governance and management, including board of directors oversight and IT management.

Evaluative questions and items to consider when examining the governance and management of IT and security activities include:

- ***IT Staffing and Structure:*** **Has management adequately staffed the IT function with the necessary skills and competencies? Is the staffing structure appropriate for the complexity of IT operations and the security program?** IT staff need to possess and maintain the necessary skills and competencies to carry out effective IT security and operations. The human resource department should have the ability to attract and retain a competent IT workforce. The IT program structure should be commensurate with the complexities of IT and security operations. Refer to the FFIEC Management, Information Security, and Architecture, Infrastructure, and Operations booklets for additional guidance on IT governance, personnel, and key roles and responsibilities.

- ***IT Risk Management:*** **Have the board and management established an effective IT risk management program?** FCA Regulation 609.905 requires the institution to engage in appropriate risk management practices (including cyber risk management). An effective IT risk management (ITRM) program includes four risk activities: 1) identification, 2) measurement, 3) mitigation, and 4) monitoring and reporting. FCA Regulation 609.905 also requires the board and management to maintain and document effective policies,

procedures, and controls to mitigate cyber risks. The ITRM program's formality should be based on the complexity of the institution and its IT operations. The ITRM program should align IT and overall business objectives and allow for flexibility to adapt to changes in the IT environment. As part of the risk management process, the board and management need to determine the organization's risk appetite related to IT. Specifically, determining the amount of risk they will accept to conduct ongoing operations and achieve strategic objectives. The board must review and approve the ITRM program (including cyber risk management) at least annually. Refer to the FFIEC Management booklet for additional guidance on ITRM. The ITRM program (including cyber risk management) must include documented processes for the following risk activities:

- *Identification* – FCA Regulations 609.930(c)(1) and (c)(1)(i) require an annual risk assessment that identifies and assesses the internal and external factors that could result in unauthorized disclosure, misuse, alteration, or destruction of current, former, and potential customer and employee information or information systems. The risk identification process should be coordinated and consistent throughout the institution. Management should maintain inventories of IT assets and systems (e.g., hardware, software, information, payment systems), event classes (e.g., natural disaster, cyber, insider abuse or compromise), threats (e.g., theft, malware, social engineering), and existing controls as an important part of effective risk identification. Inventories should also include systems and information hosted or maintained by third parties. FCA Regulation 609.930(c)(2) requires the institution to identify systems and software vulnerabilities. Refer to the FFIEC Management; Information Security; Architecture, Infrastructure, and Operations; and Development, Acquisition, and Maintenance booklets for additional guidance on risk identification considerations.

- *Measurement* – FCA Regulation 609.930(c)(1)(ii) requires the risk assessment to assess the sufficiency of policies, procedures, internal controls, and other practices in place to mitigate risks. The risk measurement process should measure identified risk using a qualitative, quantitative, or hybrid method. The process should recognize interrelated risks and prioritize risks based on the risk measurement results. Measurement is helpful in estimating the likelihood of an adverse event and its potential impact across the institution. FCA Regulation 609.930(c)(2) requires the institution to prioritize the vulnerabilities and the affected systems based on risk. There are various techniques to measure risk, including using applications. Refer to the FFIEC Management; Information Security; Architecture, Infrastructure, and Operations; and Development, Acquisition, and Maintenance booklets for additional guidance on risk measurement considerations.

- *Mitigation* – Risk mitigation is the process of reducing risk through specific controls and risk transfer practices to align the level of risk with the risk appetite. FCA Regulation 609.930(c)(2) requires the institution to perform timely remediation. The particular security measures an institution adopts will depend upon the size, risk profile, and complexity of the institution's operations and activities. Controls are implemented within institution activities and may be performed either manually by staff or through automated systems. Controls can be classified by timing (preventive, detective, corrective) or nature (administrative, technical, physical). Refer to the FFIEC Management; Information Security; and Architecture, Infrastructure, and Operations; and Development, Acquisition, and Maintenance

booklets for additional guidance on risk mitigation considerations. Note: Adequacy of specific controls in the different IT areas are examined in other IT procedures.

- *Monitoring and Reporting* – Management needs to ensure appropriate monitoring and reporting of IT activities and risk. Monitoring should be ongoing and include reviews of metrics, performance benchmarks, service level agreements, and compliance with internal policies. As part of the monitoring process, management should review the effectiveness of controls and ensure quality assurance and control practices are appropriate. Specifically, FCA Regulation 609.905 requires the institution to monitor cyber threats, mitigate any known vulnerabilities, and establish appropriate reporting mechanisms. Management should ensure there is a clear assignment of responsibilities and accountability for both monitoring and escalation processes. FCA Regulation 609.930(e) requires quarterly reporting to the board (or an appropriate board committee) on material matters related to the institution's cyber risk management program, including specific risks and threats. Reporting processes should include defined reporting channels for accurate, timely, and relevant reporting to appropriate levels of executive management and the board. IT risk reporting recipients should have the authority and responsibility to act on the reported information, provide a credible challenge for information contained in the reports, and be held accountable for the outcomes. Refer to the FFIEC Management; Information Security; and Architecture, Infrastructure, and Operations; and Development, Acquisition, and Maintenance booklets for additional guidance on risk monitoring and reporting considerations.

- ***Planning:*** **Has the board provided effective oversight of IT planning, including the review and approval of an IT strategic plan that aligns with overall business strategies? Has management developed appropriate operational technology plans and budgets? Have they incorporated these plans and budgets into the overall business planning process?** The successful development and maintenance of IT requires board commitment, planning, and appropriate oversight. Because major investments in IT resources have both short- and long-term implications, IT strategic and operational plans should be integrated into the overall business planning process. Management should develop short-term tactical IT operational plans that support the larger IT strategic plan. The technology plan(s) complexity will depend on the business model, size, risk profile, and operations of the institution. Technology plan(s) must be reviewed annually and revised as needed. FCA Regulation 609.935 requires the business plan to include a technology plan. Compliance with this regulation is examined in the *Regulatory Compliance* procedure in the *Business Strategy & Planning* Examination Manual topic. Refer to the FFIEC Management booklet for additional guidance on planning IT operations and investment and the Architecture, Infrastructure, and Operations booklet for additional guidance on strategic planning.

- ***Training:*** **Do the board and staff receive necessary training to increase awareness of IT operations, security, risks, and their roles and responsibilities in managing IT risks?** IT training programs should help provide personnel with the necessary knowledge and skills to perform their job functions while better understanding and managing IT risks. FCA Regulation 609.930(c)(4) requires the institution to describe the plan to train employees, vendors, contractors, and the board to implement the institution's cyber risk program. The board and all employees should have annual training on technology and security risks (e.g., cybersecurity). Training should also occur as needed to ensure users understand IT systems and user security protocols (e.g., lending platforms, borrower verification, acceptable use

policies). Training should support security awareness, including staff security roles and responsibilities, and strengthen compliance with IT operations and security policies. Ultimately, the board and management's behavior and priorities heavily influence employee awareness and policy compliance. Therefore, training and the commitment to IT operations and security should start with the board and management. Refer to the FFIEC Management, Information Security, and Architecture, Infrastructure, and Operations booklets for additional guidance on IT-related training.

- ***Outsourcing Technology Service Providers (TSPs):*** **Does the institution adequately manage its outsourced TSP relationships?** The FFIEC defines outsourcing as the practice of contracting through a formal agreement with a third party to perform services, functions, or support that might otherwise be conducted in-house. Many institutions contract with third-party organizations for technology-related services because it provides a cost-effective solution. An institution may outsource some or all IT-related functions, including mission-critical applications. However, outsourcing does not change expectations for safe, sound, controlled, and efficient operations. Risk exists whether the institution maintains the IT services internally or outsources them. In either situation, the board and management are responsible for managing the risk. If a TSP performs information processing for the institution or if the institution has contracted a third party to perform specific technology-related services, management should perform sufficient due diligence to ensure appropriate internal controls and sound business practices are maintained. FCA Regulation 609.930(c)(5)(iii) requires a vendor risk assessment on all vendors (IT and non-IT). FCA Regulation 609.930(c)(5)(iv) requires the institution to monitor its IT and cybersecurity risk management related vendors to ensure they have satisfied agreed upon expectations and deliverables. Monitoring may include reviewing audits, summaries of test results, or other equivalent evaluations of its vendors. Service Organizational Controls (SOC) and other attestation reports can contain valuable information about a TSP's products and processes. If relying on SOC reports, management should verify whether the review's scope and depth are sufficient to evaluate the TSP's control environment. Depending on the scope of the audit testing, findings noted in the report, or the audit opinion, additional inquiry and activities may be necessary to understand the TSP's resilience. Refer to the FFIEC Outsourcing Technology Services and Supervision of Technology Service Providers booklets for additional guidance on controls that govern TSP relationships. The FFIEC booklets include specific guidance available regarding third-party relationships for architecture, infrastructure, and operations; information security; third-party management; business continuity management; retail payment systems; wholesale payment systems; and development, acquisition, and maintenance. Additionally, see interagency guidance on Conducting Due Diligence on Financial Technology Companies dated August 2021. Refer to the *Third-Party Risk Management* procedure in the *Direction & Control of Operations* Examination Manual topic for information on examining an institution's outsourcing processes.

- ***Examination Results from Other IT & Security Procedures:*** **Did the examination of security, operations, development & acquisition, payment systems, and e-commerce evidence effective overall IT governance and controls?** Consider the results of the evaluative questions in each of the IT & Security procedures that follow to conclude on overall adequacy of the institution's IT governance and controls. Results from the examination of the other IT & Security procedures can provide insight into the effectiveness of overall IT governance and controls. If the examination identified weaknesses in governance or controls

in a particular area, the examiner should further examine if those weaknesses were a result of a systemic weakness in overall IT governance and controls.

2. Security:

Determine the quality and effectiveness of the security program in adequately safeguarding assets and protecting data (i.e., confidentiality, integrity, and availability).

Guidance:

The terms security, information security, and cybersecurity often overlap in FCA, FFIEC, and other industry guidance. The FFIEC Information Security booklet defines information security as the process by which an organization protects the creation, collection, storage, use, transmission, and disposal of information. Cybersecurity is the process of protecting information by preventing, detecting, monitoring, and responding to attempts to damage, disrupt, or gain unauthorized access to a computer, computer system, data, or electronic communications network. An increasing cybersecurity threat environment requires the board and management to understand and manage operational risks effectively. Most System institutions are interconnected from a technology perspective. As a result, smaller and less complex institutions may pose a security threat to other institutions if their computing environments are inadequately secured. All security programs should address the following commonly accepted objectives:

- *Confidentiality* – the assurance that only authorized users can access sensitive information.
- *Integrity* – the assurance that information is accurate, complete, and unaltered.
- *Availability* – the assurance that authorized users have access to information when needed.

Information security is an ongoing process that is everyone's responsibility within the institution. The board should understand security risks and provide management with direction and guidance. As part of the information security program, the board and management must establish an appropriate vulnerability management program based on sound industry standards and practices commensurate with the institution's size, risk profile, and complexity as required by FCA Regulation 609.905. The information security program's effectiveness depends on a sound security culture, appropriate risk management, and effective controls, which include policies, procedures, security controls, training, and organizational structures. Information security (including cyber risk management) training programs should help provide personnel with the necessary knowledge and skills to perform their job functions securely while better understanding and managing information security risks. An institution may outsource some or all information security-related functions. However, the board is ultimately responsible for the information security program. To evaluate the adequacy of information security training programs and outsourcing TSPs, refer to the *Governance and Management* procedure.

Refer to the FFIEC Information Security booklet for additional background and examination guidance on evaluating information security programs.

Evaluative questions and items to consider when examining the quality and effectiveness of security programs include:

- ***Information Security Governance:*** **As part of the information security program, has the board approved a written cyber risk program, overseen the program, and determined the necessary expertise for carrying out the program?** Each year, the board (or delegated committee) must approve a written cyber risk program as required by FCA Regulation

609.930(b). The program must be consistent with industry standards to ensure the institution's safety and soundness and compliance with law and regulations. The board also must oversee the development, implementation, and maintenance of the institution's cyber risk program, and determine necessary expertise for executing the cyber risk management plan and, where practical, delegate day-to-day responsibilities to management and employees. An information security program is more effective when security processes are ingrained in the culture. The board and management need to understand and support information security and provide appropriate resources for developing, implementing, and maintaining the program. The board should provide management with its expectations and requirements. This includes holding management accountable for oversight and coordination, assigning responsibility, and maintaining overall information security program effectiveness. As part of approving the cyber risk program, the Board tasks may include approving information security and technology budgets, plans, and policies; reviewing assessments of the information security program's effectiveness; and, when appropriate, discussing management's recommendations for corrective action(s). The board and management need to continually assess the capability of the institution's people, processes, and technologies to sustain the appropriate level of information security based on the institution's risk profile, size, complexity, and risk appetite. Refer to the FFIEC Information Security booklet for additional guidance on governance of information security programs.

- ***Policies and Procedures:*** **Have the board and management developed appropriate information security related policies and procedures?** FCA Regulation 609.905 requires the board and management to maintain and document effective policies, procedures, and controls to mitigate cyber risks. Board policy and management procedures should provide strong support and commitment to the institution's information security program. Policies and procedures should define the institution's control environment through a governance structure. In addition, policies should provide descriptions of required, expected, and prohibited activities regarding information security as well as appropriate reporting requirements. The board should review information security and other related policies annually. Refer to the FFIEC Information Security booklet for additional guidance on policies, standards, and procedures.

- ***Risk Management***: **Is information security sufficiently addressed in the ITRM program?** Management needs to identify and measure risks associated with information security in the IT risk assessment and maintain necessary risk mitigation practices and controls to address and monitor the risks. FCA Regulation 609.930(a) requires the institution to implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information; protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information. Refer to the FFIEC Information Security booklet for additional guidance on information security program management. Refer to the *Governance and Management* procedure to examine the ITRM program processes.

- ***Information Security Controls:*** **Has management developed and implemented appropriate controls to mitigate identified information security risks?** Controls serve to reduce risks through the introduction of processes and practices. 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. FCA Regulation 609.930(c)(6) requires

the institution to maintain robust internal controls and FCA Regulation 609.930(c)(6)(iii) requires internal systems and controls to provide reasonable assurances that the institution will prevent, detect, and remediate material deficiencies on a timely basis. Refer to the FFIEC Information Security booklet for additional guidance on control types and control implementation. The following are primary controls used to mitigate information security risks with links to related FFIEC guidance:

- Inventory and classification of assets – this could be part of the risk identification process and the inventory should include systems that address hardware, software, information, and connections
- Mitigating interconnectivity risk
- User security controls – including security screening in hiring practices, user access program, segregation of duties, confidentiality agreements, and training
- Physical security
- Network controls – including wireless network considerations
- Change management within the IT environment – including configuration management, hardening, standard builds, and patch management
- End-of-life management – including system life cycle
- Malware mitigation
- Control of information – including storage, electronic transmission of information, transit of physical media, rogue or shadow IT, and disposal of information
- Supply chain
- Logical security – including operating system access, application access, remote access, use of remote devices, application security, and database security
- Customer remote access to financial services – including customer awareness
- Encryption
- Log management

- ***Internal Controls Over Data:*** **Do security controls comply with the requirements of FCA Regulation 621.15(a)(4) regarding internal controls over data?** FCA Regulation 621.15(a)(4) requires institutions to develop, implement, and maintain an effective system of internal controls over data included in the report of accounts and exposures, including controls for maintaining borrower information confidentiality. Refer to the *Information Systems and Data* procedure within the *Portfolio Planning and Analysis* topic for evaluating compliance with the rest of this regulation.

- ***Incident Response Plan:*** **Has management established an incident response plan in accordance with FCA Regulation 609.930(c)(3)?** The institution must maintain an incident response plan that contains procedures the institution must implement when it suspects or detects unauthorized access to current, former, or potential customer, employee, or other

sensitive or confidential information. The incident response plan must contain procedures for the following:

- Assessing the nature and scope of an incident and identify what information systems and types of information have been accessed or misused.
- Acting to contain the incident while preserving records and other evidence.
- Addressing how business activities will resume during an intrusion response.
- Notifying the board when the institution learns of an incident involving unauthorized access to or use of sensitive or confidential customer or employee information as well as unauthorized access to financial institution information, including proprietary information.
- Notifying FCA as soon as possible but no later than 36 hours after determining an incident has occurred.
- Notifying former, current, or potential customers and employees of an incident in accordance with state and federal laws (including known visitors to the institutions website when warranted).

Note: Refer to the FFIEC Information Security booklet for additional guidance on threat identification and assessment, threat monitoring, incident identification and assessment, and incident response. In addition, FCA's Informational Memorandum on Reporting Security Incidents and Business Continuity Events to FCA dated June 27, 2017, includes guidance on incident response programs and plans.

- ***Review and Testing:*** **Does management use periodic review and tests to ensure the security program is effective and functioning as expected?** The board and management should review the information security program periodically to ensure it continues to support the ITRM process (including cyber risk management) and aligns with the institution's risk appetite and strategic objectives. FCA Regulation 609.930(c)(6) requires the institution to conduct regular testing of key controls, systems, and procedures of the cyber risk management program. Testing and evaluation of the security program should provide assurance that the program is effective and operating as expected. FCA Regulation 609.930(c)(6)(i) requires the frequency and nature of the tests to be determined by the institution's risk assessment. Testing and evaluation types include self-assessments, penetration tests, vulnerability assessments, and audits. FCA Regulation 609.930(c)(6)(ii) requires the tests to be completed or reviewed by independent third parties or staff independent of those who develop or maintain the cyber risk management program. After reviewing and testing the program, management should report results to the board and take any necessary actions to improve the information security program. Refer to the FFIEC Information Security booklet for additional guidance on information security program effectiveness, assurance and testing, key testing factors, types of tests and evaluations, and assurance reporting. Refer also to the *Audit* procedure and the FFIEC Audit booklet for additional guidance on audit expectations.

- ***Monitoring and Reporting:*** **Is information security monitoring and reporting effective? Has management developed satisfactory performance benchmarks and metrics for measuring performance, efficiency, and compliance with information security policies? Does**

management provide appropriate and necessary summary reports about information security to the board? Monitoring involves ongoing processes to assess the institution's risk environment and identify gaps in risk mitigation effectiveness due to changes in security conditions, threats, or vulnerabilities. In addition, updates or changes in the institution's systems, hardware, software, business operations, or service providers may result in control gaps. FCA Regulation 609.905 requires the institution to monitor cyber threats, mitigate any known vulnerabilities, and establish appropriate reporting mechanisms. FCA Regulation 609.930(e) requires quarterly reporting to the board (or board committee) on material matters related to the institution's cyber risk management program, including specific risks and threats. Reporting should provide information to the board and management about the monitoring results and the related response and follow-up actions. Refer to the FFIEC Information Security booklet for additional guidance on risk monitoring and reporting.

- ***Privacy:*** **Do processes and controls ensure compliance with FCA Regulation 609.930(d)?** Privacy is the right to control how personal information is viewed and used. FCA Regulation 609.930(d) requires the institution to consider privacy and other legal compliance issues, including but not limited to, the privacy and security of System institution information; current, former, and potential borrower and employee information; as well as compliance with statutory requirements for the use of electronic media. The institution must meet all regulatory requirements (including demonstrating compliance with applicable State and Federal privacy laws) for collecting, processing, or maintaining personal information. Data privacy breaches can lead to regulatory investigations, violations, and fines.

Refer to the following for additional information and guidance:

- FCA Informational Memorandum on The increase in ransomware attacks and how to protect critical data dated June 24, 2021
- FCA Informational Memorandum on Cybersecurity Assessment and Expectations for System Institutions dated August 5, 2015
- FCA Informational Memorandum on Cybersecurity Framework and Other Recent Guidance dated December 16, 2014
- FCA Informational Memorandum on Threats to Information Management Systems dated August 30, 1999
- National Security Agency guidance on NSA's Top Ten Cybersecurity Mitigation Strategies (March 2018)
- FFIEC Joint Statement on Risk Management for Cloud Computing Services dated April 30, 2020 and FFIEC Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Network dated June 7, 2016
- Federal Deposit Insurance Corporation Supervisory Insights journal article, A Framework for Cybersecurity, Volume 12, Issue 2 (Winter 2015)

3. Operations:

Evaluate the adequacy of processes and controls over IT operations.

Guidance:

IT operations involve the technology processes and services that an IT department provides and administers to capture, transmit, process, and store an institution's information assets and to support its day-to-day business functions. The key responsibilities and functions of IT operations fall into three areas: 1) network infrastructure, 2) server and device management, and 3) computer and help desk operations. Generally, IT operations do not include IT applications and programming activities, but some functions and management responsibilities may overlap between these departments or teams. IT operations training programs should be commensurate with its complexity. Training should provide personnel with the necessary knowledge and skills to perform their job functions while better understanding and managing IT risks. To evaluate the adequacy of IT operations training programs, refer to the *Governance and Management* procedure.

IT operational processes can be viewed as two sets of business processes: front-office and back-office. Front-office processes address how the institution interacts directly with the customer, such as marketing, sales, and service. Back-office processes are also important to the institution's operations; however, they do not normally involve direct interaction with the customer. Examples of back-office processes include finance, accounting, IT, and human resources. Operational complexity varies throughout the System. More operationally complex institutions (e.g. banks, TSPs, and some associations) usually have a dedicated IT department that manages and supports IT operations and may deliver services to their customer associations. Less operationally complex institutions often outsource most of their IT service needs to a TSP (which might be a System bank). In addition, some institutions combine in-house IT operations with a TSP. For example, an association might manage its own local area network operations, but use a TSP for loan accounting, general ledger, and other back-office operations. To evaluate the adequacy of outsourcing TSPs, refer to the *Governance and Management* procedure.

Refer to the FFIEC Architecture, Infrastructure and Operations booklet for additional background and examination guidance on evaluating an institution's controls relative to the risks of technology systems and operations that reside in, or are connected to, the institution.

Evaluative questions and items to consider when examining the adequacy of processes and controls over IT operations include:

- ***IT Operations Governance:*** **Have the board and management established a strong IT operations culture, defined responsibilities and accountability, and provided adequate support resources?** The board and management are responsible for ensuring IT operates in a safe, sound, and efficient manner throughout the institution and for strategic technology planning, which is critical to effective IT governance. The board and management can delegate the implementation and oversight of daily operations to IT management with proper reporting. IT operations management is responsible for ensuring the current and planned infrastructure is sufficient to accomplish the board and management's strategic plans. The board and management should understand and support IT operations and provide appropriate resources for developing, implementing, and maintaining operations. Refer to the FFIEC Architecture, Infrastructure, and Operations booklet for additional

guidance on architecture, infrastructure and operations governance, board and senior management responsibilities, and other roles and responsibilities.

- ***Policies and Procedures:*** **Have the board and management developed appropriate IT operations-related policies and procedures?** Policies and procedures should define the institution's control environment through a governance structure and provide descriptions of required, expected, and prohibited activities regarding IT operations. An institution should have guidance in place regarding IT operations; although, the level of detail will vary based on the size, risk profile, and complexity of institution operations. Policies and procedures guide decisions and activities of users, developers, administrators, and managers and inform those individuals of their responsibilities. The board should review all guidance periodically and review and approve policies annually. Refer to the FFIEC Architecture, Infrastructure, and Operations booklet for additional guidance on policies, standards, and procedures.

- ***Risk Management***: **Are IT operations sufficiently addressed in the ITRM program?** Risk profiles vary significantly based on the size and complexity of the institution's IT operations. Management should identify and measure risks associated with applicable IT operations in the IT risk assessment and maintain necessary risk mitigation practices and controls to address and monitor the risks. Refer to the FFIEC Architecture, Infrastructure, and Operations booklet for additional guidance on IT operations risk management. Refer to the *Governance and Management* procedure to examine the ITRM program processes.

- ***IT Operations Controls:*** **Has management developed and implemented appropriate controls to mitigate IT operations risks?** Controls serve to reduce risks through the introduction of processes and practices. An institution should implement appropriate controls over IT operations; however, the level at which the institution implements controls should depend on the institution's size, complexity, and risk profile. Management should have a clear understanding of the operating environment and build a resilient IT environment. The following areas are primary controls included in the FFIEC Architecture, Infrastructure and Operations booklet used to mitigate IT operations risks with links to related FFIEC guidance:

    - Data governance and data management – including data identification and classification and database security
    - IT asset management – including hardware and software inventories, IT asset end-of-life, and shadow IT
    - IT and business environment representations (network diagrams, data flow diagrams, and business process diagrams and narratives)
    - Managing change in architecture, infrastructure, and operations
    - Remote access
    - Personally owned devices
    - File exchange
    - Architecture – including architecture plan and IT architecture design

- Infrastructure – including hardware, network and telecommunications, software, environmental controls, and physical access controls

- Operations – including IT operational controls, operational processes (maintenance, configuration management, vulnerability and patch management, backup and replication processes, scheduling, capacity management, log management, disposal of data and media), and service and support processes

- Evolving technologies

- ***Monitoring and Reporting:*** **Is IT operations monitoring and reporting effective? Has management developed satisfactory performance benchmarks and metrics for measuring performance, efficiency, and compliance with IT operations policies? Does management provide appropriate and necessary summary reports about IT operations to the board?** Monitoring involves using ongoing processes to assess IT operations and technology environment risks and ensuring that established controls are functioning properly. Performance monitoring involves measuring operational activities, analyzing the resulting metrics, and comparing them to internally-established standards and industry benchmarks to assess the effectiveness and efficiency of existing operations. Internal audits are also beneficial for validating controls. Reporting should provide information to the board and management including monitoring results and the related response and follow-up actions. Refer to the FFIEC Architecture, Infrastructure, and Operations booklet for additional guidance on ongoing monitoring and evaluation processes, monitoring and reporting, and board and senior management reporting.

4. Development & Acquisition:

Evaluate the adequacy of processes and controls to identify, acquire, develop, install, maintain, and monitor appropriate IT systems.

Guidance:

Management should define and implement standards and adopt an appropriate methodology governing the process of identifying, acquiring, developing, installing, maintaining, and monitoring information systems and related technology. Systems development involves the process of defining, designing, testing, implementing, and maintaining a software application or IT system. It could include the internal development of customized software applications or systems or purchasing or acquiring hardware, software, or services from third parties. Software development is the process of conceiving, specifying, designing, programming, documenting, approving, testing, and debugging to create and maintain software applications, frameworks, or other components. In simple terms, software development is the process of writing and maintaining computer source code, and it includes everything from conceiving the desired software to implementing the final product. It may also include research, new development, prototyping, modification, reuse, re-engineering, maintenance, or any other activities that result in software products. The common element in development and acquisition processes is the need for effective project management techniques. Additionally, information security is a critical component of the software development process, whether internally or externally developed.

Training programs for systems development and acquisition should be commensurate with the nature and complexity of the institution's systems development and acquisition activities. Training should provide personnel with the necessary knowledge and skills to perform their job functions

while better understanding and managing IT risks. An institution may outsource some or all IT-related services and software development projects. However, outsourcing does not change expectations for safe, sound, controlled, and efficient systems development and acquisition. To evaluate the adequacy of training programs and outsourcing TSPs, refer to the *Governance and Management* procedure.

Examination activities should be based on the institution's operational complexity and extent of development and acquisition activities. Refer to the FFIEC Development, Acquisition, and Maintenance booklet for additional background and examination guidance on identifying and controlling development and acquisition risks. The booklet details general project management standards, procedures, and controls; and it discusses various development, acquisition, and maintenance project risks; and acquisition of software products.

Evaluative questions and items to consider when examining the adequacy of processes and controls to identify, acquire, develop, install, maintain, and monitor appropriate IT systems include:

- ***Policies and Procedures:*** **Have the board and management established written policies and procedures for developing, acquiring, and maintaining technology systems?** Policies and procedures should define the institution's project management techniques and provide descriptions of required, expected, and prohibited activities regarding development and acquisition projects. Structured project management techniques or standards help ensure efficient, effective, and secure technology systems. Although standards do not guarantee that an organization will appropriately develop, acquire, and maintain technology systems, standards do enhance management's control over these projects, which decreases project risk. Refer to the FFIEC Development, Acquisition, and Maintenance booklet for additional guidance on policies, standards, and procedures.

- ***Risk Management*****: Is development, acquisition, and maintenance sufficiently addressed in the ITRM program?** Risk profiles vary significantly based on the size and complexity of the institution's development, acquisition, and maintenance projects and operations. Management should identify and measure risks associated with applicable development, acquisition, and maintenance in the IT risk assessment. They must also maintain necessary risk mitigation practices and controls to address and monitor the risks. Refer to the FFIEC Development, Acquisition, and Maintenance booklet for additional guidance on IT risk management of development, acquisition, and maintenance. Refer to the *Governance and Management* procedure to examine the ITRM program processes.

- ***Project Management:*** **Has management established appropriate project management methodologies?** Project management involves planning, monitoring, controlling, and maintaining a project or activity. Appropriate management processes and controls over systems development and acquisition processes ensure efficient use of resources and minimize risk(s) within these activities. Boards, or board-designated committees, should formally approve project methodologies. Management should approve and document significant deviations from approved procedures. The Systems Development Life Cycle (SDLC) methodology is the primary project management methodology or approach described in the FFIEC Development, Acquisition, and Maintenance booklet used to plan, design, develop, test, and implement an application system or a major modification to an application system. It provides a systematic way to describe the numerous tasks associated with software development projects. An institution may use other alternative development methodologies (e.g., Agile, Waterfall) when managing any project, including software

development or hardware, software, or service acquisition projects. Management should tailor the project management methodology used to the project's characteristics and risks.

- ***Development:*** **Did management apply effective project management methodologies and practices for development projects? Was the methodology commensurate with the characteristics and risks of the projects?** Development projects involve creating software applications or integrated application systems. Organizations may complete these projects in-house, through outsourcing, or with a combined approach. An institution's use of outsourcing does not change the expectation for management to apply safe, sound, controlled, and efficient project management. Furthermore, information security is a critical part of internally and externally developed software. The institution should consider information security requirements and incorporate automated controls into internally developed programs. Similarly, the institution should ensure these controls are incorporated into acquired software before it is implemented. Refer to the FFIEC Information Security booklet for additional guidance on application security. Refer also to the National Institute of Standards and Technology's Security Considerations in the System Development Life Cycle. Refer to the FFIEC Development, Acquisition, and Maintenance booklet for additional background and guidance on development standards and controls. The booklet also provides the following information and guidance on the typical phases that make up development projects in the SDLC:

    - Initiation phase
    - Development or acquisition phase
    - Implementation and assessment phase
    - Operations and maintenance phase
    - Sunset and disposal phase

- ***Acquisition:*** **Did management apply effective project management methodologies and practices for acquisition projects? Was the methodology commensurate with the characteristics and risks of the projects?** Acquisition projects for significant hardware and software products are similar to development projects. Institutions replace the design and development phases with a bid solicitation process that involves developing detailed lists of functional, security, and system requirements and distributing them to third parties. Refer to the FFIEC Development, Acquisition, and Maintenance booklet for additional guidance on acquisition methodologies, and contracts and other agreements.

- ***Maintenance:*** **Did management apply effective project management methodologies and change controls for maintenance projects? Were the methodology and controls commensurate with the characteristics and risks of the hardware, software, and related documentation?** Maintenance projects and activities include routine servicing and periodic modification of hardware, software, and related documentation. Hardware maintenance involves replacing outdated or malfunctioning equipment or enhancing its existing performance or storage capacity. Software maintenance is necessary to address user requirements, rectify software problems, correct security vulnerabilities, or implement new technologies. Documentation maintenance is crucial for maintaining current and accurate technology-related records, standards, and procedures. Refer to the FFIEC Development, Acquisition, and Maintenance booklet for additional guidance on maintenance methodologies and related change controls. Management should establish detailed change control standards and procedures to ensure technology-related modifications are

appropriately authorized, tested, documented, implemented, and disseminated. The booklet also provides additional guidance for the following:

- Preventative maintenance
- Change management
- End-of-life
- Termination and disposal
- Maintenance documentation

5. Payment Systems:

Evaluate the adequacy of processes and controls over payment systems.

Guidance:

A payment system involves the mechanism, rules, institutions, people, markets, and agreements that make payments or funds exchange possible. A paper-based system can be used for handling checks and drafts, but most payment systems are electronic. Although electronic payment systems offer efficiency through the rapid and convenient transmission of payment information between involved parties, they can also enable the rapid spread of fraud, money laundering, and operational disruption if data is compromised. Therefore, an institution should have adequate and effective internal controls over payment systems and processes. Training programs should be commensurate with the payment system's complexity and risk profile. Training should provide personnel with the necessary knowledge and skills to perform their job functions while better understanding and managing IT and cyber related risks. An institution may outsource some or all IT-related payment system services. However, outsourcing does not change expectations for safe, sound, controlled, and efficient operations. To evaluate the adequacy of training programs and outsourcing TSPs, refer to the *Governance and Management* procedure.

The IT Handbook includes two booklets that provide examination guidance for payment systems, a Retail Payment Systems booklet and a Wholesale Payment Systems booklet. The IT handbook acknowledges there is no definitive division between retail and wholesale payments, but it provides the following generalized descriptions of the two mechanisms:

- **Retail Payment Systems**
    - Transactions occurring between two consumers, between consumers and businesses, or between two businesses
    - Used for purchasing goods and services, bill payment, person-to-person transactions, account-to-account transactions, and cash withdrawals and advances
    - Generally, process higher transaction volumes and lower average dollar values than wholesale payment systems
    - May involve using various retail payment instruments or access devices (e.g., check-based payments, Automated Clearing House (ACH), card-based electronic payments, emerging retail payment technologies)

- **Wholesale Payment Systems**
    - Transactions occurring between businesses
    - High-dollar value payments
    - Used to purchase, sell, or finance securities transactions; disburse or repay loans; settle real estate transactions; and make high-dollar, time-critical payments (e.g., payments for interbank purchase settlements and federal funds sales, foreign exchange transaction settlements, other financial market transactions)
    - Involves using interbank funds transfer systems or networks
        - *Fedwire Funds Service (Fedwire)* – Fedwire is a real-time gross settlement system provided by the Federal Reserve Banks that enables participants to transmit and receive payment orders between each other and on behalf of their customers
        - *Clearing House Interbank Payments System (CHIPS)* – CHIPS is a funds-transfer network owned and operated by the Clearing House Interbank Payments Company L.L.C., a subsidiary of The Clearing House, a banking association and payments company owned by the largest commercial banks
        - *Society for Worldwide Interbank Financial Telecommunications (SWIFT)* – SWIFT serves as a worldwide interbank telecommunications network and uses a standardized proprietary communications platform to quickly, accurately, and securely send and receive information, such as money transfer instructions

Evaluative questions and items to consider when examining the adequacy of payment systems processes and controls include:

- ***Policies and Procedures:*** **Have the board and management developed appropriate payment system-related policies and procedures?** Policies provide the basis for establishing and maintaining proper operational and security controls over the payment systems used or offered by the institution. The lack of policy guidance, procedural direction, and control processes can cause credit, financial, legal, and operational risks. Financial institutions must comply with federal and state laws and regulations, as well as with operating rules of clearing houses and payment system networks. Refer to the FFIEC Management booklet for additional guidance on policies, standards, and procedures.

- ***Risk Management***: **Are payment systems sufficiently addressed in the ITRM program?** Risk profiles vary significantly based on the size and complexity of the institution's retail and wholesale payment system products and services. Management should identify and measure risks associated with these activities in the IT risk assessment and maintain necessary risk mitigation practices and controls to address and monitor the risks. Refer to the FFIEC IT Booklets for additional guidance on retail payment systems risk management and wholesale payment systems risk management. Refer to the *Governance and Management* procedure to examine the ITRM program processes.

- ***Internal Controls:*** **Has management established effective internal controls over payment systems?** Controls should be commensurate with the size, risk profile, and complexity of the

institution's payment system products and services, IT infrastructure, and dependence on TSPs. Effective internal controls should include financial, accounting, operational, technical, procedural, and administrative controls necessary to minimize risks in the payment transaction, clearing, and settlement processes. This includes having physical and logical access controls over the payment systems equipment and processes, as well as using appropriate separation of duties and dual authorization to initiate and approve transactions. In particular, controls should include clear instructions on completing appropriate identity and request verification steps (e.g., call-back procedures, passcodes/PINs) with new wire requests or when wire instructions change (e.g., routing/account number, international wires). Controls should also include transaction and fraud monitoring, including audit log review, behavioral analytics, call-back functions, suspense accounts, daily reconciliations, and any other type of red-flag detective control to identify and shut down unauthorized payments. Effective controls also involve systems testing, backup systems, and contingency planning. Refer to the FFIEC Retail Payment Systems booklet and Wholesale Payment Systems booklet for additional guidance on retail payment instrument specific risk management controls and internal and operational controls.

Refer to the following for additional information:

- Board of Governors of the Federal Reserve System website (Federal Reserve Board - Payment Systems)
- Nacha website (ACH Network - Nacha)
- The Clearing House website (Education & Support - The Clearing House)
- SWIFT website (SWIFT - The global provider of secure financial messaging services)

6. E-Commerce:

Evaluate the adequacy of processes and controls for e-commerce.

Guidance:

E-commerce or electronic business is defined as buying, selling, producing, or working in an electronic medium. E-commerce is a business model used by businesses and consumers to buy and sell all types of goods and services over the internet. The financial services industry uses e-commerce to promote their services, disperse information, take online applications, and assist in their own internal operations. Electronic banking (e-banking) is a form of e-commerce used by financial institutions; it may also be referred to as online banking, internet banking, or web banking. E-banking includes the systems that enable financial institution customers to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet.

While e-commerce activities may provide new business opportunities, they also create new business risks and challenges that must be actively managed. The board and management should understand the risks associated with e-commerce and e-banking to make informed decisions regarding the deployment of a particular product or service. An institution may conduct these services either in-house or through a third-party relationship with other firms, or it may provide such services to other System institutions. Regardless of the method used, the board is responsible for ensuring it understands the related business risks, implements the necessary internal controls, and complies with applicable regulatory requirements. To evaluate the adequacy of outsourcing TSPs, refer to the *Governance and Management* procedure.

Evaluative questions and items to consider when examining the adequacy of processes and controls for e-commerce include:

- ***Policies and Procedures:*** **Have the board and management adopted appropriate e-commerce policies and procedures?** The board should establish the appropriate oversight and direction for the institution's use of e-commerce through board policy. Policies and procedures should address the following, when applicable:

    - Security (confidentiality, integrity, and availability) of institution and borrower data.
    - Privacy of website customers and visitors.
    - Notices to website customers or visitors when linking to an affiliate or third-party website.
    - Capability of vendor or application providers.
    - Business resumption after disruption.
    - Fraud and money laundering.
    - Intrusion prevention and management.
    - Liability insurance.
    - Prompt reporting of known or suspected criminal violations associated with e-commerce to law enforcement authorities and FCA under FCA Regulations, Part 612, Subpart B.

- ***Risk Management***: **Is e-commerce and e-banking sufficiently addressed in the ITRM program?** E-commerce and e-banking have unique characteristics that may increase the institution's overall risk profile and the level of risks associated with traditional financial services. Risks associated with these activities should be identified and measured in the IT risk assessment and management should maintain necessary risk mitigation practices and controls to address and monitor the risks. Refer to the FFIEC Management booklet for additional guidance on IT Risk Management. Refer to the *Governance and Management* procedure to examine the ITRM program processes.

- ***Internal Controls:*** **Has management developed and implemented effective internal controls applicable to e-commerce?** A strong internal control system provides the framework to accomplish management objectives, safeguard assets, ensure complete and accurate financial reporting, and comply with laws and regulations. Effective internal controls serve as checks and balances against undesired actions and, as such, provide reasonable assurance that the institution operates in a safe and sound manner. The lack of effective internal controls puts the institution at risk of material financial misstatement, mismanagement, waste, fraud, and abuse. FCA's Informational Memorandum on E-Commerce and Security Risks dated October 2, 2000, includes information about e-commerce security risks. Internal controls surrounding e-commerce are similar to information security controls covered in the FFIEC Information Security booklet. Key e-commerce controls include the following:

    - Segregation of duties
    - Dual controls
    - Reconcilements
    - Fraud detection
    - Error checks (transaction integrity and validation)
    - Clear user instructions
    - Required approvals and confirmations

- Authentication and access (also see FCA's Informational Memorandum on Guidance on Authentication in an Electronic Banking Environment dated July 2, 2002)

- ***Records Retention:*** **Has management established an appropriate record retention program to store institution records in compliance with FCA regulations and State and Federal Laws?** System institutions must have record retention programs that comply with FCA regulations and their respective State and Federal laws. Record retention programs, including policies and procedures, must ensure compliance with FCA Regulations 609.930(a) and (d). Controls must exist to protect the security, privacy, and confidentiality of current, former, and potential customer and employee information, protect against cyber threats and unauthorized access to or use of such information. Privacy and other legal compliance issues must be considered as well compliance with statutory requirements (15 U.S.C. Sections 7001-7006) for the use of electronic media. FCA Regulation 609.945 requires records stored electronically to be accurate, accessible, and reproducible for later reference. Records should also be adequately secured as outlined in the *Security* procedure. Effective record retention programs help to manage many risks, including lost or stolen information (especially personally identifiable or sensitive confidential information), excessive backlog of documents, loss of time and space, and lack of organization. An effective records retention program, including established retention periods and timely disposal of unnecessary records, reduces legal and reputation risk as maintaining documents beyond any necessary time period could result in excessive risk of loss of confidential personal and business information.

- ***E-SIGN:*** **If using electronic records, contracts, or signatures to transact business, has management taken appropriate action to comply with the Electronic Signatures in Global and National Commerce Act (E-Sign Act)?** The E-Sign Act derives its authority from 15 U.S.C. Sections 7001-7006. The E-Sign Act allows the use of electronic records, with some exceptions concerning consumer protection, to satisfy any statute, regulation, or rule of law requiring that such information be provided in writing, if the consumer has affirmatively consented to such use and has not withdrawn such consent. It governs transactions relating to the conduct of business, consumer, or commercial affairs between two or more persons. All parties to a transaction must agree in writing before E-SIGN can be used. All System institutions are required to comply with the requirements under the E-SIGN Act. Refer to FCA Informational Memorandum on Compliance with the Electronic Signatures in Global and National Commerce Act and Regulations B, M, and Z dated April 15, 2024 for additional guidance.

- ***Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act): Do processes and controls ensure compliance with the CAN-SPAM Act?*** The CAN-SPAM Act, 15 U.S.C. 7701-7713, is implemented by FTC regulations at 16 CFR Part 316. It establishes certain requirements for commercial email. Its main requirements include a ban on false or misleading header information and deceptive subject lines, a requirement that commercial email be identified as advertising, and a requirement that commercial emails inform recipients how they can opt out of future emails. It generally exempts transactional or relationship emails from most requirements.

- ***Website Compliance:*** **Does the institution's website contain clear and conspicuous disclosures as required by law, FCA regulation, and other guidance?** Financial institutions are deploying online systems to facilitate the convenient delivery of financial products and services. Laws and regulations governing these financial products and services require

specific disclosures, notices, and recordkeeping on an institution's website. When using technologies such as e-commerce and e-banking, the institution should adapt to the changing technological environment to comply with applicable laws and regulations to provide appropriate disclosures to consumers, protect customer information, and minimize financial liability and reputation risk. As described in FCA's Informational Memorandum on Web Site and Internet Guidelines dated November 8, 1999, the institution's website should include clear and conspicuous disclosures, including but not limited to, the following:

- *Privacy Policy* – A privacy policy statement that identifies the information the website gathers automatically or collects from emails or web forms, how the information is treated, how the information might be used for security or intrusion detection purposes, and a statement on weblinking. See FCA's Informational Memorandums on Recommended Elements of a Privacy Policy dated July 29, 2003; Guidance for Weblinking Relationships dated September 19, 2002; and Additional Guidance on the Risks of Weblinking dated June 4, 2003, for additional information.

- *Equal Credit Opportunity Lender* – A specific statement identifying the institution as an equal credit opportunity lender if the website contains an online loan or lease application, or if it advertises credit availability.

- *Equal Housing Lender* – A specific statement identifying the institution as an equal housing lender if the website advertises rural residence loans (including use of the approved logotype and legend in FCA Regulation 626.6020(b)).

- *Equal Opportunity Employer* – A specific statement identifying the institution as an equal opportunity employer if the website contains job announcements or online job applications.

- *Children's Online Privacy Protection Act (COPPA)* – The COPPA, 15 U.S.C. 6501-6506, is implemented by Federal Trade Commission (FTC) regulations at 16 CFR Part 312. It imposes certain requirements on operators of websites or online services that are directed at children, as well as to other operators who have knowledge that they are collecting or maintaining personal information from children. If applicable, the institution must have a privacy statement that tells visitors about the types of information the website collects, how the website collects the information, how the website uses the information, and whether the website gives the information to anyone else. This privacy statement must be clearly written, understandable, and located close to any requests for information from children. Refer to FCA Informational Memorandum on Children's Online Privacy Protection Act of 1998 dated June 26, 2003, and the FTC website for more detailed information on complying with the COPPA.

- ***Social Media*: Are risks related to social media effectively identified, measured, monitored, and controlled?** Social media is a form of interactive online communication in which users can generate and share content through text, images, audio, and video. Social media can be used in a variety of ways including advertising and marketing, providing incentives, facilitating applications for new accounts, inviting feedback from the public, and engaging with existing and potential customers. Since this form of customer interaction tends to be both informal and dynamic, and may occur in a less secure environment, it can present some unique challenges. Increased risk can arise from poor due diligence, oversight, or control. Commensurate with the level of social media used, the institution should identify the

potential risks and manage risks within the overall ITRM program. Refer to FFIEC supervisory guidance on Social Media: Consumer Compliance Risk Management Guidance, dated December 11, 2013 (See FFIEC press release and FCA Informational Memorandum on Social Media: Consumer Compliance Risk Management Guidance dated April 10, 2014) for more information on sound practices for managing risks from social media.

Refer to the following for additional information and guidance:

- FCA Informational Memorandum on Specific Guidance on Electronic Disclosures and Notices dated July 26, 2002
- FCA Board Policy Statement PS-78 addressing an institution's official name used in all written communications (including website) (effective July 8, 2011)

7. Audit:

Determine if the institution conducts an effective audit (scope, reporting, and follow-up) of IT and security.

Guidance:

The internal audit and review program is a key mechanism for ensuring IT and security processes are functioning effectively and in compliance with regulations and policies. The internal auditor or other qualified, independent party should review the adequacy of IT and security practices (including cyber risk management) to ensure compliance with applicable criteria. The audit risk assessment and scope should address IT and security topics, and audit or review frequency should be commensurate with the complexity of the institution's operations, size, and risk profile. A reliable audit program provides the board reasonable assurance that IT and security processes are sound and that related reporting is complete and accurate. Refer to the FFIEC Audit booklet for additional information and examination guidance about the IT audit function.

Note: This procedure focuses on evaluating the reliability and effectiveness of internal audits and reviews in this topical area. Refer to the *Audit & Review Programs* topic in the Examination Manual for guidance on examining the overall internal audit and review program.

Evaluative questions and items to consider when examining the audit or review of IT and security include:

- ***Audit Coverage:*** **Is there periodic audit or review coverage of IT and security (including cyber risk management)?** Audit or review coverage and frequency should be appropriate relative to risks, changes in the operating environment, regulatory requirements, and periodic testing needs. FCA's Informational Memorandum on Reporting Security Incidents and Business Continuity Events to FCA dated June 27, 2017, includes the expectation that periodic audits should be completed to test compliance with the institution's security policies and their overall effectiveness. Coverage should also be consistent with the institution's risk assessment results and annual audit plan.
- ***Scope and Depth:*** **Are audit or review scope and depth sufficient to conclude on the adequacy, completeness, and timeliness of IT and security processes (including cyber risk management)?** The scope and depth of work, including transaction testing, should cover the primary processes and controls within the area being audited or reviewed and be sufficient to determine if internal controls are functioning as intended and regulatory requirements are met. The scope and depth of coverage should be documented and consistent with the

approved audit or review plan and engagement contract (if applicable). Audit or review workpapers should be examined to verify the actual scope and depth of work performed. The workpapers may indicate the scope and depth deviated from what was identified (or implied) in the audit plan. For example, workpapers may indicate the work performed was limited to evaluating the existence of policies and procedures and didn't include reviewing other controls, such as training or reporting, or testing compliance with regulations or institution guidance. If the work deviated materially from the original planned scope, internal audit should notify the board (or Audit Committee, if so delegated) of the reasons for the change. Specific items that should be considered in the audit or review scope include:

  - Policies and procedures for all major IT and security areas (e.g., IT risk management program (including cyber risk), IT security, IT operations, systems development and acquisition, payment systems, e-commerce, cybersecurity assessments and testing, incident response plan).
  - Compliance with IT and security-related policies, procedures, industry standards, FCA regulations, and other FCA guidance.
  - Monitoring and control processes (e.g., reporting, management oversight, delegated authorities, separation of duties, management information systems).
  - IT security controls (e.g., asset inventory and classification, user security, physical security, network configuration, change management, system life cycle, supply chain, logical security, remote access, application and database security, encryption, log management).
  - IT operations controls (e.g., environmental, physical and logical security, database management, personnel management, change management, data storage and backup, disposal of media, imaging, event and problem management, user support and help desk).
  - Sufficient testing to ensure established criteria are followed.
  - Fraud-related threats and vulnerabilities, as well as anti-fraud controls.

- ***Reliability of Results:*** **Did FCA identify any concerns with audit or review reliability?** It is important to understand the scope and depth of the audit or review being examined, as discussed above, when evaluating audit or review reliability. With this understanding, the following are key considerations when evaluating the reliability of audit or review results:

  - *FCA Testing* – Evaluate the reliability of internal audit or review work by comparing the results to FCA's examination results in this area. This comparison often includes FCA testing transactions that were covered in the internal audit or review (transactions are often loans or loan applications, but may include other types of transactional activity, as well). In addition to the audit or review report, examiners should request and review the workpapers and hold discussions with the auditor to obtain a more thorough understanding of work completed. This can be especially important if the audit or review report is not sufficiently detailed or FCA's examination work and testing identifies potential concerns. Auditors and reviewers complete line sheets, flowcharts, control matrices, standard work programs,

workpaper forms, or other relevant audit evidence when conducting and supporting their work. (IIA Standards 2240, 2300, 2310, and 2320) Workpapers should adequately document the work performed and support the final report. If FCA identifies weaknesses that were not identified in the audit or review, the cause for any discrepancy should be determined.

- *Audit/Review Staffing* – Whether internal or outsourced, auditors and reviewers conducting the work need to be qualified, independent, and objective to ensure reliable results. They should have the right mix of knowledge, skills, and other competencies needed to perform the work. (IIA Standard 2230) Additionally, auditors and reviewers need to be independent of the activities they audit so they can carry out their work freely and objectively. (IIA Standards 1100, 1112, 1120, and 1130) For example, audit and review staff should not be involved in developing and installing procedures, preparing records, operating a system of internal controls, or engaging in any other activity that they would normally review. Examiners should evaluate the staffing on the individual audit or review being examined as part of determining the reliability of results.

- *Institution Review of Work Performed* – The institution should complete an independent review of the workpapers to ensure audit or review objectives and scope were met and the results and conclusions were reliable and supported. (IIA Standard 2340) Examples could include a supervisory review of in-house audit work by the CAE or other audit staff, or a review of outsourced work by the CAE or audit coordinator. Examiners should consider whether the institution completed these reviews, and if any concerns were identified, when concluding on audit or review reliability.

- ***Reports:*** **Does the internal audit or review report sufficiently communicate IT and security review results and recommendations, if applicable?** Examiners should consider the following when evaluating the audit or review report:

  - Is the report prepared and communicated in accordance with the institution's guidelines?

  - Is an executive summary or overview included to provide the board with a general conclusion on audit or review results?

  - Is the report accurate, concise, supported, and timely in communicating the audit or review objectives, scope, results, conclusions, and recommendations? (IIA Standards 2330, 2400, 2410, 2420, 2440, and 2450)

  - Are conclusions and recommendations realistic and reasonable, with material and higher risk issues clearly identified and prioritized?

  - Are conclusions and recommendations supported by convincing evidence and persuasive arguments (condition, criteria, cause, and effect)?

  - Do results in the workpapers align with report conclusions?

  - Does the report conclude whether the institution adheres to policies, procedures, and applicable laws or regulations, and whether operating processes and internal controls are effective?

- Does the report address potential vulnerabilities to fraud, if applicable?

- ***Corrective Action:*** **Are management responses to audit or review findings in this area reasonable, complete, and timely? Have corrective actions been effective?** Audits and reviews are only effective if corrective action is taken to remedy the weaknesses identified. As such, there should be a reasonable, complete, and timely management response to the audit or review report. Management commitments and agreements or any areas of disagreement should be documented in the report or in a separate memo or tracking system. (IIA Standards 2500 and 2600) If corrective actions are not resolving the issues or concerns in a timely manner, examiners should further investigate the reasons. For example, this could indicate the audit or review did not sufficiently identify the underlying causes or materiality of weaknesses, sufficient resources are not being directed toward corrective actions, or weaknesses exist in the institution's corrective action process, including board oversight of the process.