| Stmt # | Domain | Assessment Factor | Component | Maturity Level | Declarative Statement | Comment | Examination Approaches |
|---|---|---|---|---|---|---|---|
| 1 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Baseline | Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. | The board or a board committee should be tasked for the oversight of these programs and should ensure compliance with the requirements of the programs by the financial institution's management, employees, and contractors.<br><br>Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to ensure appropriate compliance with the financial institution's policies, standards, and procedures. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Business Continuity Planning (BCP) and Disaster Recovery (DR) to determine compliance with Gramm Leach Bliley Act (GLBA) and other regulatory guidance.<br><br>Review the Board Package (or delegated board committee report) and Meeting Minutes, the IT Steering Committee Meeting Minutes or other oversight committee meeting minutes that have a responsibility for the Information Security and Business Continuity Programs for discussion and approval of the Information security and business continuity programs.<br><br>Discuss with management the information security roles and responsibilities and internal reporting structure to verify appropriate information security and business continuity planning reporting channels exists for staff, management, and the board. |
| 2 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Baseline | Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. | Management is aware of highly visible cyber events through open source reporting, industry alerts, or law enforcement and regulatory alerts. Discussion of cyber events to determine the appropriate response or mitigating actions should be documented in meeting agendas or minutes. | Review the board and/or IT Steering Committee Minutes for discussions on information security topics.<br><br>Discuss with management the frequency and depth of discussions associated with information security risk to include highly visible events and regulatory alerts. |
| 3 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Baseline | Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. | A report by management on the status and effectiveness of the IS program, including the report required by the GLBA guidelines, and the reliability of the institution's BCP should be provided to the board of directors at least annually. Examiners will refer to appropriate guidance and examination handbooks when assessing the relevance and quality of these reports. | Review all applicable board reports that address the status of information security and business continuity programs and determine if they comply with the annual reporting requirement.<br><br>Review the content of the report on the status and effectiveness of the Information Security Program and determine the adequacy based on applicable regulatory guidance and regulations. |
| 4 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Baseline | The budgeting process includes information security related expenses and tools. | The financial institution's budgetary process should include information on security related expenses and tools. Institutions may blend information security expenses with an overall Information Technology or general budget, which may call for additional explanation by management. | Review the information technology budgeting process.<br><br>Determine if the information security expenditures are reasonable and sufficient for the size of the financial institution. |
| 5 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Baseline | Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. | Risks posed by other critical infrastructure sectors [16 sectors defined by Department of Homeland Security (DHS)] may present a material impact to the financial institution if the institution is subject to a cyber-attack or physical event (e.g., attack on a building or structure). The absence of the critical infrastructures can affect the financial institution's ability to restore operations and should be considered when addressing cybersecurity risk. | Obtain and review business continuity plans to verify consideration of other critical infrastructures as part of plan development.<br><br>Discuss with management any planning or coordination with local critical infrastructure organizations and evaluate use of that information in continuity and recovery plans.<br><br>Determine the Recovery time objectives and recovery point objectives are addressed when they relate to critical infrastructures. |
| 6 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Evolving | At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. | The financial institution's risk, complexity, and available resources often dictate the degree to which they separate cybersecurity processes and controls from traditional practices defined by the information security program. Many institutions will not separately implement a cybersecurity program. In this case, evaluate the quality of information security policy, procedures and standards in terms of their contribution to managing cybersecurity risks. | Review the Annual Report to the Board of Directors (or delegated board committee) meeting minutes where the Cybersecurity Program was reviewed and approved.<br><br>Evaluate the quality of information security policy, practices and guidelines in terms of their contribution to managing cybersecurity risks. |
| 7 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Evolving | Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity. | The Gramm Leach Bliley Act (GLBA) Interagency Guidelines Establishing Standards for Safeguarding Customer Information is the predominant legal expectation for financial institutions. Regulatory guidance and/or legal requirements may apply based on products, services, and legal structure. For example, institutions may need to adhere to Sarbanes Oxley (SOX), Payment Card Industry (PCI) Standards, or state legal requirements. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Business Continuity and Disaster Recovery and the Board of Director's meeting minutes to determine who is responsible for identifying and ensuring compliance with applicable regulatory and other legal requirements related by cybersecurity.<br><br>Discuss with Compliance Officer their role in ensuring compliance with legal and regulatory requirements related to cybersecurity at the financial institution. |
| 8 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Evolving | Cybersecurity tools and staff are requested through the budget process. | The budget should include information regarding operating expenses for maintaining effective security over information and systems, and additional resources and capital outlays required for improving security including: replacement of security systems, tools and processes, and for adding additional systems, tools or processes to mitigate security gaps. | Meet with appropriate managers to discuss how IT security initiatives are planned, prioritized and budgeted.<br><br>Review IT strategy and project planning documents that highlight the need for security related resources, tools, or new processes.<br><br>Review the budget process and/or discuss with management how the IT or Information Security staff facilitate budget requests to include review, approval, risk acceptance, and required documentation. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Evolving | There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process. | Management should document and implement the process for determining potential costs associated with cybersecurity incidents of varying impact. This information is used to determine funds for recovery of systems, litigations, and insurance. | Review the budget process and/or discuss with management how the IT or Information Security staff facilitate budget requests to include review, approval, risk acceptance, and required documentation.<br><br>Determine if management considers potential expense associated with cybersecurity incidents.<br><br>Verify how they arrive at estimated expenses and gain insight to their reliance on insurance to minimize expense or loss. |
| 10 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Intermediate | The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities. | The board or a committee thereof should understand cybersecurity risks. They should possess sufficient expertise to be actively engaged in discussions and present a credible challenge to management's representation of risk and governance practices. When they lack sufficient expertise, the board may seek expert consultation to assist with oversight decisions or to build internal knowledge. | Review the board or board committee composition and meetings minutes to determine if the financial institution relies on external experts or internal subject matter experts to supplement knowledge gaps.<br><br>Discuss with management the level of cybersecurity expertise on the board or board related committee. |
| 11 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Intermediate | The standard board meeting package includes reports and metrics that go beyond events and incidents to address threat intelligence trends and the institution's security posture. | Management presents information to the board, in board meetings, pertaining to threats and related trends that are most prevalent and potentially impacting to the financial institution. The objective is to offer information that addresses potential or future risk exposure, which can help identify how management might strengthen the financial institutions security posture.<br><br>The reports presented by management in board meetings provide information that address potential or future risk exposure, which can help identify how management might strengthen the financial institutions security posture. | Review the Board meeting minutes and package to determine if management presents threat analysis and trends.<br><br>Review relevant board packages or IT Steering Committee minutes to evaluate the quality and depth of information provided and note any board questions or discussions. |
| 12 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Intermediate | The institution has a cyber risk appetite statement approved by the board or an appropriate board committee. | Risk appetite can be defined as the amount of risk a financial institution is prepared to accept when trying to achieve its objectives. The statement would define certain risk tolerance metrics that help define high-risk systems and services. Risk appetite statements should be decided by management consensus and not in isolation by any one person or department and are reviewed and approved by the board. | Review the Board meeting minutes and package to determine if the financial institution has an approved risk appetite.<br><br>Review and discuss the process for developing the cyber risk appetite statement(s) and gain insight to the metrics they use to measure stated risk levels. |
| 13 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Intermediate | Cyber risks that exceed the risk appetite are escalated to management. | When cyber risk that exists within the financial institution exceeds the maximum acceptable level outlined in the risk appetite statement there is a defined process to elevate this to management's attention. | Discuss with management how the financial institution handles risk escalation to include risk acceptance, particularly for cyber risks.<br><br>Request documentation to support the cyber risk escalation process indicated by management. This could include applicable Policy, Standards and Guidelines and/or examples. |
| 14 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Intermediate | The board or an appropriate board committee ensures management's annual cybersecurity self-assessment evaluates the institution's ability to meet its cyber risk management standards. | If a financial institution completes an annual cybersecurity self-assessment it should validate the effectiveness of key cybersecurity controls. Cyber risk management standards refers to controls that help a financial institution prevent, detect, and respond to a cybersecurity attack. | Obtain and review any self-assessments conducted by the financial institution and determine if there are assessment findings that identify gaps in meeting standards.<br><br>Determine if the board or committee of the board has reviewed the assessment's findings. |
| 15 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Intermediate | The board or an appropriate board committee reviews and approves management's prioritization and resource allocation decisions based on the results of the cyber assessments. | Management has a methodology to measure and document cybersecurity risks and for determining resources required for mitigating gaps. The board reviews and approves the cyber-risks mitigation plans and the allocation of the required resources. | Review board meeting minutes, board package or supplemental information that evidences the board, or committee reviewed and approved management's priority and resource decisions related to cybersecurity risk.<br><br>Review the Financial Institution's Policy, Standards and Guidelines specific to: Risk Management to determine if the financial institution has a process for the development of priorities, decisions, and resources that may evolve from the findings of their cyber risk assessments. |
| 16 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Intermediate | The board or an appropriate board committee ensures management takes appropriate actions to address changing cyber risks or significant cybersecurity issues. | Because the cybersecurity threat environment is highly dynamic, management should quickly identify and react to external and internal factors that alter the financial institution's risk posture and they should report those changes. The board or committee should be aware of management actions and ensure that they apply sound risk-based decisions and address issues in a timely manner. | Review the Board Package (or delegated board committee report) and Meeting Minutes to determine any management decisions prompted by changes from significant cybersecurity issues. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 17 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Intermediate | The budget process for requesting additional cybersecurity staff and tools is integrated into business units' budget processes. | Requests for resources and tools used to manage cybersecurity risk will often originate in the business units. Distributed budget authority that resides with business unit can be instrumental in identifying cybersecurity resources and control needs that the IT or other operational units may not readily identify. For example, business units may recognize the need for additional security training, increased resources to manage third-party risks, or unique risk management tools to help manage cyber risk. | Discuss with management if business units are authorized to individually request staff and tools related to cybersecurity processes and controls.<br><br>Discuss with management how these requests are coordinated with IT and IS departments and understand how requests are compiled into the financial institution's overall budget. |
| 18 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Advanced | The board or board committee approved cyber risk appetite statement is part of the enterprise-wide risk appetite statement. | Risk appetite can be defined as the amount of risk a financial institution is prepared to accept when trying to achieve its objectives. The financial institution's board or committee thereof should approve, as part of the enterprise wide risk management process, specific risk appetite statements associated with cybersecurity risk. This can prevent cybersecurity risk levels from being isolated or excluded from the enterprise view of risk appetite. | Review the risk appetite statement and determine if that statement is part of the broader enterprise risk appetite.<br><br>Review the Financial Institution's Policy, Standards and Guidelines specific to: Enterprise Risk Management and discuss with management how they include cybersecurity risk as part of the enterprise wide risk statement.<br><br>Review any applicable board or committee minutes that support these discussions and risk decisions. |
| 19 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Advanced | Management has a formal process to continuously improve cybersecurity oversight. | Continuous improvement is a constant process that identifies opportunities to increase efficiency, reduce costs, and enhance processes. This statement asks if management has a formal continuous improvement process (CIP) and if they apply that process to cybersecurity oversight.<br><br>The process should include evaluation of evolving threats, research on cyber-incident trends affecting the financial industry and other sectors, and lessons-learned from cyber-incidents that have occurred at the financial institutions or other institutions. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and Cybersecurity to determine if the financial Institution has documented continuous improvement practices or processes that include cybersecurity.<br><br>Discuss with management recent changes to cybersecurity oversight that resulted from formal improvement activities. |
| 20 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Advanced | The budget process for requesting additional cybersecurity staff and tools maps current resources and tools to the cybersecurity strategy. | Management understands the current level of cybersecurity resources and how those resources are related to the overall cybersecurity strategy, which may be part of an information security strategy. The budget methodology clearly delineates the relationship between resources and strategy. This analysis helps reconcile budget requests with the cybersecurity strategy to identify potential misalignment. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Cybersecurity and Budget and determine if a process exists to map budget requests to stated strategy.<br><br>Discuss with management recent analysis or reviews of cybersecurity resources, budget requests, and strategy.<br><br>Determine if processes identify situations where budget, resources, and strategy did not align or where requests were changed or required further just because they do not map to strategy. |
| 21 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Advanced | Management and the board or an appropriate board committee hold business units accountable for effectively managing all cyber risks associated with their activities. | The financial institution's board or a board committee and management will hold each business unit accountable for managing cyber risk. In some cases, business unit managers who do not understand how to identify cyber risk in their environments may need technical support and training. While the source and type of support and training will vary by institution, it should enable the business manager to effectively carry out responsibilities. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Cybersecurity, Risk Management and discuss with management how business unit managers are held accountable for managing cyber risk in their areas. |
| 22 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Advanced | Management identifies root cause(s) when cyber attacks result in material loss. | It is appropriate for a financial institution to identify the root cause for a successful attack. This ensures accurate and complete remediation and restoration of the affected environment. When the attack results in material loss, identifying the root cause can help management understand the legal and compliance risk, and can minimize reputation risk. For example, if the root cause points to another party or control outside of the financial institution's scope of responsibility, legal risk related to customer law suits might be reduced and the financial institution is in a better position to recapture loss through insurance claims. Understanding root cause can also help minimize reputation risk or restore a damaged reputation. Understanding root cause can also help the financial institution to adjust its policies and processes to prepare for future cyber events. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Incident Response to determine if the financial Institution has processes specific to incident containment, evidence gathering, and investigation, to include forensic processes.<br><br>Review a sample of incident reports to determine if the financial Institution completed a root cause analysis as part of the investigation. |
| 23 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Advanced | The board or an appropriate board committee ensures that management's actions consider the cyber risks that the institution poses to the financial sector. | Cyber-risk, threats, and events impacting a financial institution can proliferate to the systems of other institutions due to inter-connectivity among systems. Cyber-risk can migrate to a service provider and from there to other institutions connected to the service providers or other third-parties connected to the affected institution's systems. | Review the Board Package (or delegated board committee report) and Meeting Minutes to identify evidence of board discussion pertaining to the financial Institutions activities that could present cybersecurity risk to the financial sector.<br><br>Discuss with management specific activities that pose risk and gain insight to how these risks are managed. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 24 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Innovative | The board or an appropriate board committee discusses ways for management to develop cybersecurity improvements that may be adopted sector-wide. | The board and board committee discuss the development of new processes, services, or technologies for the betterment of the financial institution and potentially the financial sector. These institutions may assist with improving financial sector cybersecurity defenses. In this case, the financial institution will be an active leader with financial sector organizations such as the Bankers Information Technology Secretariat (BITS), Financial Services Information Sharing and Analysis Center (FS-ISAC), or other state and national associations within the industry. Activities may include sharing staff expertise, discussing innovative research, or making available to the sector techniques or services applied in their own environments. | Review board package and meeting minutes, or delegated board committee, for evidence of financial sector involvement and leadership.<br><br>Discuss with management specific cybersecurity focused projects or endeavors that resulted in financial sector information sharing and/or the adoption of new processes, services, or technologies. |
| 25 | 1: Cyber Risk Management & Oversight | 1: Governance | 1: Oversight | Innovative | The board or an appropriate board committee verifies that management's actions consider the cyber risks that the institution poses to other critical infrastructures (e.g., telecommunications, energy). | The board or committee should be actively involved in monitoring cybersecurity risks that the financial institution may pose to other critical infrastructures, as well as dependencies on those critical infrastructures. The board or committee should be familiar with the Department of Homeland Security's (DHS) critical infrastructure list and, with management's guidance, the board should be aware of any critical infrastructure that the financial institution's services or activities could impact due to cyber breach. | Review the cybersecurity risk assessment and discuss with management if they have considered and identified risk posed to other critical infrastructures. If so, discuss specific activities that pose risk and gain insight to how these risks are managed.<br><br>Review board package and meeting minutes to identify evidence of board discussion pertaining to activities that present cybersecurity risk to other critical infrastructures. |
| 26 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Baseline | The institution has an information security strategy that integrates technology, policies, procedures, and training to mitigate risk. | The financial institution's IS strategy should align with the long-term business strategies and the technologies used to support these strategies. The IS strategy should consider how changes to business operations affect the financial institution's current information security requirements. The IS strategy should also leverage new technologies to help protect the financial institution from ongoing and emerging threats and risk, including those related to cybersecurity. | Review the IT Strategy and/or IS Strategy for the following: a) considers current technologies and training to identify current and emerging threats and risk; b) includes risk mitigation actions. |
| 27 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Baseline | The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management. | The financial institution should have an IT risk management policy, standards and procedures that align with risk and complexity. This documentation should establish a general framework for ownership of the IT Risk Assessment. Generally, an IT risk management policy should require that the assessment include all operations and business processes supported by technology; and define clear management accountability to include responsibilities of staff that contribute to development. Procedures and operating standards dictate how the policy is implemented and executed. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and Risk Management to determine if the policy establishes the following: a) risk assessment expectations; b) staff accountability and responsibility; c) review, approval, and reporting expectations. |
| 28 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Baseline | The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing. | By sharing threat and incident data with reputable organizations there is potential benefit to the financial sector by enabling other institutions to assess and respond to current attacks. A threat information sharing policy customarily would:<br>a) Include names of organizations (public or private sector) that they wish to communication with;<br>b) Define the type of incident and related information they are willing to share; and<br>c) Outline internal protocols to communicate data to help ensure accuracy and maintain data privacy expectations. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if there is a policy or process for how the financial Institution with the public or private sector regarding incidents. |
| 29 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Baseline | The institution has board-approved policies commensurate with its risk and complexity that address information security. | The board or committee thereof is responsible for overseeing the financial institution's information security program. This oversight includes reviewing and approving information security policies, including approval of the financial institution's written information security program as required by the Gramm Leach Bliley Act (Gramm Leach Bliley Act (GLBA) guidelines. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security.<br><br>Review the Board Package (or delegated board committee report) and Meeting Minutes to determine the date of the most recent board review and subsequent approval of the Financial Institution's Policy, Standards and Guidelines specific to: Information Security. |
| 30 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Baseline | The institution has policies commensurate with its risk and complexity that address the concepts of external dependency or third-party management. | The financial institution's third-party service provider management policy should address core governance activities such as program oversight and accountability, documentation and reporting, and periodic independent review. Also, the GLBA guidelines require institutions to oversee service providers that maintain, process, or otherwise are permitted access to customer or consumer information. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management to determine conformance to regulatory guidance. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 31 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Baseline | The institution has policies commensurate with its risk and complexity that address the concepts of incident response and resilience. | The board and management should have policies, standards and procedures that address how they will detect and respond to incidents. As part of the policies, the institution's management should consider resilience concepts, including third-party relationships. Resilience is the ability of an organization to recover from a significant disruption and resume critical operations or operate within a degraded and disrupted operational environment. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and Business Continuity and Disaster Recovery. |
| 32 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Baseline | All elements of the information security program are coordinated enterprise-wide. | Management can establish an enterprise information security program by setting a strong security culture that begins with board involvement and is expected at all levels of management and staff. The information security function should be a prominent part of all business strategies, practices, policies and procedures. Roles and responsibilities of the information security function should be clearly communicated. All staff should receive ongoing role-appropriate training. Finally, to be effective, management should enforce enterprise-wide security via internal control and process ownership, self-assessment, and periodic independent testing. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security to determine accountability for Information Security Program governance.<br><br>Discuss with management how business units within the organization participate in or directly own various aspects of information security management and activities that are distributed and presented at an enterprise level. |
| 33 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Evolving | The institution augmented its information security strategy to incorporate cybersecurity and resilience. | Cybersecurity, as defined in the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, is the process of protecting consumer and institution information by preventing, detecting, and responding to attacks. Resilience is the ability of an organization to recover from a significant disruption and resume critical operations or operate within a degraded and disrupted operational environment. | Review the IS Strategy to determine the financial institution has incorporated the concepts of cybersecurity and resilience. |
| 34 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Evolving | The institution has a formal cybersecurity program that is based on technology and security industry standards or benchmarks. | Technology and security industry standards or benchmarks can include the following: National Institutes of Standards and Technology (NIST), SANS, International Organization for Standardization (ISO), Payment Card Industry Data Security Standard (PCI-DSS), and Control Objectives for Information and Related Technology (COBIT). The FFIEC Cybersecurity Assessment Tool was developed using many of these frameworks as informative references and is a resource that may be sufficient for this purpose. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Cybersecurity to determine if it is based on a technology and/or security industry standard or benchmark. |
| 35 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Evolving | A formal process is in place to update policies as the institution’s inherent risk profile changes. | The financial institution should establish a formal process that triggers review and possible policy updates whenever the IRP is impacted by internal or external changes. | Review the Inherent Risk Profile and discuss with management any changes from the previous inherent risk profile.<br><br>Determine if the financial Institution has established and documented a process that causes management to consider policy changes when the IRP changes. |
| 36 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Intermediate | The institution has a comprehensive set of policies commensurate with its risk and complexity that address the concepts of threat intelligence. | Threat intelligence gathering involves the acquisition and analysis of this information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance the financial institution’s decision-making. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing.<br><br>Discuss with management the organizations to which they are members, how they gather and analyze information, and how they have acted upon these reports to better their cybersecurity posture. |
| 37 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Intermediate | Management periodically reviews the cybersecurity strategy to address evolving cyber threats and changes to the institution’s inherent risk profile. | The financial institution may have a separate cybersecurity strategy or they may include discussion of cybersecurity risk and threats in their IT or IS strategy. The financial institution should have a process that considers change to the environment and the IRP. The process should also ensure that management update, as needed, the IT, IS and cyber strategy to address emerging threats and change in risk. | Review the Cybersecurity Strategy to determine how often it is reviewed.<br><br>Determine if the financial Institution has established and documented a process that causes management to consider policy changes when the IRP or cyber threat landscape changes. |
| 38 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Intermediate | The cybersecurity strategy is incorporated into, or conceptually fits within, the institution’s enterprise-wide risk management strategy. | Enterprise risk management objectives and actions encompass cybersecurity risk mitigation and acceptance decisions. These decisions align with overall risk tolerance and enable, rather than limit or prohibit, business objectives. | Review the enterprise-wide risk management strategy and cybersecurity strategy, if separate, and determine if they align or are not conflicting.<br><br>Discuss with management if processes exist to update the strategic plan when change occurs. Ask if they have specifically changed the strategic direction or activities based on cyber threat, inherent risk, or increased cybersecurity risk. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 39 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Intermediate | Management links strategic cybersecurity objectives to tactical goals. | Management defines tactical goals to achieve cybersecurity strategic objectives. An objective is a measurable step or action to achieve change or improvement. Tactical goals and planning relate to actions taken day-to-day, and drive results that help achieve the objectives. In this case, tactical goals may include implementation of use of a new anti-malware solution or strengthening employee awareness training. | Review the financial Institution's cybersecurity strategy and discuss the tactical implementation with management. |
| 40 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Intermediate | A formal process is in place to cross-reference and simultaneously update all policies related to cyber risks across business lines. | The financial institution should have a formal process that updates all interrelated policies across business lines. | Review the Inherent Risk Profile and the Financial Institution's Policy, Standards and Guidelines specific to: Policy Governance.<br><br>Determine if the financial Institution has established and documented a process that causes management to consider policy changes when the IRP changes. |
| 41 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Advanced | The cybersecurity strategy outlines the institution's future state of cybersecurity with short-term and long-term perspectives. | Financial institutions should ensure they have an integrated approach to cybersecurity tailored to their business needs and IRP, addressing not only the technical controls implemented, but also the people and organizational elements necessary to improve their cyber security defenses and reduce risk. | Review the financial Institution's cybersecurity strategy and discuss with management the short-term and long-term perspectives for the future. |
| 42 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Advanced | Industry-recognized cybersecurity standards are used as sources during the analysis of cybersecurity program gaps. | The financial institution should apply industry security standards when they analyze cybersecurity risk and gaps in their controls and processes. Industry recognized standards commonly include National Institution on Standards and Technology (NIST) Computer Security Resource Center, the International Standards Organization (ISO), specifically the 27000 series of security standards, and the Control Objectives for Information and Related Technology (COBIT) which provides an IT governance and control framework. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Cybersecurity and discuss with management, their reliance on certain industry standards and frameworks as a basis for establishing security standards. |
| 43 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Advanced | The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructure in the financial services industry. | The Department of Homeland Security designates the financial services industry as a critical infrastructure sector. Each sector individually identifies risks and threats. Large institutions play a particularly important role in terms of critical infrastructure planning because of the systemic impact, to include national or global affect an adverse event could have in the financial sector. Cybersecurity strategies should recognize the financial institution's role in the financial sector as well as dependencies on other critical infrastructures. | Review the cybersecurity strategy to determine if it identifies the financial institution's role as a component of critical infrastructure in the financial services industry.<br><br>Discuss with management how the financial institution's role as a component of critical infrastructure in the financial services industry is communicated. |
| 44 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Advanced | The risk appetite is informed by the institution's role in critical infrastructure. | When the financial institution establishes their risk appetite, management recognizes its role as a critical infrastructure organization and may alter the risk appetite because of that role. | Review the financial institution's risk appetite statement and discuss with management the factors that influenced the development of the statement. |
| 45 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Advanced | Management is continuously improving the existing cybersecurity program to adapt as the desired cybersecurity target state changes. | The financial institution continually incorporates advanced technologies and practices, adapting to a changing cybersecurity landscape. Self-identification of gaps provides a roadmap for achieving the target state which is an ongoing process. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Cybersecurity and cybersecurity strategy.<br><br>Discuss with management the processes used to improve the existing cybersecurity program as the target state changes. |
| 46 | 1: Cyber Risk Management & Oversight | 1: Governance | 2: Strategy / Policies | Innovative | The cybersecurity strategy identifies and communicates the institution's role as it relates to other critical infrastructures. | The Department of Homeland Security designates the financial services industry as a critical infrastructure sector. Each sector individually identifies risks and threats. Large institutions play a particularly important role in terms of critical infrastructure planning because of the systemic impact, to include national or global affect an adverse event could have in the financial sector. Cybersecurity strategies should recognize the financial institution's role in relationship to critical infrastructure sectors. | Review the cybersecurity strategy to determine if it identifies the financial Institution's role as it relates to other critical infrastructures.<br><br>Discuss with management how the financial institution's role as it relates to other critical infrastructures is communicated. |
| 47 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Baseline | An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. | An asset inventory is a comprehensive record of a financial institution's hardware, software (e.g., physical and virtual servers, operating systems, and business applications), and data repositories (e.g., customer information files or storage area network). This record should also include the software utilized and data held at third parties. The record will typically include the device type and software version to help the financial institution manage software updates and patches. Management should keep this inventory current and an independent source should validate its accuracy periodically. | Review the financial institution's asset inventory and compare against the network topology diagram(s) to determine the accuracy of the inventory.<br><br>If there are inaccuracies, discuss with management what processes and tool(s) they have in place to collect and maintain information about each organizational asset. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 48 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Baseline | Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value. | Organizational assets include hardware, systems, data, and applications. Data classification is the identification and organization of information according to its criticality and sensitivity. The financial institution should prioritize assets according to their classification. The asset priority will guide management's decisions regarding internal controls and processes and security standards, and help assess controls applied by contracted third parties. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Data Classification and the IT Asset Inventory to determine if assets are prioritized for protection and/or assigned a protection profile.<br><br>Review the BIA for critical services and determine if systems that support critical services are appropriately classified and prioritized. |
| 49 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Baseline | Management assigns accountability for maintaining an inventory of organizational assets. | Financial institution management should establish clear accountability for the oversight of the asset inventory. Accountability would include asset identification, prioritization, and recordkeeping. Accountability may reside with one person, a department or group, or may be part of an outsourced service. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Asset Management and determine if accountability is assigned for maintaining the inventory of IT assets. |
| 50 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Baseline | A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools. | Change management involves a policy, procedures, and standards that guide a broad range of changes within a financial institution's operating environment. Changes may include configuration changes, such security settings; hardware changes that address obsolescence, routine software releases to include those provided by a third-party, or emergency fixes and patches that eliminate software or other vulnerabilities. Generally, a change management process requires a formal request and approval for any change to a financial institution's systems, hardware, or software. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Change Management and determine if the financial Institution has a process for detecting unapproved or unauthorized changes. |
| 51 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Evolving | The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets. | Management should update the asset inventory at least annually. Management should identify new assets as well as those relocated to another site. Repurposed assets are those where the function has changed. For example, management might format and load a different operating system or application(s) on a device. Sunset assets are those that have become obsolete and require replacement or decommissioning, also known as end-of-life (EOL). | Review the Financial Institution's Policy, Standards and Guidelines specific to: Asset Management to determine how often the asset inventory should be updated.<br><br>Review the documentation supporting the last IT Asset Inventory update to determine if it meets stated policy requirements. |
| 52 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Evolving | The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards. | An asset lifecycle is a process that analyzes and monitors risk associated with organizational assets. Asset monitoring carries through to its termination or disposal. The evaluation of the service or product's security safeguards occurs during a pre-purchase or pre-contract due diligence review. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, System Development Life Cycle (SDLC) to determine if they include review of security safeguards for new products and services.<br><br>If available, review documented analysis related to new services or products that evidence that security is part of due diligence. |
| 53 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Evolving | The institution proactively manages system EOL (e.g., replacement) to limit security risks. | System End of Life (EOL) is a part of the asset life cycle. Hardware, operating systems, and business applications often become obsolete over time. Systems reach EOL because hardware no longer supports upgraded software, or the third-party develops new product offerings or software versions and no longer provides product updates, patches, or releases. Unsupported software can lead to vulnerabilities, or the software may become incompatible with systems that continue to be supported—resulting in increased maintenance costs and instability within the financial institution's operational environment. | Review the Financial Institution's Policy, Standards and Guidelines specific to: System Development Life Cycle (SDLC) and Asset Management to determine the process for managing end-of-life assets.<br><br>Review the IT asset inventory for end of life assets.<br><br>Review board or committee minutes for EOL briefings describing risks involved with legacy items. |
| 54 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Evolving | Changes are formally approved by an individual or committee with appropriate authority and with separation of duties. | The financial institution's change management process should require a formal approval from an individual or committee with appropriate authority. Individuals making the request should not be involved in the review and approval process to ensure separation of duties. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Change Management to determine if an individual or committee is designated as an approving authority for change management requests.<br><br>Request a sampling of Change Management Records and determine if the approval and review of changes follow the process as stated in policy. |
| 55 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Intermediate | Baseline configurations cannot be altered without a formal change request, documented approval, and an assessment of security implications. | A baseline configuration represents an approved set of specifications for a system, or configuration item(s) within a system, such as enabled or disabled functions, or security parameters (e.g., access or password characteristics). A formal change request, approval and analysis of security impacts should be completed prior to changing an existing baseline configuration. | Request a sampling of Change Management Records related to changes in baseline configuration and determine if the changes include a review, security impact analysis and approval as stated in policy, standards, and/or guidelines. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 56 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Intermediate | A formal IT change management process requires cybersecurity risk to be evaluated during the analysis, approval, testing, and reporting of changes. | To ensure cybersecurity risks and vulnerabilities are not introduced with changes, the change management process needs to include a security impact or similar analysis. | Request a sampling of Change Management Records and determine if the changes include security impact analysis as stated in policy. |
| 57 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Advanced | Supply chain risk is reviewed before the acquisition of mission-critical information systems including system components. | The supply chain involves individual suppliers or the combination or interrelationship of third parties that provide or enable mission critical systems and functions. A review of supply chain risk refers to the process of identifying and assessing risks associated with the sequence of processes (failure points) involved in the acquisition of mission critical information systems. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Procurement to determine if management identifies supply chain risk when acquiring organizational assets, particularly for mission critical systems. |
| 58 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Advanced | Automated tools enable tracking, updating, asset prioritizing, and custom reporting of the asset inventory. | Financial institutions may use automated tools or software to manage organizational assets. Automated tools can help maintain data integrity. They enable efficient updates related to asset change and termination; and they help maintain detailed records that capture specific asset information such as hardware type, or software versions. Automated tools are more common when institutions operate large and complex networks or data centers. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Asset Management and discuss with management any automated tools in place to manage the IT asset inventory. |
| 59 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Advanced | Automated processes are in place to detect and block unauthorized changes to software and hardware. | Automated processes or tools can detect and prevent changes to hardware and software and alert management when certain changes are attempted or executed. Management can enable detection and block unauthorized changes through access management controls, or by configuring remediation activities such as blocking IPs, changing privileges, disabling accounts, blocking devices or killing applications. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and discuss with management the automated processes or tools in place to detect and block changes to hardware and software. |
| 60 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Advanced | The change management system uses thresholds to determine when a risk assessment of the impact of the change is required. | Change management threshold risk tolerances are established and documented. When a change falls outside the established thresholds, a risk assessment of the impact of the change is required. Examples of triggers or thresholds include whether the change involves a mission critical asset or storage, transmission, or access to sensitive data. | Request a sampling of Change Management Records and determine if the changes include security impact analysis as stated in policy. |
| 61 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Innovative | A formal change management function governs decentralized or highly distributed change requests and identifies and measures security risks that may cause increased exposure to cyber attack. | Decentralization is common in institutions with multiple locations. The financial institution's change management process should include a methodology that governs decentralized and/or highly distributed changes. The methodology should include a process to measure security risks associated with the change and evaluate how the change affects The financial institution's exposure to cyber threats. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Change Management to determine if the policy addresses decentralized assets. |
| 62 | 1: Cyber Risk Management & Oversight | 1: Governance | 3: IT Asset Management | Innovative | Comprehensive automated enterprise tools are implemented to detect and block unauthorized changes to software and hardware. | Automated tools can detect changes to hardware and software and alert management when certain changes are attempted or executed. Management can enable detection and block unauthorized changes through access management controls, or by configuring systems to disallow physical access to a device (e.g., disabling USB ports). | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and discuss with management the automated processes or tools in place to detect and block changes to hardware and software. |
| 63 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Baseline | An information security and business continuity risk management function(s) exists within the institution. | Each institution must have a written information security program to comply with the Gramm Leach Bliley Act (GLBA) guidelines and should have a business continuity program. The disaster preparedness program is synonymous with the business continuity program. An information security program is the written plan created and implemented by a financial institution to identify and control risks to customer information and customer information systems and to properly dispose of customer information. The plan includes policies and procedures regarding the institution's risk assessment, controls, testing, service-provider oversight, periodic review and updating, and reporting to its board of directors. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Business Continuity and Disaster Recovery to determine conformance with regulatory guidance. |
| 64 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Evolving | The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring, and reporting. | The risk management program should consider the likelihood and impact of cyber threats and identify mitigating controls. The program should also measure, monitor and report the effectiveness of controls and residual risk. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Risk Management and risk management reports to determine if they identify, measure and monitor cyber risk. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 65 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Evolving | Management reviews and uses the results of audits to improve existing cybersecurity policies, procedures, and controls. | Audit results can identify gaps in a financial institution's cybersecurity policies, procedures and controls which management should review and remediate, or accept the risk as necessary. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Policy Governance and Audit Results.<br><br>Review the financial Institution's process for remediating audit findings to determine if the financial Institution updates cybersecurity policies, procedures, or controls as a result of an audit. |
| 66 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Evolving | Management monitors moderate and high residual risk issues from the cybersecurity risk assessment until items are addressed. | Residual risk is the risk remaining after current controls are taken into account. Management should determine their residual risk tolerance level and monitor outliers until risks are mitigated. High and moderate residual cybersecurity risk should be monitored until the risks are addressed or accepted as required by policy. | Review the risk assessment and risk monitoring report and discuss with management efforts to address high and moderate risks. |
| 67 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Intermediate | The cybersecurity function has a clear reporting line that does not present a conflict of interest. | Financial institutions should assign cybersecurity roles with a clear chain of command that ensures clear reporting up and down the chain of command. It is also important that there are no conflicts of interest in the cybersecurity chain of command. For example, there should be separate reporting for the information security function from the operational IT environment. Otherwise, the operational IT environment may be placed in the position of self-reporting its own deficiencies | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Cybersecurity and verify the cybersecurity function on the organizational chart has a clear reporting structure that is independent from the operational IT environment. |
| 68 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Intermediate | The risk management program specifically addresses cyber risks beyond the boundaries of the technological impacts (e.g., financial, strategic, regulatory, compliance). | Cyber risks can lead to financial, strategic, regulatory, and compliance impacts. For example, a data breach can result in customer notification and credit monitoring costs, as well as reputational damage and regulatory fines. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Risk Management and risk management reports to determine whether they analyze the financial, strategic, regulatory and compliance impact of cyber risks. |
| 69 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Intermediate | Benchmarks or target performance metrics have been established for showing improvements or regressions of the security posture over time. | A financial institution should establish a cybersecurity baseline and set benchmarks or target performance metrics. A methodology should be implemented to determine if the financial institution is failing to meet, meeting, or exceeding those established benchmarks. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Cybersecurity to determine if they have established baseline performance metrics.<br><br>Review the cybersecurity risk metrics to determine the financial Institution's performance against the established baseline metrics. |
| 70 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Intermediate | Management uses the results of independent audits and reviews to improve cybersecurity. | Audit results identify weaknesses in a financial institution's cybersecurity program. Management should develop corrective actions to address identified weaknesses. | Review the independent audit results and audit tracking log and determine if the audit concerns are tracked and remediated. |
| 71 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Intermediate | There is a process to analyze and assign potential losses and related expenses, by cost center, associated with cybersecurity incidents. | A cost center can be a business unit or department, or there may be multiple cost centers within a business unit. Analyzing the costs associated with cybersecurity incidents helps a financial institution align and prioritize resources to risks with greater financial impacts. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if there is a process to analyze the potential losses and related expenses, by cost center, associated with cybersecurity incidents.<br><br>Review the risk assessment(s) for the analysis of potential losses and related expenses, by cost center, associated with cybersecurity incidents. |
| 72 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Advanced | Cybersecurity metrics are used to facilitate strategic decision-making and funding in areas of need. | Financial institutions should use cybersecurity metrics to determine where weaknesses or gaps exist within the cybersecurity program. The metrics can then be used to identify trends, make strategic decisions to address those trends, and allocate funding appropriately.<br><br>Cybersecurity metrics can facilitate decision making and improve performance. The metrics should be quantifiable, observable, and use objective data to establish and support the metrics. | Review the cybersecurity risk metrics, IT project list and strategic plan and discuss with management initiatives driven by cybersecurity metrics. |
| 73 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Advanced | Independent risk management sets and monitors cyber-related risk limits for business units. | A financial institution should establish a cybersecurity baseline for each business unit and set benchmarks or target performance metrics for each business unit. A methodology should be implemented to determine if each business unit is failing to meet, meeting, or exceeding those established benchmarks. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security to identify the cybersecurity risk limits for business units.<br><br>Discuss with management the process to determine if business units are complying with established risk limits. |
| 74 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Advanced | Independent risk management staff escalates to management and the board or an appropriate board committee significant discrepancies from business unit's assessments of cyber-related risk. | When significant discrepancies in a business unit's cybersecurity risk assessment exists within the institution, a process to elevate the discrepancies to management's or the Board's attention should be in place. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Risk Management to determine if there is a process in place to escalate significant discrepancies in the business unit's assessments of cyber-related risk. |
| 75 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Advanced | A process is in place to analyze the financial impact cyber incidents have on the institution's capital. | A financial institution should track the financial impact cyber incidents have on a financial institution's capital. Analyzing the financial impact associated with cybersecurity incidents helps a financial institution align and prioritize resources to risks with greater financial impacts. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if there is a process in place to analyze cybersecurity incidents for financial impacts.<br><br>Review the information security risk assessment and incident report to determine if the financial Institution documents the financial impact of cybersecurity incidents. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 76 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Advanced | The cyber risk data aggregation and real-time reporting capabilities support the institution's ongoing reporting needs, particularly during cyber incidents. | The cumulative effect of multiple cybersecurity risks in the financial institution's environment is aggregated to provide a more complete picture of the risk. During a cyber event, it is important to understand aggregate risk rather than discrete risk. | Review the cyber risk reports and discuss with management the process for aggregating data and the real-time reporting capabilities available. |
| 77 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Innovative | The risk management function identifies and analyzes commonalities in cyber events that occur both at the institution and across other sectors to enable more predictive risk management. | Predictive risk management involves anticipating future cyber threat activity by using current threat intelligence to identify similarities and trends. The financial institution responds to this information by implementing mitigating controls and managing cybersecurity resources. An example would be utilizing cyber threat analysis reports from various sources to predict potential cyber-attacks for which the financial institution may be targeted. | Review the cyber threat analysis for similarities and trends.<br><br>Discuss with management the process for identifying actionable intelligence. |
| 78 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 1: Risk Management Program | Innovative | A process is in place to analyze the financial impact that a cyber incident at the institution may have across the financial sector. | Risk managers should incorporate security issues into their risk assessment process for each risk category. Institutions should ensure that security risk assessments adequately consider potential risk in all business lines and risk categories. An adequate risk assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if there is a process in place to analyze cybersecurity incidents for financial impacts.<br><br>Review the financial Institutions' information security risk assessments, including the risk assessment required by the Gramm Leach Bliley Act (GLBA), and the incident report to determine if the financial Institution documents the financial impact of cybersecurity incidents.<br><br>Discuss with management the process for determining if the financial impact of a cybersecurity incident will have an impact across the financial sector. |
| 79 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Baseline | A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, and customer information systems. | An information security risk assessment is a required component of the written information security program as outlined by the Gramm Leach Bliley Act (GLBA) Standards for Safeguarding Customer Information. As part of the security program, financial institutions are required to perform an information security risk assessment to identity internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information and customer information systems, assess the likelihood and potential damage of these threats, and validate whether policies, procedures, and controls in place are appropriately mitigating risks. | Review the information security risk assessment to determine whether it complies with Gramm Leach Bliley Act (GLBA) requirements. |
| 80 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Baseline | The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls. | Financial institution management should conduct risk assessments to identify potential risks for all internet-based systems, as well as those that process high-risk transactions. Where indicated by their risk assessment, they should implement multifactor authentication and/or other layered controls consistent with FFIEC authentication guidance. | Review the information security or internet banking risk assessment to determine whether it complies with Gramm Leach Bliley Act (GLBA) requirements and regulatory guidance on authentication for all internet-based systems, and systems that process high-risk transactions. |
| 81 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Baseline | The risk assessment is updated to address new technologies, products, services, and connections before deployment. | Any time new technologies, products, services, connections or relationships are added to the existing business environment, management should be responsible for assessing potential risk elevation and the need for additional mitigating controls. In addition, the cyber threat environment is highly dynamic and prominent threats can necessitate revisiting these risk assessments. At least once a year, senior management should review the entire risk assessment to ensure relevant information is appropriately considered. | Review the risk assessment(s) to determine whether it includes new technologies, products and services prior to deployment. |
| 82 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Evolving | Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships. | Cybersecurity related risks should be identified, reviewed and analyzed as part of the financial institution's risk assessment processes. New products and services as well as outsourced relationships have the potential of introducing new or expanding existing cybersecurity risks. Such risks should be evaluated to determine whether appropriate controls are in place. | Review the risk assessments, including the risk assessment required by the Gramm Leach Bliley Act (GLBA) to determine whether they identify the cybersecurity risks stemming from new products, services, or relationships. |
| 83 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Evolving | The focus of the risk assessment has expanded beyond customer information to address all information assets. | The Gramm Leach Bliley Act (GLBA) guidelines require an information security risk assessment for all assets that contain or transmit customer information. This expands the risk assessment to include all information assets even if they do not directly contain or transmit customer information. This is important because many times bad actors will compromise a less important, less secure asset then pivot to information assets with customer information. | Review the financial Institutions' information security risk assessments, including the risk assessment required by the Gramm Leach Bliley Act (GLBA) guidelines to determine whether they address information assets that do not directly contain or transmit customer information but could be leveraged indirectly to pose a threat. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 84 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Evolving | The risk assessment considers the risk of using EOL software and hardware components. | System End of Life (EOL) is an established part of the overall product life cycle. EOL occurs as existing technologies are replaced by newer more functional technologies. EOL components carry increased risk of vulnerabilities due to lack of ongoing support and development of security patches. Inconsistent software and hardware updates can make them non-compliant, and vulnerable to malicious activity. | Review the financial Institutions' information security risk assessments, including the risk assessment required by the Gramm Leach Bliley Act (GLBA) to determine it includes end of life assets.<br><br>Review the Inventory of Software and Hardware, often maintained in a Configuration Management Database (CMDB), to determine if the financial Institution has end of life assets. |
| 85 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Intermediate | The risk assessment is adjusted to consider widely known risks or risk management practices. | Risk assessments are not a one-time activity. Risk assessments should be updated to the most current information regarding widely known risks and risk management practices to assist management and the board in making informed decisions. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Risk Management and the Information Security Risk Assessment to determine if the financial Institution updates the risk assessment as risks are identified.<br><br>Discuss with management the triggers for updating the risk assessment. |
| 86 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Advanced | An enterprise-wide risk management function incorporates cyber threat analysis and specific risk exposure as part of the enterprise risk assessment. | The threat intelligence analysis process is integrated with the Enterprise risk management process to ensure the risk of relevant threats are analyzed and mitigating controls or alerts can be implemented. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Enterprise-Wide Risk Management and the risk assessment to determine whether the risk assessment process includes an analysis of cyber threats and risks. |
| 87 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Innovative | The risk assessment is updated in real time as changes to the risk profile occur, new applicable standards are released or updated, and new exposures are anticipated. | The financial institutions' risk profile changes as products, technology and transaction volumes change. Management should consider the risks associated with these changes as they happen and update the risk profile accordingly. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Enterprise Wide Risk Management and discuss with management the triggers and frequency for updating the risk assessment. |
| 88 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Innovative | The institution uses information from risk assessments to predict threats and drive real-time responses. | Predictive risk management involves anticipating future cyber threat activity by using current threat intelligence. Information in the risk assessment can help a financial institution identify similarities and trends. The financial institution responds to this information by implementing mitigating controls and managing cybersecurity resources. | Review the risk assessment(s) and discuss with management how information in the risk assessment is used to predict threats and drive real-time responses. |
| 89 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 2: Risk Assessment | Innovative | Advanced or automated analytics offer predictive information and real-time risk metrics. | A proactive cyber risk management approach involves developing threat intelligence capabilities based upon real time data collection and metrics. For example, a security information and event management (SIEM) tool may be used to correlate data and produce real time alerts. | Discuss with management the tools and automated processes used to develop predictive risk analyses and metrics. |
| 90 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Baseline | Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems. | A well-planned, properly structured audit program is essential to evaluate risk management practices, internal control systems, and compliance with corporate policies concerning IT-related risks at institutions of every size and complexity. Effective audit programs are risk-focused and promote sound IT controls across the financial institution. To determine what risks exist, management should prepare an independent assessment of the financial institution's risk exposure and the quality of the internal controls associated with the development, acquisition, implementation, and use of information technology (i.e. new products, services, and delivery channels). | Review the audit schedule and audit report(s) to determine whether the scope and frequency of independent testing is consistent with the risk-based audit program schedule. |
| 91 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Baseline | The independent audit function validates controls related to the storage or transmission of confidential data. | An effective IT audit program should promote the confidentiality, integrity, and availability of information systems. Confidential data can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception. Unauthorized disclosures or modifications compromise the confidentiality or integrity of the data. | Review the audit schedule and audit report(s) to determine whether the scope of independent testing includes the validation of controls related to the storage or transmission of confidential data.<br><br>Specifically, determine if the audit scope includes tests of access controls for data storage and validates the encryption of data "at rest" and "in transit". |
| 92 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Baseline | Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance). | Information captured in logs is critical to detecting malicious activity and provide incident responders with crucial evidence for investigations. Logs may be modified by attackers, including insiders, to hide malicious activity. IT Operations management should periodically review all logs for completeness and ensure they have not been deleted, modified, overwritten, or compromised. In addition, audit should validate that appropriate logging controls and processes are functioning properly. | Review the auditor's IS risk assessment and audit report to determine if the auditor's testing included a review of the controls related to logging of security-related events |
| 93 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Baseline | Issues and corrective actions from internal audits and independent testing/assessments are formally tracked to ensure procedures and control lapses are resolved in a timely manner. | Auditors should identify weaknesses, review management's plans for addressing those weaknesses, monitor their resolution, and report to the board as necessary on material weaknesses. Proper remediation is a basic and essential component of effective audit oversight. There should be a formal tracking process through remediation and a reporting process which assigns responsibility and keeps management well informed of progress. | Review the board package (or delegated board committee report) and meeting minutes or the IT Steering Committee meeting minutes and determine if management has included all audit findings on the tracking sheet.<br><br>Review the tracking sheet for timely completion based on the criticality of risk. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 94 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Evolving | The independent audit function validates that the risk management function is commensurate with the institution's risk and complexity. | The risk management function is an essential part of corporate governance. Complex institutions should have a more robust risk management function. There should be an independent review and evaluation to validate its effectiveness. | Review the Risk Management Audit and Audit Risk Assessment to determine the audit scope and frequency.<br><br>Determine if the audit validates that the risk management function is commensurate with the financial Institution's risk and complexity. |
| 95 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Evolving | The independent audit function validates that the institution's threat information sharing is commensurate with the institution's risk and complexity. | An effective cybersecurity risk management program will include threat intelligence and information sharing practices. The appropriate practice should be commensurate with the risk and complexity of the financial institution. For instance, for smaller institutions that are non-complex and have a low inherent risk profile, threat information sharing may be sufficient. Whereas a more complex and higher risk profile institution should have a formal robust threat intelligence program in place. Independent audit is responsible for validating that appropriate risk management practices are in line with the risk and complexity of the financial institution. | Review the Risk Management Audit and Audit Risk Assessment to determine the audit scope and frequency.<br><br>Determine if the audit validates that the threat information sharing process is appropriate for the financial Institutions size and complexity. |
| 96 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Evolving | The independent audit function validates that the institution's cybersecurity controls function is commensurate with the institution's risk and complexity. | An effective audit program evaluates risk management practices, internal control systems, and compliance with corporate policies concerning IT-related risks. Cybersecurity controls are an integral part of the financial institution's information security control environment and like all control systems, independent audit is responsible for validating that they are effective and commensurate with the financial institution's risk profile. | Review the risk assessment to determine the audit scope and frequency.<br><br>Review any applicable audits to determine if they validate that the cybersecurity controls process is appropriate for the financial Institutions size and complexity. |
| 97 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Evolving | The independent audit function validates that the institution's third-party relationship management is commensurate with the institution's risk and complexity. | An effective audit program evaluates risk management practices, internal control systems, and compliance with corporate policies concerning IT-related risks. Risk management practices like third party relationship management should be commensurate with the financial institution's risk profile and validated by independent audit. | Review the risk assessment to determine the audit scope and frequency.<br><br>Review any applicable audits to determine if they validate that the cybersecurity controls process is appropriate for the financial Institutions size and complexity. |
| 98 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Evolving | The independent audit function validates that the institution's incident response program and resilience are commensurate with the institution's risk and complexity. | An effective risk-based auditing program will cover all of a financial institution's major activities. The frequency and depth of each area's audit will vary according to the audit risk assessment. An effective risk assessment process describes and analyzes the risks inherent in a given line of business. The audit risk assessment will drive the scope and frequency of updates to the audit program's procedures. Auditors should update the risk assessment at least annually, or more frequently if necessary, to reflect changes to internal controls or the operating environment. | Review the Audit Risk Assessment(s), Incident Response Audit and Disaster Recovery Audit to determine the audit scope and frequency.<br><br>Determine if the audits validate that the financial Institution's incident response program and resilience are commensurate with the financial Institution's risk and complexity. |
| 99 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Intermediate | A formal process is in place for the independent audit function to update its procedures based on changes to the institution's inherent risk profile. | An effective risk-based auditing program will cover all of a financial institution's major activities. The frequency and depth of each area's audit will vary according to the audit risk assessment. A risk assessment process to describe and analyze the risks inherent in a given line of business. The audit risk assessment will drive the scope and frequency of updates to the audit program's procedures. Auditors should update the risk assessment at least annually, or more frequently if necessary, to reflect changes to internal controls or the operating environment. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Audit and determine if it addresses procedural updates based on changes to the inherent risk profile. |
| 100 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Intermediate | The independent audit function validates that the institution's threat intelligence and collaboration are commensurate with the institution's risk and complexity. | An effective cybersecurity risk management program will include threat intelligence and information sharing practices. The appropriate practice should be commensurate with the risk and complexity of the financial institution. For instance, in smaller institutions that are non-complex and have a low inherent risk profile, threat information sharing may be sufficient. Whereas a more complex and higher risk profile institution should have a more formal and robust threat intelligence program in place. Independent audit is responsible for validating that appropriate risk management practices are in line with the risk and complexity of the financial institution. | Review the Audit Risk Assessment(s) and Cybersecurity Audit to determine the audit scope and frequency.<br><br>Determine if the financial Institution's threat intelligence and collaboration are commensurate with the financial Institution's risk and complexity |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 101 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Intermediate | The independent audit function regularly reviews management's cyber risk appetite statement. | The cyber risk appetite statement serves as the basis to determine whether risk acceptance decisions are within the financial institution's acceptable risk tolerance range. Risk tolerance levels can change based on changes in the financial institution's operating environment and threat landscape. Therefore it is important that their risk appetite statements is regularly reviewed by independent audit. | Review the Audit Risk Assessment(s) to determine the audit scope and frequency.<br><br>Determine if the cyber risk appetite statement is regularly reviewed by internal audit. |
| 102 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Intermediate | Independent audits or reviews are used to identify gaps in existing security capabilities and expertise. | Independent audits or reviews should be used to evaluate the effectiveness of a financial institution's IT control environment. The audit process should validate that current security controls are in fact working properly, as well as assess whether the financial institution has the appropriate level of expertise to effectively manage these security controls. The audit report should identify gaps in existing security capabilities and expertise. | Review the IT General Controls Audit to determine if it includes comments or findings related to personnel, capabilities and expertise. |
| 103 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Advanced | A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across the sector. | The audit risk assessment should not be limited to the major activities/operations of the financial institution. Given the evolving threat landscape across the financial sector, the risk assessment should address potential impacts and analyze whether additional procedures are necessary to validate that appropriate controls are in place. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Audit and determine if it addresses procedural updates based on changes to the Inherent Risk Profile.<br><br>Discuss with management the triggers or process to update the independent audit procedures based on changes to the financial sector cyber threat landscape. |
| 104 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Advanced | The independent audit function regularly reviews the institution's cyber risk appetite statement in comparison to assessment results and incorporates gaps into the audit strategy. | Assessment results can indicate whether the control environment, services or activities and risk acceptance decisions are within the financial institution's acceptable risk tolerance range. Audit strategy should be expanded to include gaps between risk appetite and assessment results. | Review the Audit Risk Assessment and the Cyber Risk Appetite to determine if there are any gaps in the assessment.<br><br>Discuss with management the process for incorporating gaps into the audit strategy. |
| 105 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Advanced | Independent audits or reviews are used to identify cybersecurity weaknesses, root causes, and the potential impact to business units. | Independent audits or reviews may include penetration tests, vulnerability assessments, information technology and/or information security audits, and social engineering tests to identify cybersecurity weaknesses. Root cause analysis is a process to determine the underlying reason for a control failure or undesired outcome, rather than simply addressing the symptom while the underlying weakness remains. | Review control testing exceptions to determine if the independent auditor identified the root cause of any control failures. |
| 106 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Innovative | A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across other sectors the institution depends upon. | For example, the financial sector is highly dependent on the energy and telecommunications sector. Cyber threats which target these sectors with high interdependence may warrant additional investment in power or communications resilience or additional controls to protect sensitive data (i.e. transmitted across the telecom infrastructure). The independent audit function should update its procedures to adjust for these increased cyber threats. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Audit and determine if there is a process to update procedures based on changes to the evolving threat landscape across other sectors the financial Institution depends upon.<br><br>Discuss with management the triggers or process to update the independent audit procedures based on changes to the other sectors. |
| 107 | 1: Cyber Risk Management & Oversight | 2: Risk Management | 3: Audit | Innovative | The independent audit function uses sophisticated data mining tools to perform continuous monitoring of cybersecurity processes or controls. | Internal audit collects and leverages operational reports and metrics from the use of data mining tools to identify control exceptions and possible control failures. | Review data mining tool reports and discuss with management how this information is collected and used. |
| 108 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Baseline | Information security roles and responsibilities have been identified. | Financial institution management should ensure the institution has sufficient expertise to oversee and manage their IT security operations. If there are gaps, management should obtain the needed expertise by outsourcing or improving security training for current security staff. Employees should be provided security training covering the financial institution's policies and procedures on an appropriate frequency and should periodically certify their understanding and awareness of these policy and procedures. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security to determine the financial Institution has established information security roles and responsibilities.<br><br>Review the organizational chart to determine the reporting structure for information security roles. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 109 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Baseline | Processes are in place to identify additional expertise needed to improve information security defenses. | Financial institution management should ensure the institution has sufficient expertise to oversee and manage their IT security operations. If there are gaps, management should obtain the needed expertise by outsourcing or improving security training for current security staff.<br><br>Funding, along with technical and managerial talent, contributes to the effectiveness of the 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. For example, management may plan to acquire and implement security information and event management (SIEM) tool. Deploying a SIEM requires specialized skills to effectively implement and operate. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and the IT Strategic Plan and discuss with management the process for identifying additional security expertise.<br><br>Review specialized training provided to individuals with designated information security roles. |
| 110 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Evolving | A formal process is used to identify cybersecurity tools and expertise that may be needed. | A comprehensive enterprise security risk assessment can help determine information security resource needs for a financial institution. IT enterprise security risk assessments are performed to assess, identify and modify the overall security posture and to enable security, operations, financial institution management and other personnel to collaborate and view the entire organization from an attacker's perspective. This process can assist in obtaining financial institution management's commitment to allocate resources and implement the appropriate security solutions. | Review the organizational chart and discuss with management the process for identifying gaps in expertise.<br><br>Review the IT Asset Inventory to identify cybersecurity tools and discuss with management if the financial Institution retains the appropriate expertise to operate the tools and if an assessment was conducted to determine if additional expertise or tools are needed. |
| 111 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Evolving | Management with appropriate knowledge and experience leads the institution's cybersecurity efforts. | Management has established minimum standards and certifications for Information security staff and requires continuing specialized education to ensure expertise is maintained. For example, an IT Security Engineer job description may require security certification such as a Certified Information Systems Security Professional (CISSP). | Review the IT Organizational Chart, Information Security Job Descriptions and Resume(s) of information security leadership to determine if management has the appropriate knowledge and experience. |
| 112 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Evolving | Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position. | Management has established minimum standards and certifications for Information security staff and requires continuing specialized education to ensure expertise is maintained. | Review the IT organizational chart, Information Security job descriptions and resume(s) of information staff to determine if individuals in these roles have the appropriate knowledge and experience. |
| 113 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Evolving | Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk. | Financial institutions should conduct background verifications for prospective employees, contractors and third-party vendors with similar access to confidential or sensitive data, systems, or facilities. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Human Resources and Third-Party Service Provider Management to determine whether the financial Institution has a process for conducting background verifications on employees, contractors and Third-Party service providers.<br><br>Review management reports summarizing background checks to validate the timing and frequency. |
| 114 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Intermediate | The institution has a program for talent recruitment, retention, and succession planning for the cybersecurity and resilience staffs. | Effective workforce planning entails having the right number of people with the right skills working in the right jobs at the right time. Cyber threats continue to grow in number and sophistication. The ability to protect and defend a financial institutions' infrastructure and data depends on the financial institution's ability to acquire and retain individuals with the knowledge, skills and ability to ensure the confidentiality, availability and integrity of the financial institution's assets. A security program should be organized and staffed to accomplish its mission. | Review institution's HR programs addressing recruiting of key security staff.<br><br>Review the succession plan for key critical security and resilience personnel. |
| 115 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Advanced | The institution benchmarks its cybersecurity staffing against peers to identify whether its recruitment, retention, and succession planning are commensurate. | Financial institutions can obtain peer data on cybersecurity staffing from various sources such as SANS, Information Systems Audit and Control Association (ISACA) and industry published salary surveys. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Human Resources to determine if the financial Institution has a process for benchmarking their cybersecurity staffing against peers.<br><br>Discuss with management the benchmarking process for cybersecurity staffing. |
| 116 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Advanced | Dedicated cybersecurity staff develops, or contributes to developing, integrated enterprise-level security and cyber defense strategies. | Financial institutions at this level should have dedicated staff or departments for handling cybersecurity. As part of their responsibilities they will determine the current state of security throughout the financial institution and determine the desired or target state. Once established, they will establish the strategy to get to the target state. | Review the IT organizational chart to determine if there are dedicated cybersecurity staff.<br><br>Discuss with management the process for developing the cyber defense strategies. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 117 | 1: Cyber Risk Management & Oversight | 3: Resources | 1: Staffing | Innovative | The institution actively partners with industry associations and academia to inform curricula based on future cybersecurity staffing needs of the industry. | The National Initiative for Cybersecurity Education (NICE) is a national initiative to address the cybersecurity workforce needs of government and the private sector. Institutions can participate on related public-private partnership initiatives between government, academia, and the private sector. | Discuss with management whether the financial Institution has an outreach program to assess any partnerships with universities and how they aid in assessing necessary changes in curricula direction.<br><br>Review the Cybersecurity strategy and discuss with management to determine the level of involvement planned with industry and universities. |
| 118 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Baseline | Annual information security training is provided. | The financial institution should have an organizational-wide information security training program designed to increase employees' awareness of information security threats and knowledge of information security controls. The training program should consider the evolving and persistent threats and should include annual certification that personnel understand their responsibilities. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security to determine if it includes requirements and timeframes for mandatory training for employees, contractors and third parties.<br><br>Review the training records to determine that employees, contractors and third parties have completed the required training. |
| 119 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Baseline | Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues. | The information security training program should support policy awareness and compliance, and be frequently updated to address the various types of cyber-threats (phishing, social engineering, DDoS, account takeover, ransomware, etc.). Training should describe the threats, the attack vectors, and the impact on the targeted institution's systems. | Review the security training material content to assess if it includes incident response and current cyber threats.<br><br>Discuss with management how content is updated to address emerging issues. |
| 120 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Baseline | Situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts. | An effective information security awareness program should be implemented throughout the financial institution. This program should quickly incorporate current cyber threats applicable to the financial institution as they are identified and communicate key information to staff and contractors to mitigate the threat. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security to determine if the financial Institution has a process to validate situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts.<br><br>Review a sampling of situational awareness materials to determine if materials were distributed according to policy. |
| 121 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Baseline | Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials). | The financial institution should inform customers of current cyber threats. A method for informing the financial institution's customers and stakeholders of cyber threats and their role in cybersecurity is to provide relevant information on the financial institution's website. The site should also include security requirements that customers should follow, and the respective security responsibilities of the financial institution and the customers. | Review the customer awareness materials provided by the financial Institution. |
| 122 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Evolving | The institution has a program for continuing cybersecurity training and skill development for cybersecurity staff. | Financial institution management should develop a formal cybersecurity training program that includes learning goals and objectives specific to skill sets needed by the cybersecurity staff. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security for specialized training requirements for cybersecurity staff.<br><br>Review the training records of cybersecurity staff to determine if they receive additional training. |
| 123 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Evolving | Management is provided cybersecurity training relevant to their job responsibilities. | Financial institutions should develop a cybersecurity training program that includes learning goals and objectives that aligns cybersecurity with employee's job responsibilities. Management and senior executives should receive training to understand their roles and perform their responsibilities. | Review the training program to determine if it includes specific training requirements for management and staff consistent with their job descriptions.<br><br>Review a sample of training materials and training records for selected employees and managers to determine whether the training was completed as required. |
| 124 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Evolving | Employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility. | Privileged users include network, systems and database administrators that are granted elevated system access privileges and permissions. These individuals should have additional training that focuses on the management of systems' security and the judicious use of their privileged access. | Review the training program to determine if it includes specific training requirements for privileged users and other individuals granted elevated access based on user levels and responsibilities. |
| 125 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Evolving | Business units are provided cybersecurity training relevant to their particular business risks. | Financial institutions should develop a cybersecurity training program that addresses the cyber risks that might impact a business unit's mission and objectives. | Review the training program to determine if it includes specific training requirements and content for business units based on the issues identified in the business unit risk assessment or cyber risks that might impact a business unit's mission and objectives. |
| 126 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Evolving | The institution validates the effectiveness of training (e.g., social engineering or phishing tests). | Financial institutions should validate the effectiveness of their cybersecurity training. By employing techniques such as phishing campaigns or social engineering exercises financial institutions can identify areas of focus to provide additional training. | Review the most recent social engineering test for scope and purpose to determine if it reflects real world sophistication and effectively assessed staff training.<br><br>Discuss with management if any other validation methods are used by internal audit or management. |
| 127 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Intermediate | Management incorporates lessons learned from social engineering and phishing exercises to improve the employee awareness programs. | Management should ensure that results from social engineering testing and phishing exercises are used to shape future training initiatives that address identified weaknesses. | Review management's responses to testing results and discuss how the program has been updated to reflect issues identified in the social engineering exercises. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 128 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Intermediate | Cybersecurity awareness information is provided to retail customers and commercial clients at least annually. | Cybersecurity awareness information that addresses ongoing cybersecurity risk should be delivered to both retail and commercial customers of a financial institution. The information should be updated periodically to reflect new cybersecurity risk. The materials should be updated as needed but at least annually. | Review customer awareness materials and discuss with management how the financial Institution's materials are distributed to customers and at what frequency. |
| 129 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Intermediate | Business units are provided cybersecurity training relevant to their particular business risks, over and above what is required of the institution as a whole. | Cybersecurity training should be aligned with the level of cybersecurity risk that exists within a business unit. For example, a mobile business unit with company-issued mobile devices or laptops could require additional security training specific to the risks associated with device portability and fewer security layers than those protecting internal network users. | Review the training program to determine if it includes specific training requirements and content for business units based on the issues identified in the business unit risk assessment or cyber risks that might impact a business unit's mission and objectives. |
| 130 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Intermediate | The institution routinely updates its training to security staff to adapt to new threats. | Information security training should be current and relevant. As cybersecurity threats change, training should be adapted to address the changing threat landscape. | Review the training materials and discuss with management the process or triggers for updating its training to security staff to adapt to new threats. |
| 131 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Advanced | Independent directors are provided with cybersecurity training that addresses how complex products, services, and lines of business affect the institution's cyber risk. | Members of the board of directors should be included in the cybersecurity training plan. The board of directors should receive training to understand the potential cyber risk of implementing business decisions as part of their duties. | Review the Board Package (or delegated board committee report) and Meeting Minutes for discussions on cybersecurity training for members of the board. |
| 132 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 1: Training | Innovative | Key performance indicators are used to determine whether training and awareness programs positively influence behavior. | The financial institution has defined metrics and related objectives for training and awareness programs that it measures, reports and tracks over time. For example, number of malware exposure incidents due to employees clicking on links in email messages. | Review the Key Performance Indicators (KPI) that evidence the completeness and effectiveness of cyber-training. |
| 133 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 2: Culture | Baseline | Management holds employees accountable for complying with the information security program. | Management should implement processes to ensure employees know and understand their information security responsibilities. Employees should provide a signed acknowledgment, indicating that they have read, understand, and agree to abide by the rules that describe their responsibilities and expected behavior with regard to their information security roles and responsibilities. For instance, employees may be required to review and signoff on information security policies annually. Policies should also provide for disciplinary action if the employee fails to follow them. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Acceptable Use Policies and Employee Handbook to determine if it addresses employee's accountability for cybersecurity. |
| 134 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 2: Culture | Evolving | The institution has formal standards of conduct that hold all employees accountable for complying with cybersecurity policies and procedures. | Management should implement processes to ensure employees know and understand their information security responsibilities. For instance, employees may be required to review and signoff on information security policies annually. Policies should also provide for disciplinary action if the employee fails to follow them. The financial institution may have a formal code of conduct that holds employees accountable for information security. | Review the Employee Handbook and Employee Code of Conduct to assess if they address compliance with cybersecurity policies. |
| 135 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 2: Culture | Evolving | Cyber risks are actively discussed at business unit meetings. | Cyber risks should be actively discussed outside of the information security unit. Cyber risks to the financial institution should be discussed across all business units within the organization. | Discuss with management whether business unit meetings include discussion and recommended actions on cyber risks. |
| 136 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 2: Culture | Evolving | Employees have a clear understanding of how to identify and escalate potential cybersecurity issues. | A process should be in place and understood by all management and employees on what steps need to be taken to identify cyber risk and the appropriate methods and channels to escalate potential cyber security issues. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and Incident Response to determine if the financial Institution has a process for escalating and reporting cybersecurity concerns.<br><br>Review incident response plan to identify whether it includes an escalation process. |
| 137 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 2: Culture | Intermediate | Management ensures performance plans are tied to compliance with cybersecurity policies and standards in order to hold employees accountable. | Management should implement processes to ensure employees know and understand their information security responsibilities. Documented performance plans should be updated to include a financial institution's cybersecurity policies and standards. Employees should be held accountable for knowing, understanding, and practicing those standards. | Review a sample of performance plans and determine if they are tied to compliance with cybersecurity policies and standards. |
| 138 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 2: Culture | Intermediate | The risk culture requires formal consideration of cyber risks in all business decisions. | Consideration of cyber risks should be embedded in strategic and tactical planning activities and not managed as a downstream, separate function. A formal process should be instituted that ensures that cyber risks to the financial institution are considered across all business units within the organization. | Review the Strategic Planning Process and Tactical Planning Process to determine how cybersecurity related risks impact the financial Institution. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 139 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 2: Culture | Intermediate | Cyber risk reporting is presented and discussed at the independent risk management meetings. | Cyber risk reporting should be developed, presented and discussed in independent risk management meetings. This enables management to measure, monitor, and control cyber risk to the fullest extent possible. | Review cyber risk reports and risk management meeting minutes to determine if cyber risks are discussed at independent risk management meetings. |
| 140 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 2: Culture | Advanced | Management ensures continuous improvement of cyber risk cultural awareness. | Management should strive for continuous improvement in cybersecurity cultural awareness. Cybersecurity cultural awareness should permeate all aspects of the institution and its stakeholders and include the board of directors, management, employees and customers. | Discuss with management their activities for expanding cultural awareness of cyber risks. |
| 141 | 1: Cyber Risk Management & Oversight | 4: Training & Culture | 2: Culture | Innovative | The institution leads efforts to promote cybersecurity culture across the sector and to other sectors that they depend upon. | When it has the opportunity and capability, a financial institution should take the lead in efforts to promote a cybersecurity culture across the financial sector and other dependent sectors. | Discuss with management the level of participation by institutions in promoting cybersecurity culture across the sector and to other sectors that they depend upon. |
| 142 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Baseline | The institution belongs or subscribes to a threat and vulnerability information sharing source(s) that provides information on threats (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC], U.S. Computer Emergency Readiness Team [US-CERT]). | Vulnerabilities and emerging threats are ever changing and increasing. Situational awareness is considered foundational to effective cybersecurity risk management. As a result, financial institutions should subscribe to information sharing resources that include threat and vulnerability information for situational awareness. There are many sources of information such as US-CERT, critical infrastructure sector information sharing and analysis centers (ISACs), industry associations, vendors, and federal briefings such as InfraGard. | Review the list of threat and vulnerability information sharing source(s) and determine whether sources are sufficient.<br><br>Review the board package (or delegated board committee report) and meeting minutes or the IT Steering Committee meeting minutes to determine if threat and vulnerability information is adequately shared. |
| 143 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Baseline | Threat information is used to monitor threats and vulnerabilities. | Threat information is readily available from a variety of resources available to institutions. As threat and vulnerability information is gathered, management should determine if it is applicable to the organization. For example, institutions can monitor threats and vulnerabilities by visiting information sharing resources such as US-CERT or FS-ISAC, on a regular basis and/or by subscribing to alerts, warnings and RSS feeds of threat and vulnerability information from the information sharing resources. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process for monitoring threat and vulnerability information gathered from information sharing sources. |
| 144 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Baseline | Threat information is used to enhance internal risk management and controls. | As threat and vulnerability information is gathered, management should determine if it is applicable to the organization. If so, management should perform a risk analysis of the threat and implement compensating controls. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing, Risk Management to determine if there is a process for integrating threat information into risk management processes.<br><br>Review the risk management reports for examples where threat information is analyzed for risks to the financial institution. |
| 145 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Evolving | Threat information received by the institution includes analysis of tactics, patterns, and risk mitigation recommendations. | Threat information gathered should include enough detail to become actionable intelligence. Information received provides context to the threat by providing a more in-depth analytic product that ties together related threat and intruder activity, describing the activity, how to detect it and mitigation and remediation measures. | Review the threat intelligence to determine if it includes enough information to prompt action by the financial Institution. |
| 146 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Intermediate | A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources. | A formal threat intelligence program should include documented processes for receiving threat and vulnerability information from various sources. The program should provide procedures for analyzing threat information and a standardized reporting format. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a formal threat intelligence program.<br><br>Review threat intelligence reports to determine if they are incorporated into the risk assessment. |
| 147 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Intermediate | Protocols are implemented for collecting information from industry peers and government. | Documented practices for collecting information could include:<br>• Defining the requirement.<br>• Validating the sources<br>• Standardization of information (format)<br>• Personnel identified to receive the information<br>• Controls on dissemination (e.g., Traffic Light Protocol) | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if they have a process for collecting threat intelligence information. |
| 148 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Intermediate | A read-only, central repository of cyber threat intelligence is maintained. | Appropriate personnel have the ability to access the threat repository. The threat intelligence repository should be read only to preserve the integrity of the information and the source. | Review the repository settings to determine permissions are set to "read-only" access and discuss with management / staff the content housed in the repository. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 149 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Advanced | A cyber intelligence model is used for gathering threat information. | Cyber intelligence model refers to the entire cyber intelligence function, addressing items such as strategy, budget, processes, policies, procedures, and resources including staffing. A cyber intelligence model includes a documented methodology for the collection, processing, integration, evaluation, analysis, and interpretation of available information. Specific components or considerations include:<br>• Establishing a threat profile for the function or service that includes characterization of likely intent, capability, and target of threats to the function/service;<br>• Prioritizing and monitoring threat information sources that address all components of the threat profile;<br>• Analyzing and prioritizing identified threats; and<br>• Addressing threats according to the assigned priority. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution is using a cyber threat intelligence model for gathering information. |
| 150 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Advanced | Threat intelligence is automatically received from multiple sources in real time. | To allow for timely analysis and response to potential threats and vulnerabilities, threat intelligence gathering should leverage automated feeds. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process for automatically receiving threat intelligence. |
| 151 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Advanced | The institution's threat intelligence includes information related to geopolitical events that could increase cybersecurity threat levels. | Threat intelligence includes information that may not be cyber specific, but could have cyber consequences. Cyber threat actors may either be motivated by geopolitical events or use those events to enable attacks. For example, Iran was cited as the source of disruptive DDoS attacks against major U.S. institutions in apparent retaliation for Western economic sanctions aimed at halting its nuclear program. Local political events could also have consequences on international locations. | Review the threat intelligence reports for geopolitical threat indicators or information. |
| 152 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Innovative | A threat analysis system automatically correlates threat data to specific risks and then takes risk-based automated actions while alerting management. | A threat analysis system correlates threat information to a financial institution's vulnerabilities and other factors to provide the financial institution with a risk calculation. The threat analysis system integrates with intrusion prevention, intrusion detection, and data loss prevention technologies to provide alerts and real-time remediation of threat activity. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a threat analysis system.<br><br>If the financial Institution has a threat analysis system, discuss with management how the system assigns risk levels in order to determine the appropriate actions for automated responses. |
| 153 | 2: Threat Intelligence & Collaboration | 1: Threat Intelligence | 1: Threat Intelligence and Information | Innovative | The institution is investing in the development of new threat intelligence and collaboration mechanisms (e.g., technologies, business processes) that will transform how information is gathered and shared. | The financial institution procures and/or builds information sharing technologies that push threat information to non-security parts of the organization that may be targeted by those threats. The financial institution enables non-security parts of the organization to easily provide threat information to the security function.<br><br>For example, a software solution designed to facilitate the collection of cyber threat intelligence from various sources, convert it into an industry standard language, and provide timely information to users. | Review the Intelligence Strategy and discuss with management any new threat intelligence and collaboration mechanisms being developed or acquired. |
| 154 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Baseline | Audit log records and other security event logs are reviewed and retained in a secure manner. | All systems, including network devices should have logging enabled. Logs should be stored in a centralized read-only repository and have a retention process to ensure the integrity and availability of log information. Logs should be reviewed regularly as perpetrators often seek to delete audit or security logs to eliminate evidence of malicious or unauthorized activity. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Network Management & Monitoring to determine if the financial Institution has a process for reviewing audit logs and security event alerts.<br><br>Review the sample of log reviews and alerts to determine if audit logs and security event logs are reviewed in accordance with policy.<br><br>Discuss with management the process for securing and retaining logs. |
| 155 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Baseline | Computer event logs are used for investigations once an event has occurred. | System event logs provide incident responders with crucial evidence in identifying and investigating malicious activity. Financial institution management should consider the value of log data when designing and implementing a log management infrastructure. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and discuss with management how logs are used to support incident response activities and investigations. |
| 156 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Evolving | A process is implemented to monitor threat information to discover emerging threats. | Such a process would typically be documented and address the scope and frequency of monitoring as well as an analysis of the pertinence of the threat to the financial institution. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process to monitor threats continuously to identify emerging threats.<br><br>Review examples of threat intelligence analysis for emerging threat analysis. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 157 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Evolving | The threat information and analysis process is assigned to a specific group or individual. | Threat Intelligence Analysis is a specialized skill set. Management should ensure that a qualified individual or group of individuals are assigned to review and analyze threat information. | Discuss with management where within the organization the threat intelligence function resides.<br><br>Review the IT organizational chart, or consult with management, to determine the individuals assigned to the Threat Intelligence Analysis function. |
| 158 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Evolving | Security processes and technology are centralized and coordinated in a Security Operations Center (SOC) or equivalent. | A security operations center (SOC) is a facility where information systems are monitored for information security related events. It provides centralized visibility and coordination to identify and manage information security incidents or events. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a SOC or equivalent implemented to centralize and coordinate security operations. |
| 159 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Evolving | Monitoring systems operate continuously with adequate support for efficient incident handling. | Device and network monitoring technologies should provide real-time, actionable information to inform and support the incident response function. Examples include Intrusion Detection or Intrusion Prevention Systems. | Review the sample reports and alerts from the financial Institution's device and network monitoring solutions and discuss with management how these reports support the incident response or incident handling functions. |
| 160 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Intermediate | A threat intelligence team is in place that evaluates threat intelligence from multiple sources for credibility, relevance, and exposure. | Management should establish a dedicated group to perform threat information analysis. Management should develop and implement standard practices for evaluating information based on the source of the information and its relevance to the financial institution. | Review the organizational chart to determine the individuals assigned to the Threat Intelligence Analysis function. |
| 161 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Intermediate | A profile is created for each threat that identifies the likely intent, capability, and target of the threat. | A threat profile includes identification of threat scenario campaigns and for each campaign selecting critical assets, threat actors, and threat scenarios. Threat profiles contain both background context on the threat as well as indicators of compromise related to the file and network-based traits of the threat. Creating a threat profile provides institutions with the necessary information to prioritize threats and the allocation of resources for mitigation. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing and determine if the financial Institution has a process for creating and managing threat profiles.<br><br>Review a sample threat profile to determine if it identifies the likely intent, capability, and target of the threat. |
| 162 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Intermediate | Threat information sources that address all components of the threat profile are prioritized and monitored. | The financial institution should maintain prioritized sources of threat information related to attackers' malware, network infrastructure, and tactics in the network, motivations, targeting, and post-attack activity. Information on new threats relevant to the financial institution leads to the creation of new threat profiles. New information on previously known threats is, as a matter of practice, added to existing threat profiles. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing and determine if the financial Institution has a process for prioritizing and monitoring threat sources.<br><br>Discuss with management the process for prioritizing and monitoring threat sources. |
| 163 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Intermediate | Threat intelligence is analyzed to develop cyber threat summaries including risks to the institution and specific actions for the institution to consider. | Threat analysis summaries convert technical information into business language to inform senior executives and non-technical resources. This allows them to make informed risk based decisions on how to reduce or mitigate cyber threats. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process for developing threat intelligence summaries for senior management.<br><br>Review a sample of threat intelligence summaries to determine if they include risks to the financial Institution and specific actions for the financial Institution to consider. |
| 164 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Advanced | A dedicated cyber threat identification and analysis committee or team exists to centralize and coordinate initiatives and communications. | A dedicated group within the financial institution is responsible for receiving all threat information, analyzing it, and communicating, as appropriate, to other parts of the financial institution for strategic, operational and tactical purposes. | Review the organizational chart to determine individuals assigned to the threat identification and analysis function and discuss with management if there is a dedicated function for centralizing and coordinating initiatives and communications within that function. |
| 165 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Advanced | Formal processes have been defined to resolve potential conflicts in information received from sharing and analysis centers or other sources. | Threat information from multiple sources can be conflicting and inaccurate. To ensure the accuracy, technical competency and degree of diligence is coming from a trusted source the financial institution's threat intelligence team should have formal documented processes for evaluating the credibility of threat information. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process to validate the accuracy and resolve conflicts in threat intelligence. |
| 166 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Advanced | Emerging internal and external threat intelligence and correlated log analysis are used to predict future attacks. | Financial institutions can use shared internal and external threat information such as indicators, tactics, and tools to develop proactive defense strategies. Integrating this information with correlated log analysis can provide a financial institution with early warning indicators to predict future attacks. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process for performing predictive analysis of cyber threat information. |
| 167 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Advanced | Threat intelligence is viewed within the context of the institution's risk profile and risk appetite to prioritize mitigating actions in anticipation of threats. | Threat intelligence analysis is incorporated into the financial institution's risk management process. Mitigation of identified threats should be prioritized according to the financial institution's risk tolerance. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process for prioritizing threat mitigation.<br><br>Discuss with management the process for prioritizing threat mitigation. |
| 168 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Advanced | Threat intelligence is used to update architecture and configuration standards. | The financial institution recognizes when threat intelligence is related to vulnerabilities in their technology infrastructure and has policies and procedures to quickly address those vulnerabilities in hardware, software and infrastructure components. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process to update architecture and configuration standards based on threat intelligence. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 169 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Innovative | The institution uses multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and geopolitical events to predict potential future attacks and attack trends. | Financial institutions can use shared internal and external threat information such as indicators, tactics, and tools to develop proactive defense strategies. Integrating this information with correlated log analysis can provide a financial institution with early warning indicators to predict future attacks. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process for performing predictive analysis of cyber threat information.<br><br>Discuss with management to determine if alerts, internal traffic flows, and geopolitical events are included in the analysis performed to predict potential future attacks and attack trends. |
| 170 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Innovative | Highest risk scenarios are used to predict threats against specific business targets. | Organizations define threat scenarios to describe how the events caused by a threat source can contribute to or cause harm. Development of threat scenarios is analytically useful, since some vulnerabilities may not be exposed to exploitation unless and until other vulnerabilities have been exploited. Analysis that illuminates how a set of vulnerabilities, taken together, could be exploited by one or more threat events is therefore more useful than the analysis of individual vulnerabilities. In addition, a threat scenario tells a story, and hence is useful for risk communication as well as for analysis. | Discuss with management how the results of table top tests are used to predict and assess the likelihood of threats against specific business targets. |
| 171 | 2: Threat Intelligence & Collaboration | 2: Monitoring & Analyzing | 1: Monitoring and Analyzing | Innovative | IT systems automatically detect configuration weaknesses based on threat intelligence and alert management so actions can be prioritized. | A financial institution can employ technologies that ingest threat information, vulnerability information, and IT configuration data to proactively identify the highest risk of attack to specific IT systems in the financial institution. | Discuss with management their process for incorporating threat intelligence into automated processes for detecting configuration weaknesses. |
| 172 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Baseline | Information security threats are gathered and shared with applicable internal employees. | Threat information is collected and analyzed for dissemination to the appropriate individual(s) for action. When establishing and reviewing information sharing rules, the financial institution should request input from their legal and privacy officials, information owners, the management team, and other key stakeholders to ensure that the sharing rules align with the organization's documented policies and procedures. | Discuss with management how threat intelligence reports are communicated to applicable staff. |
| 173 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Baseline | Contact information for law enforcement and the regulator(s) is maintained and updated regularly. | Financial institutions should establish relationships with law enforcement and maintain contact information to facilitate information sharing and rapid incident response. Ongoing communication is essential for fostering trust, establishing stronger ties and continuously improving information sharing practices. Local, state and Federal law enforcement agencies can be helpful partners to financial institutions in the fight against fraud and security issues; therefore, institutions are encouraged to establish positive working relationships to enhance information sharing about emerging trends. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response, Business Continuity to determine if the financial Institution maintains emergency contact information for law enforcement |
| 174 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Baseline | Information about threats is shared with law enforcement and regulators when required or prompted. | Management is required to report breaches to law enforcement and their primary regulator when the financial institution suspects or detects unauthorized access to customer information systems. In addition, institutions should notify customers in accordance with state law requirements and otherwise should notify customers as described in the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice." Institutions should have formal procedures that establish when and under what circumstances to notify and involve regulators, customers, and law enforcement. Further, through information sharing relationships, institutions should share unusual cyber activity. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing and Incident Response to determine if the financial Institution has formal processes for notifying law enforcement of threats.<br><br>Discuss with management any incidents that required notification to law enforcement since the last exam. |
| 175 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Evolving | A formal and secure process is in place to share threat and vulnerability information with other entities. | To protect the confidentiality and the integrity of threat and vulnerability information, institutions should have formal procedures to facilitate information sharing. The financial institution should identify trusted Information sharing partners and ensure secure communication channels are established for dissemination of threat information. Information sharing policies should provide guidance for the handling of confidential data and describe proper safeguards for managing the privacy risks associated with sharing such data. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has formal procedures for the secure communication of threat information with other entities. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 176 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Evolving | A representative from the institution participates in law enforcement or information-sharing organization meetings. | The financial institution should assign individuals to participate in law enforcement or information-sharing organization meetings to receive external threat and vulnerability information. Examples include FBI InfraGard meetings, local ad hoc security groups, and FS-ISAC biweekly threat monitoring conference calls. | Review the list of information sharing partners and discuss with management the level of participation of designated individuals. |
| 177 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Intermediate | A formal protocol is in place for sharing threat, vulnerability, and incident information to employees based on their specific job function. | Information-sharing activities are formally established in policies, standards and processes. These policies, standards and processes are supported by sufficient resources (people, funding, and tools) and include key stakeholders based on function (e.g., connected financial institutions, vendors, sector financial institutions, regulators, internal entities).<br><br>Examples:<br>Notifying call center employees regarding a social engineering attack in a specific area or country.<br>Notifying IT infrastructure of a pervasive vulnerability such as ShellShock. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing and Incident Response to determine if the financial Institution has formal procedures for notifying employees of threats, vulnerabilities and incidents according to their job function. |
| 178 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Intermediate | Information-sharing agreements are used as needed or required to facilitate sharing threat information with other financial sector organizations or third parties. | Threat and vulnerability information is often very confidential in nature. To protect the confidentiality and the integrity of the information, institutions should have formal information sharing agreements that document the nature of the information being shared, handling and storage, ownership, retention, and related matters. These agreements are typically cancellable by either party with minimal notice. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process in place for establishing and maintaining Information-sharing agreements.<br><br>Review a sample of information sharing agreements to understand the nature of the relationship, type of information shared, ownership, retention, etc. |
| 179 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Intermediate | Information is shared proactively with the industry, law enforcement, regulators, and information-sharing forums. | Proactively sharing threat intelligence helps institutions achieve broader cybersecurity situational awareness among external stakeholders. Once validated, threat intelligence should be shared as appropriate. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process for sharing threat intelligence externally with industry peers, law enforcement, regulators, and information-sharing forums. |
| 180 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Intermediate | A process is in place to communicate and collaborate with the public sector regarding cyber threats. | Sharing current relevant threat information with the public sector helps to inform entities quickly analyze potential threats and implement mitigations to reduce the risk associated with threat. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing to determine if the financial Institution has a process for communicating and collaborating with the public sector regarding cyber threats. |
| 181 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Advanced | Management communicates threat intelligence with business risk context and specific risk management recommendations to the business units. | The threat intelligence risk assessment should contain actionable information to assist business units in developing specific mitigating controls and defenses. | Review samples of threat intelligence risk assessments shared with business units for specific risk mitigation recommendations to management. |
| 182 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Advanced | Relationships exist with employees of peer institutions for sharing cyber threat intelligence. | A financial institution's employees can establish threat intelligence sharing relationships directly with peer institutions outside of industry information sharing organizations, public or private. For example, participating in local FBI InfraGard chapter meetings can help establish and foster collaborative relationships. | Review examples of relationships, meeting agendas, attendees and minutes and discuss with management the financial Institution's level of engagement. |
| 183 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Advanced | A network of trust relationships (formal and/or informal) has been established to evaluate information about cyber threats. | It is important to share threat and vulnerability information with other entities. This information is often very confidential. The financial institution should identify a network of trusted partners to securely communicate and evaluate cyber threats. | Review the list of Information Sharing Partners to determine if the financial Institution has established a network of trusted partners for evaluating cyber threats. |
| 184 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Innovative | A mechanism is in place for sharing cyber threat intelligence with business units in real time including the potential financial and operational impact of inaction. | Threat information is processed and delivered with actionable mitigating controls to the appropriate business units real-time. The threats should be prioritized by the level of risk and consequence. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing and determine if the financial Institution has a process for sharing cyber threat intelligence with business units in real time.<br><br>Review the Threat Intelligence Report recommendations to determine if it includes the potential financial and operational impact of inaction. |
| 185 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Innovative | A system automatically informs management of the level of business risk specific to the institution and the progress of recommended steps taken to mitigate the risks. | Enterprise risk management tools enable automatic risk scoring. These tools can also be used to automatically alert management and other personnel when a risk reaches a specific threshold based on predetermined risk factors. | Review the Enterprise Risk Management Tool(s) to determine if the management is automatically informed of the level of business risk specific to the financial Institution and the progress of recommended steps taken to mitigate the risks. |
| 186 | 2: Threat Intelligence & Collaboration | 3: Information Sharing | 1: Information Sharing | Innovative | The institution is leading efforts to create new sector-wide information- sharing channels to address gaps in external-facing information-sharing mechanisms. | The industry's ability to improve threat intelligence gathering, analysis and sharing is becoming more important to respond to the ever changing threat landscape. Institutions should develop new and innovative ways to mature their processes. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Threat Intelligence and Information Sharing and discuss with management their initiatives to improve threat intelligence gathering, analysis and sharing sector-wide. |
| 187 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | Network perimeter defense tools (e.g., border router and firewall) are used. | A financial institution's network perimeter enables or restricts connection to, and communication with, the internet. To control network traffic, the financial institution should use devices such as border routers and firewalls to restrict and filter traffic. These tools should be securely configured and maintained with current operating systems. | Review the network topology diagram(s) and asset inventory to identify the perimeter defense tools in use at the financial Institution. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 188 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. | A firewall is a network device or application that prevents unauthorized access either to or from trusted and untrusted networks. A financial institution or its service provider should establish specific firewall rules that either allow or deny inbound and outbound traffic and access to the network. | Review the network topology diagram(s) and discuss with appropriate personnel how publically facing systems and systems accessed by external parties are protected.<br><br>Confirm management periodically reviews the inbound/outbound traffic firewall rules for publically facing systems.<br><br>Discuss with management who establishes the firewall policy and rules.<br><br>Review the results from the firewall review and determine/verify the review was conducted by a person qualified to render an opinion on such technology.<br><br>Review testing and assessment results for findings and verify all findings were documented in the report, and all findings have been addressed and tracked by the financial Institution. |
| 189 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | All ports are monitored. | Ethernet is a combination of different technologies that physically connect network devices and facilitate data transfer. Many internal networks are Ethernet-based. Certain network devices monitor and control each network connection (ports). Monitoring the financial institution's Ethernet may include alerts when ports are manually enabled/disabled, or when unauthorized devices are plugged into the financial institution's network. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Cybersecurity and, Network Management & Monitoring to verify that they address the need to monitor all Ethernet and Wireless ports.<br><br>Review summary list of network controls, monitoring systems and the risk assessment to determine if port monitoring is included.<br><br>If management is receiving automated alerts, determine by what method and under what circumstances an alert will be received. |
| 190 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | Up to date antivirus and anti-malware tools are used. | Antivirus and anti-malware tools help protect data and systems by detecting malicious code or malware to include viruses, Trojans, rootkits, and destructive malware. Having antivirus and malware protection on systems, desktops, laptops, and other devices is critical given today's threats. Institution management should actively manage anti virus and anti-malware software by regularly updating attack signatures. | Review malware mitigation and anti-virus policies and processes and confirm with management that an independent periodic review of anti-virus practices occurs.<br><br>Validate that a process exists to monitor and determine if the software and anti-virus signature updates are occurring on all workstations, servers, and devices. |
| 191 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced. | Industry configuration standards are published by various organizations. Sometimes a vendor will offer suggested minimum security settings. The financial institution should develop security standards based on “hardening” or configuration guidelines. These guidelines establish specific baseline security controls and may be recorded in the form of checklists or templates. Hardening or configuration guidelines should be applied when implementing new assets and when validating compliance with stated standards. | Review the hardening or configuration guidelines or standards to determine whether they are based on industry standards and determine if they are enforced on the financial institution's information technology assets.<br><br>Confirm an independent review of the hardware, operating system, and application configuration hardening and configuration guidelines exists.<br><br>Review third-party or internal audits, vulnerability assessments, or penetration tests to determine configuration gaps or non-compliance with stated standards |
| 192 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | Ports, functions, protocols and services are prohibited if no longer needed for business purposes. | Systems (desktops, servers, other devices) and hardware (networking, printers, etc.) have many ports, functions, protocols and services that are not required for daily use. Upon installation, manufacturer configuration often enable or open functions or services as a default to enable access. These should be disabled and documented in configuration standards. | Discuss with management the process for scanning IT assets for unnecessary services or misconfiguration before they are deployed to the production environment.<br><br>Confirm there has been independent testing to determine if ports, functions, protocols and services are disabled when necessary.<br><br>Review the results from the firewall review and determine if the findings and recommendations include the adoption of configuration standards, or security templates. |
| 193 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. | Controls should exist for all changes to applications and hardware. Some changes warrant less scrutiny prior to the change such as identification of a bad actor IP address being added to the firewall, or a call center employee requiring a PC software update, while other changes may warrant significant advanced oversight and approval. In either case, all changes should have a review and approval process. | Determine which individuals are authorized to implement changes to configuration standards and settings for hardware, operating systems, and applications.<br><br>Choose a sample of changes to determine if these changes required the proper review, approval, documentation (e.g. ticketing system), and post implementation validation.<br><br>Optional: If warranted, request a demonstration of the change control / issue tracking tool. Review key reports that summarize change activity. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 194 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | Programs that can override system, object, network, virtual machine, and application controls are restricted. | Financial institutions use programs, often referenced as utility programs, to help analyze, configure, optimize or maintain computer devices on a network. They enable many different tasks and may allow a user to create, modify, move, rename, copy, or delete code and data. If not controlled and restricted to authorized users, utility programs can impact network performance and disable key controls. Institutions should restrict access and monitor all use of utility programs. | Identify authorized utility program users and determine if access rights align with role and responsibilities and there are no segregation of duties conflicts. |
| 195 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | System sessions are locked after a pre-defined period of inactivity and are terminated after pre-defined conditions are met. | Sessions on systems and applications that handle sensitive member data should have controls in place to lock or close the session, and require users to re-authenticate. This may include the security settings or parameters for inactivity in Windows Active Directory and the core processing system. | Review unique network and application standards that define session lock and termination parameters. (i.e., Active Directory Inactivity Timeout Setting).<br><br>Discuss with management and determine if there is an independent periodic review of network and application standards that define session lock and termination parameters. (i.e., Active Directory Inactivity Timeout Setting) |
| 196 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | Wireless network environments require security settings with strong encryption for authentication and transmission. (*N/A if there are no wireless networks.) | A risk assessment on the use of a wireless network should be conducted prior to implementation. Once implemented, wireless networks, particularly those on the financial institution's network, should include end-to-end encryption and strong authentication protocols such as WPA2 + AES. | Review the Financial Institution's Policy, Standards and Guidelines specific to Wireless Access.<br><br>Determine the type of wireless access (internal network access, guest account, public) offered by the financial institution.<br><br>Confirm that internal wireless network access is reviewed by an independent third party annually. |
| 197 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Evolving | There is a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and internal network(s). | Firewalls are implemented to prevent threats from infiltrating a financial institution's demilitarized zone (DMZ) and internal network. A DMZ by definition must be accessible to the public, however it can be protected from unwanted access with a router or firewall between it and the internet service provider. | Review the network topology diagram(s) and discuss with appropriate personnel (or if network management is outsourcing - the vendor) how the DMZ and network perimeter are protected.<br><br>Review the network topology diagram(s) and identify the number of network segments and number of firewalls between the internet, DMZ, and internal networks. |
| 198 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Evolving | Antivirus and intrusion detection/prevention systems (IDS/IPS) detect and block actual and attempted attacks or intrusions. | Anti-virus software and intrusion detection or prevention systems help identify unusual activity by analyzing network traffic or code and alerting or take action, such as blocking traffic that enters the network. Anti-Virus protection should be deployed on all resources. In instances where anti-virus protection cannot be deployed, management should and provide mitigating measures in the financial institution's risk assessment.<br><br>An Intrusion prevention system (IPS) should be fully deployed throughout the financial institution. Ideally, both host and perimeter IPS exist. The Host IPS should be placed inline (in the direct communication path between source and destination), while the perimeter IPS would be in front of or directly behind the perimeter firewall. Both should be actively analyzing and taking automated actions on all traffic flows that enter the network. | Review network topology diagram(s) to determine IPS implementation and placement in the network.<br><br>Discuss with management their controls and tools used in detecting and blocking malicious activity.<br><br>Review any current audit reports or penetration tests that attest to effectiveness. |
| 199 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Evolving | Technical controls prevent unauthorized devices, including rogue wireless access devices and removable media, from connecting to the internal network(s). | Technical controls are security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. Examples of technical controls may include authentication, audit trails, logs, encryption, access control lists, integrity checks, intrusion detection systems (IDS), antivirus, firewalls, routers, Data Loss Prevention (DLP) solutions and network access control solutions. | Determine if the financial Institution has identified network access points and evaluate how they monitor these for unauthorized access. |
| 200 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Evolving | A risk-based solution is in place at the institution or Internet hosting provider to mitigate disruptive cyber attacks (e.g., DDoS attacks). | Identification of disruptive cyberattacks such as Distributed Denial of Service (DDOS) relies on a coordinated collection and analysis of performance data and alerts. Many risk-based network tools are available to monitor uptime and system responsiveness. When an attack is identified, the financial institution or its provider should closely investigate data and alerts, identify issue root cause, and respond accordingly. The financial institution should have devised different mitigation approaches, using internal or external resources that align with their risk exposure. DDoS mitigation approaches include both managed service providers and infrastructure solutions. | Review the risk assessment for threats from cyber attacks and identify the controls they have in place to address this risk.<br><br>Discuss with management what measures, if any, are in place to mitigate disruptive cyber attacks both at the financial Institution and through third-party service providers. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 201 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Evolving | Guest wireless networks are fully segregated from the internal network(s). (*N/A if there are no wireless networks.) | A guest network can be wired and/or wireless. To be fully segregated from the internal network, guest networks should connect to their internet service provider (ISP) outside the firewall. | Review the wireless network diagram and verify guest networks, if implemented at the financial Institution, are fully segregated.<br><br>If guest wireless is implemented at the financial Institution, discuss with management the controls in place to fully segment guest wireless networks from the internal network. |
| 202 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Evolving | Domain Name System Security Extensions (DNSSEC) is deployed across the enterprise. | The Domain Name System (DNS) is the system that translates domain names (ex: www.google.com) into an IP address. Domain Name System Security Extensions (DNSSEC) is a suite of extensions that add security to the DNS protocol by enabling DNS responses to be validated. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks. Full deployment of DNSSEC will ensure the end user is connecting to the actual web site or other service corresponding to a particular domain name. | Review the evidence provided, if any, and discuss with management their implementation of Domain Name System Security Extensions (DNSSEC). |
| 203 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Evolving | Critical systems supported by legacy technologies are regularly reviewed to identify for potential vulnerabilities, upgrade opportunities, or new defense layers. | Legacy technologies refer to an application, system, or component which is significantly aged and may be difficult to manage, maintain and sufficiently protect against todays threats and vulnerabilities. The financial institution should have an asset inventory of all critical systems, dependencies, and interdependencies which identify legacy technologies. Those legacy technologies should be scanned regularly for vulnerabilities and the results should be reviewed and accepted by the IT steering committee or the board of directors. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Vulnerability Management and determine if it addresses the need to regularly review and identify vulnerabilities in critical systems, components, and applications.<br><br>Review the IT Steering Committee Minutes for discussions of legacy technologies.<br><br>Discuss with management their processes to identify and manage legacy systems and technologies. |
| 204 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Evolving | Controls for unsupported systems are implemented and tested. | Unsupported operating systems and components may introduce significant risk to the financial institution, as updates, patches, and fixes are no longer available. Compensating controls implemented to protect against the threats to unsupported systems should be implemented and periodically tested. For example, Windows XP is an unsupported operating system and could place a financial institution at increased risk of compromise if compensating controls, such as network segmentation or isolation, are not properly implemented | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Asset Management and discuss with management the controls in place for unsupported or end-of-life assets and systems. |
| 205 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Intermediate | The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks. | Segmenting is evidenced by separate local area networks (LANs) or virtual local area networks (VLANs) (supported by a unique subnet) for each floor or department at a site, for each branch, and most definitely between public facing and private sections of the network. It might include a separate LAN for automated teller machines (ATMs). LANs are defined as being able to communicate with each other. Only specific devices can communicate between LANs.<br><br>Financial institutions should implement subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks. Connections to external networks or information systems are only allowed through managed interfaces consisting of boundary protection devices [routers, firewalls, virtual private network (VPN) devices] arranged in accordance with an organizational security architecture. | Review the network topology diagram(s) for the financial Institution and determine how the network is segmented.<br><br>Discuss with management the controls in place to establish trust and security zones within the network. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 206 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Intermediate | Security controls are used for remote access to all administrative consoles, including restricted virtual systems. | Remote administration means a defined number of individuals within the financial institution or its contractors or vendors receive privileged access rights that include remote access capabilities. Remote access (e.g., mobile device or offsite workstation) enables network troubleshooting, update, and maintenance. These users often have access to highly critical systems and data; therefore, the financial institution must establish strong security controls and closely monitor all access.<br><br>There are many types of remote administration tools. Some are built into operating systems such as Windows, Linux, and Mac OS X, while others are available as commercial or open-source solutions.<br><br>Security controls such as encryption, access roles and privileges, strong authentication, patching, access logging, and auditing should be in place to effectively protect against the numerous risks that remote administration poses to the financial institution. | Confirm with management the business justification for authorized remote access to the financial Institution.<br><br>Review the risk assessment to identify controls that exist to protect and monitor remote access sessions. |
| 207 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Intermediate | Wireless network environments have perimeter firewalls that are implemented and configured to restrict unauthorized traffic. (*N/A if there are no wireless networks.) | A perimeter firewall separates the financial institution's internal networks from the Internet, a public network residing on the "edge" or externally facing network, and controls all traffic. A perimeter firewall should exist on any wireless network segments to prevent unauthorized traffic from entering the network. | Review the network topology diagram(s) to determine if the traffic flowing between network environments is protected by a firewall. Additionally, ask for evidence to show ALL Wireless Access Points coincide with the asset inventory. |
| 208 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Intermediate | Wireless networks use strong encryption with encryption keys that are changed frequently. (*N/A if there are no wireless networks.) | Wireless network encryption is a strong control to ensure data is not accessed by unauthorized systems and people. The level of encryption determines the strength of the control. Wireless Encryption Protocol (WEP) and Wi-Fi Protected Access (WPA) utilize encryption which can be broken easily. WPA2-type encryption should be used in an enterprise environment. | Agree with modification: If there is no audit or assessment, then the examiner should determine if encryption is appropriate.<br><br>Verify, through discussion with management or a reporting mechanism, all WAP's are using WPA2 or higher encryption.<br><br>Review the wireless assessment and determine if the assessment was conducted by someone qualified. Verify the result did not encounter any issues with the current version of encryption used among the access points. |
| 209 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Intermediate | The broadcast range of the wireless network(s) is confined to institution-controlled boundaries. (*N/A if there are no wireless networks.) | Wireless broadcast ranges should be confined within the boundaries of the financial institution to prevent wireless leakage into areas accessed by the public. Access points can be tailored to limit their broadcast areas. | Review the wireless heat map report to determine the broadcast coverage and ranges of all the access points within the financial Institution. |
| 210 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Intermediate | Technical measures are in place to prevent the execution of unauthorized code on institution owned or managed devices, network infrastructure, and systems components. | A variety of technical controls (security controls are considered technical controls) can be used to prevent execution of unauthorized code on institution owned devices, infrastructure, and system components. Examples of such technical controls are: Access Control Lists (ACLs), Routers, Encryption, Antivirus, Data Loss Prevention (DLP), Firewalls, Intrusion Prevention System (IPS), Usernames, passwords, and Terminal Access Controller Access Control System (TACACS). | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Asset Management and Mobile Code to determine if the financial Institution has established implementation guidance for the acceptable code technologies and usage restrictions.<br><br>Discuss with management the controls or tools in place to prevent execution of unauthorized code on the network and mobile devices. |
| 211 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Advanced | Network environments and virtual instances are designed and configured to restrict and monitor traffic between trusted and untrusted zones. | In a virtual environment a single physical server can operate and process data for several individual operating systems and related applications. These combined resources are referred to as virtual instances, or virtual machines. A virtual instance resides within the overall network environment. The manner in which these traditional physical devices and virtual instances communicate, transfer data, and store information is governed by secure configuration and active monitoring that help establish trusted and untrusted segments or zones. Controls commonly implemented include establishing granular access controls, use of firewalls and routers to properly direct traffic flow, and strong data and user logging capabilities, such as cross system log correlation.<br><br>An independent review should be conducted of the environment itself to ensure security and design gaps are identified. | Review the assessments of the infrastructure and virtual environment and determine if the environments are adequately designed and monitored by the appropriate staff. Additionally, if there are recommendations within the assessments, determine if action was taken to remediate high or critical findings and/or recommendations. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 212 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Advanced | Only one primary function is permitted per server to prevent functions that require different security levels from co-existing on the same server. | For example, there are many types of functions a server could provide such as a web server, a database server, file share server, a single or group of servers functioning to provide loan services, collections, or items processing. The objective is to ensure each server is participating in only one of those roles or functions at a time. If a database server also provides web services (in addition to a database function), this would be a red flag. As would be a file share server which is also used to process loans. | Review the documentation, determine if any of the servers are providing more than one primary function; such as a database server also providing an e-mail function. Each function (database and e-mail) caters to different audiences and requires different levels of access and authorization.<br><br>Discuss with management if they provision servers within only one primary function per server or multiple functions per server |
| 213 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Advanced | Anti-spoofing measures are in place to detect and block forged source IP addresses from entering the network. | In an attempt to bypass a firewall, cyber attackers will try to spoof packets using the internal IP range of a network to make it look like the request originated internally. Enabling the IP spoofing feature on firewalls helps prevent these types of attacks. | Determine how the financial Institution may be blocking IP addresses from the outside. They may be relying solely on the firewall, or a combination of their ISP, ISP router, firewall, and IDS/IPS.<br><br>Discuss with management what anti-spoofing measures are in place to detect and block forged source IP addresses from entering the network. |
| 214 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Innovative | The institution risk scores all of its infrastructure assets and updates in real time based on threats, vulnerabilities, or operational changes. | Using risk scoring, a financial institution can prioritize threats to gather actionable data, implement mitigating measures and ensure effectiveness of security controls to support continuous monitoring activities. Rather than rely on alerts and notifications from event monitoring agents, enterprises can use threat modeling, through timely and accurate inputs, to mitigate and defeat attack scenarios before they fully unfold. | Review the Asset Risk Score Report, if available, and discuss with management the methodology for calculating the risk score for each infrastructure asset. |
| 215 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Innovative | Automated controls are put in place based on risk scores to infrastructure assets, including automatically disconnecting affected assets. | Using risk scoring, a financial institution can prioritize threats and implement mitigating measures. Rather than rely on alerts and notifications from event monitoring agents, the financial institution may use automated alerts and threat modeling to automatically disconnect an affected asset from the network to mitigate and defeat attack scenarios before they fully unfold. | Discuss with management the automated tool(s) and controls in place to monitor infrastructure asset based on their risk scores. |
| 216 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Innovative | The institution proactively seeks to identify control gaps that may be used as part of a zero-day attack. | Every financial institution is at risk for zero-day exploits regardless of size. These exploits will often circulate for months until the vulnerability is made public, leaving financial institutions unprotected.<br><br>For the malicious zero-day exploits to remain valuable and useful, the exploit needs to remain undetected by a financial institution's defense in-depth strategies until after the goal of the attacker has been achieved. The longer the exploit goes undetected, the more potentially lucrative it is.<br><br>The best defense against zero-day exploits are packet inspection methods using behavioral-based, signature-based, statistical-based, and hybrid methods to detect and block zero-day exploits. | Review the risk assessment to determine if the financial Institution has the appropriate controls implemented to protect the financial Institution against zero-day attacks (defense-in-depth strategy).<br><br>Discuss with management their defense-in-depth strategy |
| 217 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Innovative | Public-facing servers are routinely rotated and restored to a known clean state to limit the window of time a system is exposed to potential threats. | On a schedule, public facing servers (web servers) are removed from production, wiped, and restored from a template which has never been placed into production (clean). Today, most environments are virtualized. In an example using virtualization, a public web server would be taken out of production, the working image destroyed, a new "clean" image would be implemented, and the system would be updated, and then placed back into production. The image used would be one that has never been implemented into production, but rather a standard template used to configure all servers or servers of a particular type and function. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Asset Management and Configuration Standards and determine if they contain processes for refreshing the servers in the financial institution's demilitarized zone (DMZ). Specifically; they should include how often servers are refreshed, as well as which servers are refreshed.<br><br>Discuss with management if they routinely rotate and restore public facing servers to a known clean state to limit the window of time a system is exposed to potential threats |
| 218 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | Least privilege refers to the security objective of granting users only the level of access they need to perform their official duties. For example, data entry clerks may not have any need to run analysis reports of their database. For a core processing system, roles and privileges are typically defined based on templates and common job descriptions such as teller, loan officer, collection manager, etc. Where feasible, staff that performs accounting functions and makes G/L entries should not be able to perform transactions on customer accounts. | Discuss with management how privileged user accounts are authorized and monitored.<br><br>Discuss with management how often employee access rights are reviewed.<br><br>Review core users list and determine if employees appear to be included in appropriate security groups.<br><br>Review the security groups' permissions to verify that access is reasonable for that particular position. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 219 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Employee access to systems and confidential data provides for separation of duties. | Separation of duties refers to dividing roles and responsibilities so a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment. | The information security policy should have a statement in it attesting to the commitment of separation of duties in key operational areas. Assessments conducted in those areas should show compliance. |
| 220 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls). | The Account Management process should provide the necessary reviews and authorization (approval) for privileged access when requested. Privileged access refers to the ability to override system or application controls. Good practices for controlling privileged access include: identifying each privilege associated with each system component, implementing a process to allocate privileges and allocating those privileges either on a need-to-use or an event-by-event basis, documenting the granting and administrative limits on privileges, and finding alternate ways of achieving the business objectives. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Administrative Access to determine if the financial Institution has documented practices for requesting, granting and monitoring elevated privileges.<br><br>Discuss with management if any admin user accounts are shared.<br><br>Discuss with management if admin user accounts require stronger passwords than regular users. |
| 221 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | User access reviews are performed periodically for all systems and applications based on the risk to the application or system. | Periodic review of user accounts and access levels (both internal and external) is perhaps the most important information security audit function, consistent with GLBA guidelines for safeguarding customer information and one most institutions should have the capability to perform as an ongoing operational control. User roles can change frequently, and if not managed properly, leads to inactive accounts (i.e. belonging to former employees). The accumulation of inactive accounts can increase cybersecurity risk. | Review the results of user reviews conducted and verify changes to user rights are showing periodic changes and identifying users who no longer require access (transitions, separations, etc.). If user reviews are not capturing any changes, it may not be an effective control.<br><br>Review the violation report and determine it covers ALL the critical applications, systems, and sites.<br><br>Discuss with management how often employee access rights are reviewed and the actions taken when exceptions are identified. |
| 222 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel. | The goal of access control is to allow access by authorized individuals and devices and to disallow access by all others. Authorized individuals may be employees, technology service provider (TSP) employees, vendors, contractors, customers, or visitors. Access should be authorized and provided only to individuals whose identity is established, and their activities should be limited to the minimum required for business purposes.<br><br>A typical change management request for user access should include the request itself, the business purpose or need, who reviewed it, who authorized/denied it, and how long the access is needed. Additionally, user transitions should trigger a change request to ensure as staff leave or transition within the financial institution, permissions and access to information are appropriate to their function. | Review the Identity and Access Management (IAM) policies to determine if a formal process for requesting, modifying and removing access is implemented and followed. Requests should be approved by the manager or system owner.<br><br>Review a sample of documentation supporting access changes. |
| 223 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Identification and authentication are required and managed for access to systems, applications, and hardware. | Financial institution management should ensure all users are identified and authenticated when accessing systems, applications and hardware. Identification of a user is commonly associated with a user account name or login credential, such as a unique identifier, account number or email address. To authenticate a user, a password or passphrase is required. Because single passwords can be a weak form of authentication, critical and high risk systems should feature strong authentication, such as complex passwords (e.g., exceeding 10 multi-character combinations), layered authentication (e.g., a password and a challenge question) or multi-factor authentication (e.g., something known combined with token or biometric). | Review the Financial Institution's Policy, Standards and Guidelines specific to: Identity and Access Management (IAM) to determine if it includes authentication requirements and methods for core and other critical applications and systems.<br><br>Discuss with management if multi-factor authentication is used to access third-party web sites that contain personally identifiable information (PII) or confidential financial information. |
| 224 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Access controls include password complexity and limits to password attempts and reuse. | Strong passwords help mitigate credential guessing and cracking. Password complexity is determined by length and the combination of unpredictable characters. For example, more complex passwords will be at least 8 characters and require lowercase and uppercase letters, digits, and symbols. Access controls also include limiting the number of password attempts, typically three, before a user is locked out. Controls also prohibit the reuse of passwords. This means users are not allowed to enter a new password based on alteration of one character. Instead the system requires an entirely new character string. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Identity and Access Management (IAM) and determine if it provides minimum guidelines in regards to password complexity and password reuse for all critical applications, systems, and services.<br><br>Review provided assessments and tests of controls to determine if password complexity and reuse settings follow the standards within the Information Security Policy and Standards. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 225 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | All default passwords and unnecessary default accounts are changed before system implementation. | Hardware and software are purchased with default passwords that enable an administrator to implement the device or software. The default password is the same for whomever purchases the product and is widely available in public user manuals. They are also very easy to guess or is blank. (e.g., "admin" or "Password1"). If, upon installation, the financial institution does not create a complex password for the default administrative account, the network will be highly vulnerable to attack or employee abuse. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Identity and Access Management (IAM) to determine if there are documented password complexity and reuse guidelines.<br><br>Review the assessments of applications or systems as validation of compliance to the Policy, standard, and guidelines. |
| 226 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Customer access to Internet-based products or services requires authentication controls (e.g., layered controls, multifactor) that are commensurate with the risk. | Financial institutions should conduct risk assessments and use effective authentication methods appropriate to the level of risk. Best practices include:<br>• Selecting authentication mechanisms based on the risk associated with the particular application or service.<br>• Considering whether multi-factor authentication is appropriate for each application, taking into account the standard practice of multi-factor authentication for many forms of electronic banking and electronic payment activities.<br>• Encrypting the transmission and storage of authenticators (e.g., passwords, personal identification numbers (PINs), digital certificates, and biometric templates).<br><br>To ensure the controls are working as designed they should be periodically tested for effectiveness. | Review the risk assessment to determine if controls such as multi-factor authentication and layered controls such as hardware firewalls, application firewalls, IDS/IPS were assessed.<br><br>Discuss with management how customers are authenticated to the home banking environment. |
| 227 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no production environment exists at the institution or the institution's third party.) | Separation of non-production (e.g., development) from the production environment is important to safeguarding the confidentiality and integrity of information. Institutions can establish test environments which may house either live production or test data. These environments should both include strong security controls, logical and physical separation (e.g., firewalls and segmentation), active monitoring, and individual test (usually limited to development staff) and production user access privileges that are regularly reviewed and approved. Gaps in production and test environment controls could lead to unintended data modification, unauthorized access, and malicious or fraudulent activity.<br><br>Examples of controls that should be used to separate non-production from production environments may include:<br>• Development systems segregated from production systems (separated by firewalls and network rules).<br>• Separate development and production roles used for privileged system, application and network access entitlements. | Review the network topology diagram(s) to determine how production and non-production environments are segregated.<br><br>Have management show you on the network diagram how production and non-production environments are segregated. |
| 228 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems. | Physical security controls vary according to the assets at risk (e.g., data, infrastructure, systems). For example, data centers commonly house the financial institution's data repositories and most critical systems. In this case, management should consider physical controls that address all internal and external threats (e.g., unauthorized access, theft, damage) and environmental threats inherent to physical locations. Physical controls may involve devices that detect adverse events and help prevent theft and safeguard the equipment, like surveillance. The devices should provide continuous coverage, send alarms when responses is necessary, and support investigations. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Physical Security to determine if the financial Institution has formal documentation for the implementation and monitoring of physical security controls.<br><br>Review physical security assessment results to determine whether the financial Institution has implemented adequate physical controls and confirm they have been tested and are working as intended. |
| 229 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | All passwords are encrypted in storage and in transit. | Securing user information begins with a proper understanding of security controls and the protection of user passwords. Encrypting passwords in storage and transmission can be achieved by various tools, methods or software specifically designed to protect the confidentiality of passwords. Encrypting communications containing passwords or transmitting cryptographic password hashes instead of plaintext passwords help protect against threats to capture passwords. | Discuss with management the mechanism(s) or controls in place to encrypt all passwords in storage and transit |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 230 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Confidential data are encrypted when transmitted across public or untrusted networks (e.g., Internet). | Financial institutions, as a standard part of their data management practices, should identify and classify confidential data held internally and residing at third parties. Management should understand how that data is used, exchanged, and transmitted and encrypt all confidential data in transit on public or untrusted networks. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security; Data Classification and determine if the financial institution has a process for classifying data and protecting data.<br><br>Review the network topology diagram(s) and data flow diagram(s) and discuss with management if all connections where confidential information is traversing public or untrusted networks is properly encrypted and secured. |
| 231 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Mobile devices (e.g., laptops, tablets, and removable media) are encrypted if used to store confidential data. (*N/A if mobile devices are not used.) | Mobile device encryption, using either hardware or software-based solutions, is a way to secure data on smartphones, tablets, and mobile devices against the loss of information due to a loss or theft. Institutions should ensure any mobile device storing or accessing confidential information has implemented an effective encryption solution.<br><br>The ability to access email does not mean data is downloaded to the device. However, if the device does have the ability to download documents it should be encrypted. Password protection, with a complex password, might be sufficient for a device that cannot download. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Mobile Devices to determine if the financial Institution has documented formal standards addressing the level of encryption that must be present on types of mobile devices identified during the risk assessment.<br><br>Review the IT Risk Assessment and determine if it identifies the types of mobile devices present within the financial Institution and the types of data stored on those types of devices.<br><br>Discuss with management how or what mobile device management (MDM) solution they use to encrypt and manage mobile devices. |
| 232 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. | Financial institutions should secure remote access to and from their critical systems. Typically, remote access to systems and devices are gained through virtual private network (VPN) gateways and remote access technologies such as WebEx or Citrix. Communications should be encrypted to ensure the privacy and confidentiality of information.<br><br>Multi-factor authentication could be in the form of software tokens, financial institution issued certificates, hardware tokens, biometrics or various other forms. The objective is more than one method of authentication, preferably out of band. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Identity and Access Management (IAM) and Remote Access to determine if the financial Institution defines control standards regarding employee and third-party remote access connections.<br><br>Discuss with management whether remote access to critical systems uses encrypted connections and multi factor authentication. |
| 233 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software. | All systems and user devices (desktops, mobile, tablets, servers, etc.) should prohibit installation of unauthorized software, except when performed by an authorized user. This can be accomplished by ensuring the operating system settings do not grant local administrator capabilities and parameters prohibit executable files from launching on the system or device. Financial institutions should not rely on a written or verbal policy alone to enforce this control. | Determine whether the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Acceptable Use, and/or Administrative Access address the level of access, including administrative access, employees are permitted. Verify employees (without administrative access) are unable to install or remove software. |
| 234 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Customer service (e.g., the call center) utilizes formal procedures to authenticate customers commensurate with the risk of the transaction or request. | Call centers/help desks should have a documented protocol for user identification before addressing issues or taking requested actions.<br><br>There are now many methods available to enable caller authentication. Common examples for validating the authentication of a customer calling in to a call center of a financial institution typically include something the user knows, such as recent transactions, current account balance or pin number. For example, a call center representative will request a verbal passcode or phrase from the customer or may ask a random question about the customers profile or banking activity. | Review documentation and identify how customer service representatives authenticate members.<br><br>Review the risk assessment to determine if the controls exist to mitigate the threat of unauthorized access. |
| 235 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Data is disposed of or destroyed according to documented requirements and within expected time frames. | A data destruction policy is a part of the data retention policy. Completing and implementing a data retention policy will help determine where information and data is stored, which makes it easier to delete old data no longer needed. Once the data has been mapped to the stored locations and a retention policy developed outlining how long it should be kept, a disposal process should be formalized and implemented.<br><br>Disposal of electronic information and computer-based media should ensure any residual data, remaining after deletion, is properly removed. To prevent data recovery, sensitive data should be destroyed using techniques such as overwriting or degaussing. | Review the Data Classification, Data Destruction, or Data Retention policy; the policy should address the following:<br>• the length of time data and information will be retained.<br>• a method of destruction for all the various types of data and media either physical or electronic.<br>• the need for formal processes to implement the policy<br>• a method of tracking and logging what is destroyed, how it was destroyed, and when.<br><br>Review the risk assessment to determine if data destruction controls are identified. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 236 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Evolving | Changes to user access permissions trigger automated notices to appropriate personnel. | Changes to access privileges of critical systems should be continuously monitored and any changes to those access privileges should result in an alert and notification to the proper security team to investigate, document, and resolve them. | Review the SIEM logs or other logs for critical systems and devices and confirm that alerts and notifications are going to appropriate staff when changes occurred, and appropriate actions were taken as a result. |
| 237 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Evolving | Administrators have two accounts: one for administrative use and one for general purpose, non-administrative tasks. | System administrators should have two separate accounts. One account should be used for critical tasks requiring elevated privileges and a separate account should be used for all other activities, such as email or Internet use. The use privileged and non-privileged accounts enables more granular monitoring and auditing capabilities. The risk involved with using a privileged account for general activities is the threat of credential theft. If an attacker steals the administrator credentials, they would acquire all privileges assigned to that account. This presents significant risk of malware injection, system manipulation, and data compromise. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Identity and Access Management (IAM) to determine if the financial institution has processes requiring standard User accounts and Administrative accounts have separate logins. For example; LAN Administrators should not be using an Administrative account to perform standard activities such as reading e-mail, opening documents, and other daily non-administrative functions.<br><br>Review the list of Active Directory users to determine if administrators have a standard user account and separate administrator account. |
| 238 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Evolving | Use of customer data in non-production environments complies with legal, regulatory, and internal policy requirements for concealing or removing of sensitive data elements. | Many times development groups rely on production data to populate their development systems in the development, testing, and staging environments. It is imperative, if this is done, the same controls be implemented to protect the confidentiality of sensitive customer information. All key controls with regard to the protection of production data must be in place to protect non-production environments. A best practice involves concealing or removing sensitive data once it is used or using data generation tools that create dummy or test data, thus mitigating risk to production data. | Review the risk assessment to determine if it assesses controls over sensitive member data in non-production environments. |
| 239 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Evolving | Physical access to high-risk or confidential systems is restricted, logged, and unauthorized access is blocked. | The financial institution should identify all areas that are considered "high-risk" or are used to house and operate systems with confidential data. Typically, institutions keep their most critical technology assets in an access controlled data center(s) or secured room(s). Access to these areas must be highly restricted and all access must be logged. Automated logs are preferred, but smaller institutions may employ manual methods of recording and monitoring access. Typically, access is enabled or prohibited using access control cards, biometrics readers or keypad entry. Access reports can be reviewed and used in investigations, if needed. Surveillance cameras and automated entry logs are also used to digitally record all access to the secured areas. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and Identity and Access Management (IAM) and determine if there are controls describing how the financial Institutions physical security is managed (a listing of those areas would be ideal).<br><br>Review the IT General Controls Audit and determine if physical security controls exist that are tested regularly.<br><br>Determine who is responsible for the management of those physical controls to high-risk or confidential systems and discuss how staff are authorizing and monitoring access to those restricted areas. |
| 240 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Evolving | Controls are in place to prevent unauthorized access to cryptographic keys. | Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys used to secure sensitive data and hence, compromise of the data. While users may understand it is important to encrypt certain documents and electronic communications, they may not be familiar with minimum standards for protecting encryption keys, for their ATMs for example. Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.<br><br>Due to the important nature of keys some financial institutions may outsource the management of those keys. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, PCI-DSS and/or the IT Risk Assessment and discuss with management the controls in place to prevent unauthorized access to encryption keys.<br><br>Review the risk assessment to verify controls over cryptographic keys are tested for appropriate protections to prevent compromise and disclosure.<br><br>Discuss with management how they monitor and restrict access to cryptographic keys. |
| 241 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Intermediate | The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data. | Financial institutions can invest in tools to protect their confidential information and intellectual property by trying to prevent data leakage or data loss. They can adopt policies and implement technical controls to stop the loss and disclosure of sensitive information to outside attackers as well as inadvertent and malicious insiders. Software tools might include blocking or encrypting files and emails with sensitive member data. USBs drives might be disabled, along with CD Rom read, write and execute abilities. USBs if they exist should be credit union owned, inventoried, and encrypted. These can be registered as the only USBs that can be used. Reasonable exceptions to policy would be cameras for marketing and collections, and for legitimate business uses. | Review the risk assessment and determine if it discusses controls or tools to prevent the unauthorized access or exfiltration of data. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 242 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Intermediate | Controls are in place to prevent unauthorized escalation of user privileges. | Privilege escalation is an attack technique that attempts to gain unauthorized access to a network. Successful privilege escalation attacks grant hackers privileges normal users don't have. The attacker takes advantage of programming errors or design flaws that enable elevated access to the network, data, and applications. There are two types of privilege escalation: vertical and horizontal.<br><br>Vertical privilege escalation requires the attacker to grant himself higher privileges. Attackers will perform kernel-level operations that allow the attacker to run unauthorized code. The kernel is the central module of an operating system (OS) and performs functions such as memory, process, and disk management.<br><br>Horizontal privilege escalation requires the attacker to use the same level of privileges granted, but they assume the identity of another user with similar privileges.<br><br>Controls used to mitigate occurrence of privilege escalation include: application firewalls that prevent Uniform Resource Locator (URL) tampering, strong access management and coding controls. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Account Management and discuss with management the administrative or technical controls in place to prevent unauthorized escalation of privileges. |
| 243 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Intermediate | Access controls are in place for database administrators to prevent unauthorized downloading or transmission of confidential data. | Management should implement strong database access controls that help prevent unauthorized download or transmission of confidential data. Management should identify the criticality of the database content and set privileged and/or role-based user access. Typically, database administrator (DBA) privileges allow important actions such as database design, access management, update and configuration changes. The DBA will also work with network administrators to establish security controls pertaining to data management. Generally, the DBA should not have isolated or sole ability to download or transmit data except in authorized, controlled, and monitored sessions. Monitoring tools should include alerting or logging capabilities tied to data transmission, copy, or download. | Verify the controls over database monitoring are performed by an independent party such as the Information Security team or similar. Review the triggers, check for appropriateness. Also validate the group receiving alerts appropriately responds to them. |
| 244 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Intermediate | All physical and logical access is removed immediately upon notification of involuntary termination and within 24 hours of an employee's voluntary departure. | Access management policies and procedures should establish a process for terminating users. If a financial institution terminates an individual's employment, there should be measures in place that require that user's access to any asset or system be removed immediately. This recognizes that involuntary termination may lead to a hostile situation or lead to malicious activity by an individual. Voluntary terminations typically occur within 24 hours of an employee's departure. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Account Management, specifically the section over terminations and separations to determine if the financial Institution has a process to remove access (physical and logical) immediately upon termination.<br><br>Select a sample of terminations and determine if they were removed within 24 hours of an employees' departure. |
| 245 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Intermediate | Multifactor authentication and/or layered controls have been implemented to secure all third-party access to the institution's network and/or systems and applications. | Multifactor authentication (MFA) is a security control that requires more than one authenticating element to verify the user's identity (e.g., something known, something the user has, or something they are).<br><br>Layered control is a combination of authentication factors, but may be limited to one authentication form. For example, layered authentication may involve a user providing three known facts (e.g., challenge questions), but may not involve something the user has or is. MFA is a type of layered defense that is more difficult to compromise because the user will have a physical credential (card or token) and/or a biometric. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Account Management, and Third-Party Service Provider Management to determine if multifactor authentication is required for vendor accounts with access to the financial Institutions systems and/or applications.<br><br>Discuss with management how many external parties have access to the network and the method of authentication they use to access the network. |
| 246 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Intermediate | Multifactor authentication (e.g., tokens, digital certificates) techniques are used for employee access to high-risk systems as identified in the risk assessment(s). (*N/A if no high risk systems.) | Risk assessments help institutions identify high-risk assets and systems (e.g., wire transfer). Employee access to high risk systems should require use of Multifactor Authentication (MFA). MFA is a security control that requires more than one authenticating element to verify the user's identity which will feature something known, something the user has, or something they are. MFA is a type of layered defense that is more difficult to compromise because the user is required to rely on a physical credential (card, digital certificate, or token) and/or a biometric. | Determine if IT Risk assessment contains the identification of high risk systems.<br><br>Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Identify and Access Management (IAM) to determine if they contain the use of multifactor authentication for employees with access to the financial Institutions systems and/or applications identified as high risk. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 247 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Intermediate | Confidential data are encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones. | Data in transit is commonly delineated into two primary categories – data that is moving across public or "untrusted" networks such as the Internet, and data that is moving within the confines of private networks such as corporate Local Area Networks (LANs). A related concept is data in use, which refers to data that is being processed. One example would be a financial institution balance transaction update, which needs to occur in a secure tamper-proof environment. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security for encryption standards.<br><br>Review the classification policy in conjunction with the network topology diagram(s) to understand what is considered confidential, where it exists, and where it is moving back and forth among other vendors and staff.<br><br>Notate all areas where public connections (untrusted networks) and trusted zones (internal network) exist and verify data crossing those links is encrypted.<br><br>There may be a risk assessment associated with the need to encrypt data across trusted and untrusted zones. You may need to refer to it if the financial Institution is not encrypting data in transit across all connections. |
| 248 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Intermediate | Controls are in place to prevent unauthorized access to collaborative computing devices and applications (e.g., networked white boards, cameras, microphones, online applications such as instant messaging and document sharing). (* N/A if collaborative computing devices are not used.) | Collaborative systems enable connectivity among people and tools for more efficient and effective communication and information sharing. Sometimes these goals are contrary to security goals that foster confidentiality and data integrity assurance. Collaborative environments must be implemented to ensure strong user authentication and access controls based on need to know privileges. Connections that enable access must be formally authorized and systems should be monitored to detect unauthorized access to collaborative sessions. Failure to prevent unauthorized access to these devices can result in subsequent compromises of organizational information including, for example, eavesdropping on conversations. | Review the risk assessment to determine if collaborative devices are included and controls for securing these devices are defined.<br><br>Review any assessments of those controls listed for sufficiency and appropriateness. |
| 249 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Advanced | Encryption of select data at rest is determined by the institution's data classification and risk assessment. | "Data at rest" is generally resident data stored on mobile devices, desktops, servers, within application and log files, or databases or storage repositories. Management is responsible for identifying where data resides, to include data hosted by external service providers. They must decide if encryption is necessary to protect that data from unauthorized access or theft. Decisions to encrypt should be based on an IT risk assessment, data classification policies, or compliance requirements, such as that set by the Payments Card Industry (PCI). Financial institutions should consider encrypting highly confidential data at rest, such as customer information or proprietary information pertaining to systems or strategies. | Review the risk assessment and determine if it addresses the need to encrypt data confidential data at rest (for example, in database or on file servers).<br><br>Discuss with management if they have a data classification policy.<br><br>Discuss with management whether they encrypt select data at rest based on the data classification policy. |
| 250 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Advanced | Customer authentication for high-risk transactions includes methods to prevent malware and man-in-the-middle attacks (e.g., using visual transaction signing). | High-risk transactions involve access to customer information or the movement of funds to other parties. For example, a high-risk system is one that is remotely accessible and allows direct access to funds, fund transfer mechanisms, or sensitive customer data.<br><br>Authentication techniques should prevent advanced types of compromise such as Man in the Middle attacks or malware injection. Controls may involve multi-factor authentication, out-of-band authorization, and session encryption. The techniques employed should be commensurate with the risks associated with the products and services. Financial institutions should not rely solely on any single authentication control for authorizing high risk transactions, but rather institute a system of layered security. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Online and Mobile Banking and discuss with management their methodology for defining high-risk transactions.<br><br>Review the Electronic Banking Risk Assessment(s) to determine if there were any findings related to customer authentication. |
| 251 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Innovative | Adaptive access controls de-provision or isolate an employee, third-party, or customer credentials to minimize potential damage if malicious behavior is suspected. | Adaptive access controls involve actively changing access privileges for various users based on defined attributes, such as event, action or behavior. Privilege is escalated or revoked based on changing risk factors. The challenge involved with this type of access management is calibrating the attributes and risk factors so that privileges do not inadvertently block access when needed or grant excessive access when not required. Financial institutions should document these attributes and monitor access. | Discuss with management or have them demonstrate the tool(s) implemented for Identify and Access Management (IAM). |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 252 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Innovative | Unstructured confidential data are tracked and secured through an identity-aware, cross-platform storage system that protects against internal threats, monitors user access, and tracks changes. | Data can be entered in to applications or stored in databases in structured or unstructured formats. Structured data is entered in a defined or special format that organizes data for different purposes such as analysis, reporting, and storage. Unstructured data does not follow a specific format. Examples include data found in email messages, instant messages, or applications like Adobe PDF or Microsoft Word. Financial institutions should identify where confidential unstructured data originates, how it is stored and secured, and they should establish strong access controls to protect that data. | Discuss with management or have them demonstrate any tool(s) they have implemented for Data Loss Prevention.<br><br>Discuss with management their process for identifying personally identifiable information (PII) at rest. |
| 253 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Innovative | Tokenization is used to substitute unique values for confidential information (e.g., virtual credit card). | Tokenization is a process by which a primary value is replaced with a surrogate value called a token. De-tokenization is the reverse process of redeeming a token for its associated primary value. The security of an individual token relies predominantly on the infeasibility of determining the original primary value knowing only the surrogate value.<br><br>Tokenization technology could be used to substitute unique values in confidential information, most notably for credit card numbers. | Discuss with management if they are Europay, MasterCard, and Visa (EMV) chip compliant for their debit and credit card base.<br><br>Discuss with management if they have any additional plans to implement tokenization beyond debit and credit card products. |
| 254 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Innovative | The institution is leading efforts to create new technologies and processes for managing customer, employee, and third-party authentication and access. | Financial institutions may employ passwords, tokens, or biometrics to authenticate user identities, or in the case of multifactor authentication, some combination of one or more of the above. A financial institution's IT organization should be in control of centralized vendor access pathways that allow them to enforce access control policies and to record and monitor all third-party activity. Financial institutions often select two or three authentication solutions that can be implemented together to achieve acceptable levels of risk mitigation:<br>• Shared information—Secret information or images that are shared between the customer and the institution.<br>• Device identification—A profile of the connecting device that can be used to authenticate the user in future transactions.<br>• Geo-location—Establishing the geographic location from which the customer is connecting.<br>• Internet Protocol (IP) intelligence—Using the customer's unique IP address.<br>• Encrypted cookies—Special bits of data that the institution places on the customer's computer to assist in authenticating the customer.<br>• Out-of-band communication—Cell phone call or e-mail message providing verification.<br><br>Each of these processes alone adds strength to the authentication process. Combining several processes greatly increases the strength of the security and is an effective risk management strategy. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Identity and Access Management (IAM) to gain an understanding of how access controls are regulated among third parties.<br><br>Discuss with management if they are developing or working with a third party vendor to develop any new technologies and processes for managing customer, employee, and third-party authentication and access. |
| 255 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Innovative | Real-time risk mitigation is taken based on automated risk scoring of user credentials. | The financial institution has implemented a real-time risk management solution to address the rapidly changing threat landscape with up to the minute information about threats, vulnerabilities, and assets to provide comprehensive visibility of the entire IT infrastructure, while continuously assessing existing security controls. Using risk scoring, a financial institution can prioritize threats and implement mitigating measures. Rather than rely on alerts and notifications from event monitoring agents, the financial institution may use automated alerts and threat modeling to automatically disconnect an affected asset from the network to mitigate and defeat attack scenarios before they fully unfold. Risk scoring estimates the risk associated with an activity. When a risk score exceeds an established threshold, based on the severity of the occurrence, mitigation activities can be triggered. | Discuss with management or demonstrate their Security Information and Event Management (SIEM) tool. Ask them if this tool imports threat information from a well-known source, and validate the system is producing automated risk scoring. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 256 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Baseline | Controls are in place to restrict the use of removable media to authorized personnel. | Failure to control or manage the use of removable media can lead to material financial loss, the theft of information, the introduction of malware and the loss of reputation. Financial institution management should perform a risk assessment on the use of removable media and apply appropriate and proportionate security controls, in the context of their business and risk appetite. Risk mitigation approaches that financial institution management may implement to address these risks may include:<br>• Formal policies on the use of removable media that outline where removable media cannot be used.<br>• Active antivirus scanning on all systems where removable media can be used.<br>• Only allowing organizational deployment and use of removable media (i.e. corporate owned)<br>• Encrypting the information on removable media.<br>• Implementing a monitoring strategy to detect and react to the unauthorized use of removable media.<br>• Actively managing the use and disposal of removable media.<br>• Educating users and maintaining awareness of the risks of improper use of removable media. | Discuss with management and have them demonstrate how they address removable media.<br><br>Discuss with management or have them demonstrate any tool(s) they have implemented for data loss prevention.<br><br>Discuss with management and have them demonstrate how USB ports and CD/DVD Rom drives are restricted to authorized personnel. |
| 257 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Evolving | Tools automatically block attempted access from unpatched employee and third-party devices. | Defending mobile and remote machines against the latest known threats involves solutions that verify that the necessary fixes or patches are in place and that the machines are in compliance with corporate policies. For example, institutions may require that machines have up to date antivirus software.<br><br>Two types of tools are available to assess vulnerabilities on mobile and remote devices. Network-based assessment tools: these reside on VPN gateways and detect open ports, identify services running on these ports, and reveal possible vulnerabilities associated with these services. These solutions can screen mobile devices before they connect to the corporate network, and deny non-compliant machines access. Host-based vulnerability assessment tools: these reside on the mobile or remote machine and audit the machine for system-level vulnerabilities including incorrect file permissions, registry permissions, and software configuration errors. They also ensure that the system is compliant with predefined company security policies. | Review the Financial Institution's Policy, Standards and Guidelines specific to:<br>Patch Management and discuss with management their process for identifying and taking action on non-compliant machines attempting to access to the network.<br><br>Review the patch management report and determine if it contains a list of exceptions or unpatched devices. |
| 258 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Evolving | Tools automatically block attempted access by unregistered devices to internal networks. | Defending mobile and remote machines against the latest known threats involves solutions that verify that the necessary fixes or patches are in place and that the machines are in compliance with corporate policies. For example, institutions may require that machines have up to date antivirus software.<br><br>Two types of tools are available to assess vulnerabilities on mobile and remote devices. Network-based assessment tools: these reside on VPN gateways and detect open ports, identify services running on these ports, and reveal possible vulnerabilities associated with these services. These solutions can screen mobile devices before they connect to the corporate network, and deny non-compliant machines access. Host-based vulnerability assessment tools: these reside on the mobile or remote machine and audit the machine for system-level vulnerabilities including incorrect file permissions, registry permissions, and software configuration errors. They also ensure that the system is compliant with predefined company security policies. | Review the Financial Institution's Policy, Standards and Guidelines specific to:<br>Network Management, Asset Management and discuss with management how unregistered or unauthorized devices attempting to connect or connected to the network are detected and any predetermined actions taken on these devices once identified.<br><br>Ask management to demonstrate any tool(s) they using to prevent unregistered or unauthorized devices attempting to connect to the internal network. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 259 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Evolving | The institution has controls to prevent the unauthorized addition of new connections. | A connection may be any internal or external connection. For example: wireless, VPN, third-parties, network segments, or leased-lines. Controls to prevent such activity will be those used to gain access to the technologies such as VPN devices, routers, and wireless technologies. Controls to prevent such activity will be those used to prevent access to the technologies such as VPN devices, routers, and wireless technologies. Strong authentication and authorization controls are key. Multi-factor authentication is a stronger control in comparison to relying solely on an approach such as strong passwords with a requirement to change them every 45 days. Detection plays another role in ensuring controls used to prevent unauthorized activity are working as intended. | Review the Financial Institution's Policy, Standards and Guidelines specific to:<br>Network Management and discuss with management how they would detect a new connection to the network or what tools are they using to prevent someone from plugging into the network and connecting. |
| 260 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Evolving | Controls are in place to prevent unauthorized individuals from copying confidential data to removable media. | Removable media devices (USB, CD, and DVD) should be restricted for use, and monitored for inappropriate activity. For example, technology should be implemented to prevent users from attaching a USB drive to their portable or desktop system. The attempt should be logged and appropriate staff should be alerted to the activity. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Data Loss Prevention and ask management to demonstrate the data loss prevention tool and security controls that manage removable media.<br><br>Discuss with management or have them demonstrate the financial Institution's ability to restrict access to removable media devices to authorized personnel. |
| 261 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Evolving | Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices). | Commercial antivirus and antimalware application(s) are deployed to ALL end-point devices. The list of end-point devices should tie closely to the asset inventory. For example, many financial institutions maintain an Active Directory, as well as a patching tool, and conduct vulnerability assessments. A list of inventory can be obtained from all three to ensure ALL end-point devices are properly protected. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Antivirus and Anti- Malware Management and discuss with management the antivirus and anti-malware technology implemented at the financial Institution.<br><br>Review the formal reconciliation documentation to see if action is taken if devices are found to not be recorded under any of the three lists.<br><br>If formal documentation is not available, compare the antivirus, asset inventory and vulnerability scanner lists to determine if the devices on each list are substantially the same. If devices are missing, determine if management knows why. |
| 262 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Evolving | Mobile devices with access to the institution's data are centrally managed for antivirus and patch deployment. (*N/A if mobile devices are not used.) | Unmanaged mobile devices with access to confidential information can pose a significant risk. Therefore, any mobile device with such access should be receiving antivirus definitions and critical software patches from a centralized institution-managed system. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Mobile Device Management (MDM) and discuss with management the MDM software platform implemented at the financial Institution.<br><br>Discuss with management how anti-virus and patch management is deployed to mobile devices. |
| 263 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Evolving | The institution wipes data remotely on mobile devices when a device is missing or stolen. (*N/A if mobile devices are not used.) | Mobile Device Management solutions (MDM) allow a financial institution to remotely wipe mobile devices when reported lost or stolen. Each MDM solution should be setup to wipe the devices and this control should be periodically tested for effectiveness. | Discuss with management how the MDM solution ensures that data is wiped clean from a missing or stolen device. |
| 264 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Intermediate | Data loss prevention controls or devices are implemented for inbound and outbound communications (e.g., e-mail, FTP, Telnet, prevention of large file transfers). | A DLP solution has been implemented that encompass both inbound and outbound communications, specifically ensuring they address more common means of data transfer such as e-mail, FTP, Telnet, or TFTP. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Data Loss Prevention (DLP) and discuss with management how the DLP solution prevents or monitors inbound and outbound personally identifiable information (PII) from leaving or moving in the network, respectively. Discuss with management how the DLP solution monitors large file transfers.<br><br>Discuss with management that the DLP solution for email is monitoring all parts of the email, including the subject. Of particular importance is monitoring of the body of the email and the contents of attachments. |
| 265 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Intermediate | Mobile device management includes integrity scanning (e.g., jailbreak/rooted detection). (*N/A if mobile devices are not used.) | An MDM solution allows a financial institution to monitor and manage mobile devices. The MDM solution should be able to detect a jailbroken or rooted device and prevent the device from accessing information and systems of the financial institution. When detected, an alert should be sent to the proper individuals and action taken (this may be an incident). | Discuss with management how the MDM solution identifies jailbroken or rooted devices and what actions are taken if a mobile device of this nature is identified. |
| 266 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Intermediate | Mobile devices connecting to the corporate network for storing and accessing company information allow for remote software version/patch validation. (*N/A if mobile devices are not used.) | An MDM solution allows a financial institution to monitor and manage mobile devices. Some devices allow the use of remote access software such as Citrix, RDP, or LogMeIn. These types of applications should be continuously patched for vulnerabilities and this type of access should be tightly monitored. | Review MDM reports and discuss with management how the MDM patches mobile devices.<br>Discuss with management how the MDM validates the patch status of the mobile device. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 267 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Advanced | Employees' and third parties' devices (including mobile) without the latest security patches are quarantined and patched before the device is granted access to the network. | Endpoint solutions in conjunction with network access controls (NAC) have the ability to force devices to comply with a set of policies. Features within these policies can quarantine a device that does not comply with a patched state. If the system or device is not in compliance with the patching security the device is not permitted access to the network. When this occurs, an alert should be generated to the proper individuals and action should be taken. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Network Management and discuss with management what network access controls (NAC) solutions the financial Institution has implemented, if any.<br><br>Discuss with management what tools are in place to quarantine a device that does not comply with the managed patch level and determine if the tools continue the quarantine until patch status is brought to a level of compliance. |
| 268 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Advanced | Confidential data and applications on mobile devices are only accessible via a secure, isolated sandbox or a secure container. | Sandboxing is a computer security term referring to when a program is set aside from other programs in a separate environment so that if errors or security issues occur, those issues will not spread to other areas on the computer. Programs are enabled in their own sequestered area, where they can be worked on without posing any threat to other programs.<br><br>Mobile devices are deployed using technology that will store all confidential data and enterprise applications in a secure container and only allow confidential materials to be viewed and accessed in a sandboxed environment. | Discuss with management if they have implemented a secure container allowing the secure downloading of email and the secure reading of documents via applications within the container, or if the MDM just used to manage the device itself without a secure container. |
| 269 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Innovative | A centralized end-point management tool provides fully integrated patch, configuration, and vulnerability management, while also being able to detect malware upon arrival to prevent an exploit. | The financial institution has deployed a cutting-edge, state-of-the-art management tool which brings together many of the single-application solutions used in the prevention of exploits and vulnerabilities such as patch management, configuration management, malware/antivirus detection, and vulnerability management into one centralized tool. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Network Management, Vulnerability & Patch Management and discuss with management if they have implemented a centralized end-point management tool or process that provides for a fully integrated patch, configuration, and vulnerability management solution, while also being able to detect malware upon arrival to prevent an exploit. |
| 270 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Baseline | Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards. | The system development life cycle is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. There are many different system development life cycle (SDLC) models and methodologies, but each generally consists of a series of defined steps or phases.<br><br>Unsafe coding practices can result in costly vulnerabilities in application software that leads to theft of sensitive data. Coding standards encourage programmers to follow a uniform set of rules and guidelines determined by the requirements of the project and organization, rather than by the programmer's familiarity or preference. Developers and software designers can apply these coding standards during software development to create secure systems.<br><br>For applications to be designed and implemented with proper security, secure coding practices and a focus on security risks should be integrated into day-to-day operations and the development processes. Application developers should adhere to secure coding requirements set by the financial institution regardless of the device used for programming. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Secure Application Development, System Development Lifecycle (SDLC) and discuss with management what software or processes they use to adhere to secure coding practices when developing software. |
| 271 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Baseline | The security controls of internally developed software are periodically reviewed and tested. (*N/A if there is no software development.) | Financial institutions developing software applications generally have formally approved secure coding guidelines for the technology (Java, .NET, PHP, etc.) they use. As threats and vulnerabilities change, the coding guidelines should be current, and internally developed software should be continuously reviewed and tested. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Secure Application Development, System Development Lifecycle (SDLC) and discuss with management what software or processes they use to adhere to secure program development and secure coding and practices when developing software.<br><br>Sample the IT risk assessment or documentation on recent coding reviews and testing for previously developed code.to determine if the internally developed software is continuously reviewed and tested. |
| 272 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Baseline | The security controls in internally developed software code are independently reviewed before migrating the code to production. (*N/A if there is no software development.) | Newly created code/software/applications may have security weaknesses. Therefore, an independent internal, or external third-party, code review should be conducted before applications are released for business use. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Secure Application Development, System Development Lifecycle (SDLC) and discuss with management the process for software code reviews.<br><br>Define the individuals involved in the process to move the software into production.<br><br>Review the IT risk assessment or penetration test results to determine if the security controls of internally developed software are assessed before migrating to production. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 273 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Baseline | Intellectual property and production code are held in escrow. (*N/A if there is no production code to hold in escrow.) | Holding the intellectual property and production code in escrow can help ensure mission critical software applications are available in the event that an adverse event impacts the third-party developer. The financial institution enters into a software escrow agreement with the developer. The agreement requires the code to be stored at an independent third-party repository for safe keeping. | Discuss with management if the production code of the core data processing system is escrowed.<br><br>Review a sample of contracts for code development to determine that escrowing is covered in relevant contracts. |
| 274 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Evolving | Security testing occurs at all post-design phases of the SDLC for all applications, including mobile applications. (*N/A if there is no software development.) | Financial institutions should determine whether application security should be considered at the pre or post development phase or throughout the SDLC process of application development. Application developers and architects should know the importance of security to their applications and how security as a process should be incorporated during their development lifecycle.<br><br>For any SDLC model that is used, information security should be integrated into the SDLC to ensure appropriate protection for the information that the system will transmit, process, and store. | Discuss with management the specific phases where security testing is performed in their system development life cycle methodology. |
| 275 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Intermediate | Processes are in place to mitigate vulnerabilities identified as part of the secure development of systems and applications. | Applying the risk management process to system development enables institutions to balance requirements for the protection of their information and assets with the cost of security controls and mitigation strategies throughout the SDLC. Therefore, as vulnerabilities are uncovered during the process, those identified are risk ranked and mitigated accordingly. Vulnerabilities should be identified, risks should be identified and ranked, and each should be mitigated or associated risks accepted. | Discuss with management how they identify and mitigate identified vulnerabilities identified during phases of the SDLC.<br><br>Review documented risk assessments, reviews and any formal acceptance of risks. |
| 276 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Intermediate | The security of applications, including Web-based applications connected to the Internet, is tested against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes. | Prior to implementing major revisions to internet facing applications, penetration testing should be completed to ensure known and unknown vulnerabilities are identified before they move to production environments. | Discuss with management how applications, including web-based applications connected to the Internet, are tested against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes.<br><br>Review testing documentation including management's responses to determine if concerns were found and what action (if any) was taken to remediate those concerns. |
| 277 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Intermediate | Software code executables and scripts are digitally signed to confirm the software author and guarantee that the code has not been altered or corrupted. | Code signing is the process of digitally signing executables and scripts to confirm the identity of the software author and guarantee that the code has not been altered or corrupted since it was signed. Publicly trusted certification authorities (CAs) confirm signers' identities and bind their public key to a code signing certificate. | Discuss with management the process for how the financial Institution digitally signs software executables and scripts to protect the integrity of the code. |
| 278 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Intermediate | A risk-based, independent information assurance function evaluates the security of internal applications. | Internally developed applications should be tested throughout the software development life-cycle to identify security vulnerabilities. Testing of these applications should be performed by an independent function to provide an unbiased evaluation. | Discuss with management how internally developed applications are evaluated for security risks. |
| 279 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Advanced | Vulnerabilities identified through a static code analysis are remediated before implementing newly developed or changed applications into production. | Static code analysis, also commonly called "white-box" testing, looks at applications in a non-runtime environment. This method of security testing has distinct advantages in that it can evaluate both web and non-web applications and through advanced modeling, can detect flaws in the software's inputs and outputs that cannot be seen through dynamic web scanning alone. | Discuss with management if they use "white-box" testing for software prior to the release into a production environment. |
| 280 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Advanced | All interdependencies between applications and services have been identified. | The identification of dependencies has become increasingly important in today's networked environments because applications and services rely on a variety of supporting services. Dependencies and interdependencies among applications and services should be included when conducting code reviews, security assessments, and testing. | Discuss with management or review the requested artifacts to determine if the financial Institution has documented the interdependencies between applications and services. |
| 281 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Advanced | The security controls in internally developed software code are independently reviewed before migrating the code to production. | Manual or automated code review is an examination of computer source code. It is intended to find and fix mistakes introduced into an application in the development phase, improving both the overall quality of software and the developers' skills. Code review procedures are done in various forms, such as pair programming, informal walk through and formal inspections. | Review independent code review results to determine if the financial Institution identifies findings in the independent review and performs remediation efforts based on the review. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 282 | 3: Cybersecurity Controls | 1: Preventative Controls | 4: Secure Coding | Innovative | Software code is actively scanned by automated tools in the development environment so that security weaknesses can be resolved immediately during the design phase. | Code review is a phase in the software development process in which the authors of code, peer reviewers, and perhaps quality assurance (QA) testers get together to review code. Finding and correcting errors at this stage is relatively inexpensive and tends to reduce the more expensive process of handling, locating, and fixing bugs during later stages of development code | Discuss with management what automated tools are used to scan the code to help identify weaknesses. |
| 283 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Baseline | Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network. | A vulnerability scan identifies a financial institution's known vulnerabilities. A penetration test attempts to exploit potential vulnerabilities.<br><br>Due to the risk level of external facing systems and internal networks management should validate controls via penetration testing and vulnerability scans, conducted by a qualified independent contractor or office (e.g., internal audit). | Review the risk assessment to determine the testing cycle for external and internal penetration and vulnerability testing.<br><br>Review the two most recent test dates to determine compliance with the established time frame in the risk assessment.<br><br>Review the testing results as well as management's responses. Determine if concerns have been remediated or risk accepted. |
| 284 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Baseline | Antivirus and anti-malware tools are used to detect attacks. | Malware has become more and more sophisticated in recent years, evolving from annoyance attacks or proof-of-concept attacks to rootkits and key loggers designed to steal critical business data. To combat these types of threats, financial institutions should use tools to detect viruses and malware on all systems (laptops, tablets, servers, mobile, etc.).<br><br>Typical controls to protect against malicious code use technology, policies and procedures, and training, all applied in a layered manner from perimeters inward to hosts and data. The controls are of the preventative and detective/corrective varieties. | Review the reports available or observe the anti-virus console to determine a solution is active and in place on systems as appropriate.<br><br>Review the reports for the last 30, 60, or 90 day period to identify if the devices found to be infected with malware removed or quarantined. |
| 285 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Baseline | Firewall rules are audited or verified at least quarterly. | Establishing an effective firewall audit program customarily involves defining policies, collecting firewall data, and evaluating the firewall data for policy violations and other issues. Firewall policies addressing access control between the financial institution's network and other networks should be audited and verified at least quarterly. This can be an internal review process by qualified staff. There should be an independent review conducted periodically. At a minimum the review should ensure that all firewall rules are adequately documented as to their business purpose. Further validation includes determining whether the rules remain necessary and proper or have become obsolete. | Discuss with management if, and how the firewall rules are reviewed or verified.<br><br>Review audits to determine if there were any concerns noted.<br><br>Review management's responses and documentation of any remediation taken or acceptance of risk. |
| 286 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Baseline | E-mail protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links). | Email is inherently insecure. The three major protocols used for the vast majority of electronic mail (POP, IMAP and SMTP) are all clear text protocols that were designed without much thought to security. These protocols in their basic form offer absolutely no expectation of privacy. A financial institution's email can be subject to interception, alteration and counterfeiting by anyone on the virtual path between the sender and the recipient. Enforcement of malicious code filtering is performed by anti-virus, anti-spyware, and anti-spam filtering, and the blocking of downloading of executable files. | Discuss with management the methods and solutions in place to protect email from common cyber threats. |
| 287 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Evolving | Independent penetration testing of network boundary and critical Web-facing applications is performed routinely to identify security control gaps. | Independent tests include penetration tests, vulnerability assessments and audits. Independence provides credibility to the test results. A vulnerability assessment simply identifies and reports noted vulnerabilities, whereas a penetration test attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing should be performed more frequently than annually. | Review the engagement letter to determine whether the scope of testing included publically-facing applications.<br><br>Review the final reports to determine if concerns were found, what management's responses were, and what remediation was taken (or if risks were accepted). |
| 288 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Evolving | Independent penetration testing is performed on Internet-facing applications or systems before they are launched or undergo significant change. | Penetration testing should be performed on internet-facing applications and dependent systems prior to deployment into a production environment. Institutions which develop software should have staging systems and a staging environment. This is usually where this type of testing is performed. | Review the Financial Institution's Policy, Standards and Guidelines specific to: System Development Life Cycle (SDLC) to verify the financial Institution has processes for testing applications and systems prior to deployment into production.<br><br>Review independent scans and testing for internally developed programs to validate that the financial Institution's software development process follows secure development practices and is periodically tested. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 289 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Evolving | Antivirus and anti-malware tools are updated automatically. | Anti-virus and anti-malware tools used today automatically update their virus definitions. When updates are automatically scheduled, ALL devices should receive those updated definitions and application updates. Therefore, it is necessary for each institution to provide sufficient evidence to show their inventory of systems are in fact receiving them in a timely manner, especially those which operate outside the internal network, such as mobile devices, portable laptops, and tablets. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Antivirus and Anti- Malware Management and determine if it addresses the process for updating antivirus and anti-malware signatures and tools.<br><br>Review the configuration settings for antivirus and anti-malware tools and determine if the tools are updated automatically. |
| 290 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Evolving | Firewall rules are updated routinely. | Firewall rules should be reviewed on a routine basis for necessity (whether they are required), obsolescence (are they frequently used), and function (their function is documented). Additionally, firewall rules should be reviewed by an independent party to ensure the firewall is properly managed, maintained, and kept current. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Network Management and to determine the timeframe and appropriate process and personnel (internal or third-party) allowed to initiate and implement changes to perimeter devices, specifically firewalls.<br><br>Discuss with management the process for updating firewall rules.<br><br>Review audits or reviews related to firewall rules to verify firewall rules were reviewed and updated according to the policy/process as discussed with management. |
| 291 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Evolving | Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices. | Vulnerability management is a key control to ensure known vulnerabilities in systems, applications, and devices are uncovered before they are placed into production. Vulnerability scanning is normally conducted on a routine basis. However, as this control objective clarifies, it is imperative that the vulnerability management process includes scanning not just of existing components on the network today, but also prior to deployment into a production environment, including redeployment. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Change Management to determine requirements for scanning and analysis of new or existing devices prior to deployment or redeployment.<br><br>Review the management response or department's remediation plan/report (including change management records) to determine the corrective actions were taken based on findings from scanning/testing. |
| 292 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Evolving | Processes are in place to monitor potential insider activity that could lead to data theft or destruction. | Insiders pose a significant threat to a financial institution. An insider threat could be an employee, a former employee, contractor, or business partner who has or had authorized access to the financial institution's network, systems, or information. Processes and supporting technologies should be in place to monitor insider activity that could lead to theft or destruction of data. Examples of such technologies include: encryption, access monitoring, security information and event management (SIEM), data loss prevention (DLP), data redaction, training, and two-factor authentication. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Data Loss Prevention, Insider Threat to determine if the financial Institution has an established processes for detecting and mitigating insider theft of data.<br><br>Discuss with management any automated tools or processes in place to detect, prevent or monitor for insider activity that could lead to data theft or destruction. |
| 293 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Intermediate | Audit or risk management resources review the penetration testing scope and results to help determine the need for rotating companies based on the quality of the work. | An independent review and validation of vendors conducting penetration testing ensures the relationship between IT and the vendor are not compromised resulting in sub-standard reviews and skewed results. Therefore, the results from penetration testing vendors should be periodically reviewed for both quality and objectivity. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management to determine the financial Institution's process for ensuring due diligence in selecting vendors.<br><br>Discuss with management their process for verifying the quality and independence of third parties in evaluating their suitability to perform penetration testing. |
| 294 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Intermediate | E-mails and attachments are automatically scanned to detect malware and are blocked when malware is present. | The majority of e-mail virus and malware scanning solutions scan e-mails before they reach their intended destination. E-mails should be scanned both outgoing and incoming. Once detected, any e-mails with a virus or malware should be blocked, and an alert should be sent to the appropriate personnel, who typically review, document, and respond. | Review the report from the security solution used to prevent malware or viruses from entering the network via email and determine the solution is detecting, preventing, and logging incoming or outgoing emails with malware or viruses. |
| 295 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Advanced | Weekly vulnerability scanning is rotated among environments to scan all environments throughout the year. | This entails running automated vulnerability scanning tools against all systems and applications over the course of a year to ensure all are scanned at least once. Scaling down the scan program into more targeted [specific internet protocol (IP) address range] scans on a weekly or more frequent basis allows the testing to be conducted at different times. This allows scheduling of scans to include systems or applications that may only be operational for specific functions at certain times of a month or day, and might not have coincided with the scanning cycle. The objective is to ensure all systems are scanned for vulnerabilities at least annually with a prioritized lists of the most critical vulnerabilities delivered to each responsible system administrator along with the risk scores that compare the effectiveness of system administrators and departments in reducing risk. | Review the network topology diagram(s), asset inventory, and vulnerability scanning processes; or discuss with management, to verify how often and for what environments vulnerability scanning is performed. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 296 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Advanced | Penetration tests include cyber attack simulations and/or real-world tactics and techniques such as red team testing to detect control gaps in employee behavior, security defenses, policies, and resources. | Penetration testing tactics may include more rigorous techniques such as red/blue team simulations. Red Team Tests simulate real-world attacks against an organization, challenging its defenses against electronic, physical, and social exploits. The Blue team defends against the red team. These engagements are designed to identify gaps in security practices and controls that are not readily apparent by conducting standard technical tests. Red Team Testing focuses on identifying potential damage that a determined, directed attacker could accomplish, and should serve as a tool to train defenders on identifying real indicators of active attacks. | Review the scope of work detailed in the contract and the final penetration test report to verify the financial Institution documented the scope of testing to be performed (to include red team testing) and review the test results to determine if all activities within the contract were performed within the scope of testing. |
| 297 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Advanced | Automated tool(s) proactively identifies high-risk behavior signaling an employee who may pose an insider threat. | The financial institution has established a profile of high-risk behavior and implemented tools to proactively monitor and detect activity that may be considered a threat. | Review the security reports from automated systems monitoring and discuss with management the processes they have implemented to follow for detecting high-risk behavior (anomalous login times, attempts to elevate user privileges). |
| 298 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Innovative | User tasks and content (e.g., opening an e-mail attachment) are automatically isolated in a secure container or virtual environment so that malware can be analyzed but cannot access vital data, end-point operating systems, or applications on the institution's network. | Sandboxing is a computer security term referring to when a program is set aside from other programs in a separate environment so that if errors or security issues occur, those issues will not spread to other areas on the computer. Programs are enabled in their own sequestered area, where they can be worked on without posing any threat to other programs.<br><br>Sandboxes can look like a regular operating environment, or they can be much more basic. Virtual machines are often used for what are referred to as runtime sandboxes. To achieve this control objective, users modifying documents, downloading documents, and opening documents are doing so in a sandboxed environment. | Discuss with management how they implement a secure container environment, monitor its operations, and change its functions to maintain security.<br><br>Reviewing available reports from the container solution will note the frequency and effectiveness of the system's use. |
| 299 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Innovative | Vulnerability scanning is performed on a weekly basis across all environments. | This entails running automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and delivering prioritized lists of the most critical vulnerabilities to each responsible system administrator along with the risk scores that compare the effectiveness of system administrators and departments in reducing risk. SCAP-validated vulnerability scanners look for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries - CVE Score) and configuration-based vulnerabilities (Common Configuration Enumeration - CCE). There may be multiple environments in a financial institution, such as production, testing, staging, and development. | Review the network topology diagram(s), asset inventory, and vulnerability scanning processes; or discuss with management, to verify how often and for what environments vulnerability scanning is performed. |
| 300 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Baseline | The institution is able to detect anomalous activities through monitoring across the environment. | Anomalous activity monitoring is critically important for consumer electronic banking channels to manage fraud risk. For networks, intrusion detection and/or prevention systems monitor internal network and system communications and report anomalous activity. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Network Monitoring and reports and alerts to detect anomalous activity to verify the financial Institution and their third parties have processes in place to monitor and detect anomalous behavior.<br><br>Review the network topology diagram(s) to determine intrusion detection system (IDS) and intrusion prevention system (IPS) placement on the network. |
| 301 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Baseline | Customer transactions generating anomalous activity alerts are monitored and reviewed. | Financial institutions should have safe and efficient systems for transferring funds internally, among themselves, and with their customers for large-dollar payments relating to financial market transactions and settling wholesale and consumer payments. This may include:<br>• Establishing dual controls and separation of duties for funds transfer systems;<br>• Monitoring and logging access to funds transfer systems;<br>• Maintaining an audit trail of all sequential transactions; and<br>• Providing management activity and quality control reports which disclose unusual or unauthorized activities and access attempts. | Review the process used by management/staff to identify and review alerts generated by systems (i.e. core system or online banking).<br><br>Discuss with management the financial Institution's process for reviewing alerts once anomalous activity is identified. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 302 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Baseline | Logs of physical and/or logical access are reviewed following events. | The financial institution maintains sufficient logs of physical and logical access to review an event.<br><br>Events may include:<br><br>• Failed login attempts<br>• Administrative or root access<br>• Remote access<br>• Database access<br><br>The correlation of physical audit information and audit logs from information systems may assist financial institutions in identifying examples of suspicious behavior or supporting evidence of such behavior. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Identity and Access Management (IAM), Network Monitoring to determine if the financial Institution has established a process for the review of user access following an event.<br><br>Review most recent incident reports to determine if access logs were included in the review. |
| 303 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Baseline | Access to critical systems by third parties is monitored for unauthorized or unusual activity. | Appropriate access controls and monitoring should be in place between service provider's systems and the financial institution. Institutions generally have procedures in place detailing specific activities that are authorized by third-party service providers and systems which monitor and alert on unauthorized activity. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Remote Access to determine how the financial Institution controls and monitors access to critical systems by third parties.<br><br>Use the business impact analysis to obtain the list of critical services and systems. |
| 304 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Baseline | Elevated privileges are monitored. | Financial institutions need to be vigilant about what actions privileged users are taking, and can use a variety of logging and monitoring techniques to identify and prevent privileged insider abuse. | Review a list of elevated privileges and determine the assigned user(s).<br><br>Review the list of employees with elevated privileges and compare to their job function to determine if the assigned privileges are required for their role.<br><br>Review the list of recent access level changes with department manager or HR to determine validity of the change. |
| 305 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Evolving | Systems are in place to detect anomalous behavior automatically during customer, employee, and third-party authentication. | Anomalies in authentication behavior can indicate changes in systems or network usage. These changes may be due to new applications or new servers, or they may be due to attackers and compromised systems. A log correlation engine normalizes logs that indicate successful authentication attempts to items such as the 'login' event type. The 'login-failure' event type is used to classify failures to authenticate. These types of alerts and log correlation engines help to identify potentially suspicious authentication attempts | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Incident Response, Online Banking and Mobile Banking to determine if and how the financial Institution is controlling and monitoring access for anomalous behavior. |
| 306 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Evolving | Security logs are reviewed regularly. | Logs from key systems, applications and devices have been identified and are reviewed on a frequent basis such as daily or weekly. Logs can be reviewed individually or from a system which collects and aggregates them. By definition, security logs can be subjective in nature. A financial institution produces many logs from many systems and applications. The key is identifying which ones contain authorization, authentication, systems or data changes, network activity, resource access, malware activity, and failures or critical errors. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security to determine the frequency of security log reviews.<br><br>Review the date of the most recent log review report to determine if it was reviewed in accordance with policy. |
| 307 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Evolving | Logs provide traceability for all system access by individual users. | A log is only as good as the information it contains. Therefore, each log file should contain useful information. If the logs do not track information and resources users are accessing, they do not fulfill this control objective. | Review a sample of logs to determine if the content provides adequate traceability of users. |
| 308 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Evolving | Thresholds have been established to determine activity within logs that would warrant management response. | Once security logs with useful content have been identified, thresholds should be established to provide alerts and notifications to the proper personnel when those thresholds are exceeded. An exception report is an example of management setting thresholds and generating a report when those thresholds are exceeded. Security logs should be built with the same frame of reference. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security to determine if thresholds and triggers have been established for escalating log reviews to management.<br><br>Review security log reports to verify that events exceeding set thresholds are recorded. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 309 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Intermediate | Online customer transactions are actively monitored for anomalous behavior. | Behavioral Monitoring services designed for online banking and institutions track the behavior of individual users. When these users login to access services, their current behavior is analyzed against their typical behavior based on past logins and activity. This is important in recognizing account takeover, as a compromised account may begin displaying behavior that is very different than the typical behavior of the true account holder. When Behavioral Monitoring services can analyze and compare behavior on the individual user level, as opposed to comparing one user's behavior to what is considered normal site behavior based on the entire user base, it is better able to detect account takeovers and prevent or contain losses. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Online and Mobile Banking to determine if the financial Institution has processes and tools in place to monitor transactions for anomalous behavior.<br><br>Review authentication solution documentation, if available, and discuss with management how these transactions are monitored for anomalous behavior. |
| 310 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Intermediate | Tools to detect unauthorized data mining are used. | Data mining is generally part of a larger business intelligence or knowledge management initiative. The purpose of data mining is to identify patterns to make predictions from information contained in databases. An IDS may be configured to identify inappropriate and/or unauthorized data mining activity. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and discuss with appropriate staff the software application solutions used to detect unauthorized data mining activity. |
| 311 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Intermediate | Tools actively monitor security logs for anomalous behavior and alert within established parameters. | A log correlation system or Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization's IT security. The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations and being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary. A SIEM system collects logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network devices. | Discuss with management the process for monitoring security logs for anomalous behavior and alerting personnel.<br><br>Demonstrate or describe automated tools in place for monitoring security logs. |
| 312 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Intermediate | Audit logs are backed up to a centralized log server or media that is difficult to alter. | Relevant logs should be copied to a remote, secure server to ensure they cannot be tampered with. Additionally, file hashes should be used to identify any attempt to tamper with the logs. | Review the information security specific to audit logs or backups to determine how the financial Institution backs up audit logs from critical systems.<br><br>Discuss with management/staff the frequency of audit log backups and the security implemented to prevent the logs from being altered. |
| 313 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Intermediate | Thresholds for security logging are evaluated periodically. | As thresholds are originally created and alerts generated, it's equally as important to continuously review those thresholds for changes that may have occurred in the systems, the industry, the applications, or their usage. | Review the information security policy and discuss with management/staff how log thresholds are established and how often the thresholds are updated. |
| 314 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Intermediate | Anomalous activity and other network and system alerts are correlated across business units to detect and prevent multifaceted attacks (e.g., simultaneous account takeover and DDoS attack). | Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization's IT security. The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations and being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary. A SIEM system collects logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment -- and even specialized security equipment like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. To allow the system to identify anomalous events, it's important that the SIEM administrator first creates a profile of the system under normal event conditions. SIEM systems are typically expensive to deploy and complex to operate and manage. | Determine if the financial Institution is using a SIEM or equivalent solution to correlate system alerts.<br><br>Discuss with management/staff how the solution is integrated with the incidence response plan and how it is monitored. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 315 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Advanced | An automated tool triggers system and/or fraud alerts when customer logins occur within a short period of time but from physically distant IP locations. | Adaptive authentication is a matrix of variables whose combination results in a risk profile otherwise known as a digital fingerprint. A digital fingerprint can look at a number of characteristics including IP address, geo-location, PC configuration, browser, time of day, and other factors comparing the current login to an existing customer baseline information. Any variance from the baseline may require additional authentication requirements before certain functions can be performed. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Online and Mobile Banking and discuss with management the process for monitoring and alerting personnel when anomalous behavior is detected.<br><br>Discuss with management or have them demonstrate automated tools in place for monitoring for anomalous behavior and any actions taken if activity is detected. |
| 316 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Advanced | External transfers from customer accounts generate alerts and require review and authorization if anomalous behavior is detected. | Risk-based authentication, sometimes called adaptive authentication, can most easily be described as a matrix of variables whose combination results in a risk profile. Based on that risk profile, additional authentication requirements may be added before certain functions can be performed. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Online and Mobile Banking, Payments to assess the controls used to review and authorize transfers on accounts which trigger red flag alerts (address changes 90 days, IP address, recent account lockouts). |
| 317 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Advanced | A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities. | Identifying insider threats requires visibility into user activity and the detection of anomalies in user behavior. The system compares normal usage patterns in interactions with the financial institution's resources to identify anomalies indicative of a potential insider threat. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Employee Monitoring, Insider Threat and discuss with management the processes and/or tool(s) in place to monitor and detect employee anomalous behavior.<br><br>Discuss with management the alerts or actions taken if anomalous behavior is detected. |
| 318 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Advanced | An automated tool(s) is in place to detect and prevent data mining by insider threats. | Data mining is normally part of a larger business intelligence or knowledge management initiative. The purpose of data mining is to identify patterns to make predictions from information contained in databases. A data mining intrusion detection systems (IDS) may be used to identify inappropriate or unauthorized behavior. According to the United States Computer Emergency Readiness Team (US-CERT), a malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. Unique patterns of insider threat behavior include: intellectual property (IP) theft, IT sabotage, fraud, espionage, and accidental insider incidents. In addition, insider threats can also be unintentional (non-malicious). | Review the Financial Institution's Policy, Standards and Guidelines specific to: Employee Monitoring, Insider Threat and discuss with appropriate management/staff software application solutions used to detect data mining.<br><br>Discuss with management or have them demonstrate the tool to determine if the solution is monitoring internal network traffic and employee activities. |
| 319 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Advanced | Tags on fictitious confidential data or files are used to provide advanced alerts of potential malicious activity when the data is accessed. | Organizations may place fictitious data (false data or SSN or account info) into files or shares as a way of tracking access and data flow, similar to the use of bait money in a teller drawer. Tags are a more liberal way to add metadata that is usually unstructured. Typically, the user can enter any tags that they think will relate to the document's contents or other attributes. This can provide advance notice of a systems breach before authentic sensitive data is compromised. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Employee Monitoring, Insider Threat and discuss with management how they are using fictitious data and data tags to monitor for unauthorized access.<br><br>Discuss with management the automated tool(s) implemented to monitor for unauthorized access to the staged data. |
| 320 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Innovative | The institution has a mechanism for real-time automated risk scoring of threats. | A mechanism for real-time automated risk scoring of threats:<br>• Provides services to implement sensors and dashboards;<br>• Delivers near-real time results;<br>• Prioritizes the worst problems within minutes, versus quarterly or annually;<br>• Enables defenders to identify and mitigate flaws at network speed; and<br>• Lowers operational risk and exploitation of IT systems and networks. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Risk Management and any automated solutions utilized and managed at the financial Institution for real-time automated risk scoring of threats.<br><br>Discuss with management what data is being used to inform the scoring of threats at the financial Institution. |
| 321 | 3: Cybersecurity Controls | 2: Detective Controls | 2: Anomalous Activity Detection | Innovative | The institution is developing new technologies that will detect potential insider threats and block activity in real time. | Technologies to detect potential insider threats can include tools that perform activities such as: database activity monitoring, whitelisting, network flow analysis, security information and event management (SIEM) and data loss prevention (DLP). | Review the Financial Institution's Policy, Standards and Guidelines specific to: Data Loss Prevention (DLP), Employee Monitoring, and Insider Threat to assess whether the institution is capable of detecting and blocking insider threats in real time. |
| 322 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Baseline | A normal network activity baseline is established. | Financial institutions should perform an analysis of their network traffic and then develop a normal activity baseline. A baseline is a process for studying the network at regular intervals to ensure that the network is working as designed. It is more than a single report detailing the performance or health of the network at a certain point in time. | Review the IT strategy and Information Security Policy to determine the frequency for establishing and monitoring the baseline.<br><br>Discuss with management the methodology or tool(s) used to establish a baseline of normal activity for the network. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 323 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Baseline | Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks. | Financial institutions should have system event and antivirus systems configured to alert management and/or appropriate security personnel when an event is detected.<br><br>Host intrusion detection systems (HIDS) include anti-virus and anti-spyware programs. Host-based intrusion detection systems are recommended by NIST for all mission-critical systems, even those that should not allow external access. | Review the security tools used and Incident response plan to assess how management is alerted to incidents. |
| 324 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Baseline | Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. | The financial institution should have a comprehensive system for monitoring access to critical and mission critical systems, devices, components, and software for unauthorized access. Typically, a security information and event management (SIEM) or log aggregation solution will be used to collect logs from multiple devices and software, and send alerts when inappropriate behavior is detected. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and Incident Response to identify the processes in place for monitoring unauthorized access to systems, or applications.<br><br>Review the inventory of security tools and discuss with management if the financial Institution uses security tools to monitor for unauthorized users, devices, connections, and software. |
| 325 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Baseline | Responsibilities for monitoring and reporting suspicious systems activity have been assigned. | The most effective way to detect and prevent network compromise and data breaches is through early recognition and investigation of potentially suspicious network activity. If a financial institution cannot detect activity that is out of the ordinary, then unexpected usage, unauthorized changes, and malicious attacks can go unnoticed. This may lead to network resource exhaustion, network compromise, and data breaches. Therefore, appropriate staff should be responsible for monitoring and reporting suspicious systems activity.<br><br>The responsibility and authority of security personnel and system administrators that perform monitoring should be defined. Tools used should be reviewed and approved by appropriate management. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Incident Response to verify monitoring and reporting duties have been assigned. |
| 326 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Baseline | The physical environment is monitored to detect potential unauthorized access. | Financial institutions should monitor the physical environment (such as entrances, restricted areas, confidential data repositories, vault areas, and ATMs) to detect and respond to unauthorized access attempts. Implementing appropriate preventative and detective physical controls protects systems, data, employees, and infrastructure against malicious or unauthorized persons. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Physical Security and discuss with management the implemented physical security controls for detecting unauthorized access.<br><br>Review the inventory of security tools and discuss with management if the financial Institution uses security tools to monitor for unauthorized access to the financial Institution's physical environment. |
| 327 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Evolving | A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall). | A security information and event management (SIEM) tool is an approach to security management that a financial institution can take that provides a holistic view of an organization's IT security. A SIEM system collects logs and other security-related documentation for analysis and correlation. To allow the system to identify anomalous events, it's important that the SIEM administrator first creates a profile of the system under normal event conditions. SIEM systems are typically expensive to deploy and complex to operate and manage. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and discuss with management the processes in place for correlating system and network event information across the financial Institution.<br><br>Determine if the financial Institution is using an application or tool to correlate system alerts and how the solution is integrated with the incidence response plan and how it is monitored. |
| 328 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Intermediate | Controls or tools (e.g., data loss prevention) are in place to detect potential unauthorized or unintentional transmissions of confidential data. | Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Data Loss Prevention and risk assessments to determine if the financial Institution has processes or controls in place to detect potential unauthorized or unintentional transmissions of confidential data.<br><br>Review the inventory of security tools and discuss with management if the financial Institution uses security tools to detect potential unauthorized or unintentional transmissions of confidential data. |
| 329 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Intermediate | Event detection processes are proven reliable. | Event detection processes include some of the following design considerations: Fault tolerance, adaptability, autonomy, and transparency. Event detection may fall under testing of key controls. Event detection processes may be tested by running exercises or testing that emulates the types of events they are designed to detect. The effectiveness of event detection depends on the quality of the data and data rules. | Review the solutions used to detect events and the solution testing to determine if the solution is configured and functioning correctly. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 330 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Intermediate | Specialized security monitoring is used for critical assets throughout the infrastructure. | Protecting institutions from cyber threats requires constant vigilance over security infrastructure and critical information assets. Real time security logs and alerts help identify and thwart malicious activity, while balancing numerous ongoing operational and strategic security tasks. Scalable processes and advanced analysis technology are also key elements for effective detection of and response to threats. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and the Risk assessment to determine the process for identifying critical assets to receive additional monitoring.<br><br>Discuss with management how security monitoring tools are implemented to monitor critical assets. |
| 331 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Advanced | Automated tools detect unauthorized changes to critical system files, firewalls, IPS, IDS, or other security devices. | Configuration management control tools are deployed on endpoints, mobile devices, and security devices (firewalls, IDS, IPS, routers) which alert when changes occur to system files. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Change Management to determine the approved process for making changes to various critical systems (security, network, core system).<br><br>Discuss with management how they utilize automated tools to monitor for changes and assess whether that tool is monitoring all critical systems. |
| 332 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Advanced | Real-time network monitoring and detection is implemented and incorporates sector-wide event information. | Network traffic is monitored in real-time with automated tools. This type of service can be managed by both institution personnel and third-party staff. An example of such a service is FireEye which monitors outgoing internet traffic. Suspicious or malicious traffic detected by this monitoring service is shared with all clients for real-time preparedness. Information sharing of network metrics and anomaly detection can assist sector entities in better understanding cyber threats and vulnerabilities, as well as individual institution's relative risk profiles and capabilities. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Incident Response, Network Management to determine how management is using automated solutions monitor network and sector events in real time.<br><br>Discuss with management how the solutions are configured to detect suspicious or malicious events. |
| 333 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Advanced | Real-time alerts are automatically sent when unauthorized software, hardware, or changes occur. | Advanced network monitoring tools can be deployed on the network to detect any change to software and hardware. From there, management can review the change for authorization and trace it back to change management source documentation for proper authorization as defined in policy. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Asset Management and Change Management and discuss with management if the financial Institution has processes in place for alerting personnel in real-time when unauthorized asset changes occur.<br><br>Discuss with management any solutions implemented to monitor for changes and alerts in real-time when unauthorized software, hardware, or changes occur.<br><br>Review the most recent report of alerts triggered by unauthorized asset changes and discuss with management actions taken as a result of the alerts. |
| 334 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Advanced | Tools are in place to actively correlate event information from multiple sources and send alerts based on established parameters. | This generally refers to Security Incident and Event Management (SIEM). The server housing the SIEM aggregates logs from all devices on the network (activity logs, syslog, configuration changes) and correlates behavior (activity) throughout the network for potential malicious activity and alerts senior management accordingly. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution has an alert and response process.<br><br>Review the listing of software or application solutions used by the financial Institution to monitor and correlate events. |
| 335 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Innovative | The institution is leading efforts to develop event detection systems that will correlate in real time when events are about to occur. | New and emerging security analytics solutions can provide real-time threat detection and alerting to administrators and security analysts. These solutions can integrate with intrusion prevention, intrusion detection, and data loss prevention technologies to provide alerts and enable real-time remediation of threat activity. | Review the IT strategy and determine how management is planning to use the solutions and the time frame and resources assigned to the projects. Review the project plans for the new technologies to assess the project plans and direction of projects. |
| 336 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Innovative | The institution is leading the development effort to design new technologies that will detect potential insider threats and block activity in real time. | According to US-CERT, unique patterns of insider threat behavior include: intellectual property (IP) theft, IT sabotage, fraud, espionage, and accidental insider incidents. | Review the IT strategy and project plans to assess the technologies being developed. Review project plans for compliance with project charters and goals. |
| 337 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Baseline | A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner. | Patch Management is an easy concept to understand, but a challenge to execute. Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. Patch management is required by various security compliance frameworks, mandates, and other policies. For example, NIST Special Publication (SP) 800-532 requires the SI-2, Flaw Remediation security control, which includes installing security-relevant software and firmware patches, testing patches before installing them, and incorporating patches into the organization's configuration management processes. Another example is the Payment Card Industry (PCI) Data Security Standard (DSS), which requires that the latest patches be installed and sets a maximum timeframe for installing the most critical patches. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management and discuss with management the process for applying software and firmware patches. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 338 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Baseline | Patches are tested before being applied to systems and/or software. | Effective patch management may include establishing procedures to stay abreast of patches, to test them in a segregated environment, and to install them when appropriate. Testing software and firmware updates can identify compatibility and instability issues that could cause serious operational disruptions. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management and discuss with management the process for testing patches prior to deploying to production.<br><br>Review a sample of patch management updates to determine if the financial Institution tests patches prior to deploying to production. |
| 339 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Baseline | Patch management reports are reviewed and reflect missing security patches. | Patch management solutions can produce a variety of reports that include showing patch compliance, exceptions, and days outstanding. Reports reflecting missing critical patches to servers, desktops, laptops, and other devices should be remediated as soon as possible. | Review a sampling of patch management reports and determine if they reflect missing patches.<br><br>Discuss with management their process for reviewing patch management reports. |
| 340 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Evolving | A formal process is in place to acquire, test, and deploy software patches based on criticality. | Patch management standards should include procedures for identifying, evaluating, approving, testing, installing, and documenting patches and to identify available patches and to acquire them from trusted sources.<br><br>Rather than automatically applying every patch and hotfix that is released by vendors, a process should be developed to evaluate the criticality and applicability of the software patch. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management and determine if the financial Institution has documented a process to acquire, test, and deploy software patches based on criticality.<br><br>Discuss with management the methodology for determining the criticality of patches. |
| 341 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Evolving | Systems are configured to retrieve patches automatically. | Patch management software solutions automatically scan for and detect missing patches and can add them to a repository database for future deployment. Many patch management solutions will automatically download patches for the software they detect. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management and discuss with management the methodology for obtaining patches and whether this process occurs automatically. |
| 342 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Evolving | Operational impact is evaluated before deploying security patches. | The patch management process takes into account the business impacts of the systems and applications being patched. Patches are deployed to systems and applications taking into account any established system availability requirements and previously established maintenance windows. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management and determine if the financial Institution has documented a process to acquire, test, and deploy software patches based an evaluation of operational impact. |
| 343 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Evolving | An automated tool(s) is used to identify missing security patches as well as the number of days since each patch became available. | The patch management software automatically scans and identifies missing patches in its inventory. It also tracks the number of days outstanding that the patches have not been deployed since they were issued. | Review a sampling of patch management reports and determine if the tool identifies the number of days since the unapplied patch became available.<br><br>Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management<br>or discuss with management the timeframe a patch must be tested and deployed from when it is released. |
| 344 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Evolving | Missing patches across all environments are prioritized and tracked. | The patch management solution should be comprehensive, crossing all technologies and environments (e.g., DMZ, LAN, WAN, Windows, Telecommunications, Routers, Switches, ATMs, and other infrastructure devices). Patches should be risk rated and prioritized. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management and discuss with management the methodology for prioritizing and tracking unapplied patches.<br><br>Review the patch management report and determine if patches are risk rated and prioritized according to patch management policy, standards, and/or guidelines. |
| 345 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Intermediate | Patches for high-risk vulnerabilities are tested and applied when released or the risk is accepted and accountability assigned. | Patches and vulnerabilities should be identified and prioritized (risk ranked). Patches not applied (exceptions) should be tracked and, if not corrected, presented to management or an appropriate committee for review and acceptance. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management and discuss with management the process for accepting the risk of not applying patches for high-risk vulnerabilities.<br><br>Discuss with management the method used to prioritize the remediation of vulnerabilities, and deployment of patches. |
| 346 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Advanced | Patch monitoring software is installed on all servers to identify any missing patches for the operating system software, middleware, database, and other key software. | Patch management solutions should be scalable, easy to use and robust enough to identify missing patches on a wide variety of systems and commercial software. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management and discuss with management if the financial Institution identifies missing patches for the operating system software, middleware, database, and other key software.<br><br>Review the patch management reports for missing patches and discuss with management any actions that will be taken as a result of the missing patches. |
| 347 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Advanced | The institution monitors patch management reports to ensure security patches are tested and implemented within aggressive time frames (e.g., 0-30 days). | The financial institution's patch management policy and procedures should reflect aggressive time frames for patching critical vulnerabilities on critical and mission critical systems (a risk-based approach). For example; the policy may dictate all patches with a CVSS Score of 7-10 be deployed to all systems within 2 weeks of deployment; while all patches with a CVSS Score of 4-6 be deployed by 4 weeks, and those with a CVSS Score of 1-3 deployed during the next patching cycle. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management to determine the time frames patches are required to be implemented within.<br><br>Review patch management reports and verify patches are deployed within the time frames according to policy. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 348 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Innovative | The institution develops security patches or bug fixes or contributes to open source code development for systems it uses. | This statement addresses the capability of a financial institution to participate in the development of patches regarding open source software (e.g., SSL, Linux, and JAVA). This software is free for use in most cases and institutions may opt to take advantage of the lower cost solution. In doing so, they may be introducing potential risks into their computing environment. A mature organization has the capability to assist in developing patches or fixing open source security flaws. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management; Software Development and discuss with management the financial Institution's process for developing security patches or bug fixes for open source code used in system development. |
| 349 | 3: Cybersecurity Controls | 3: Corrective Controls | 1: Patch Management | Innovative | Segregated or separate systems are in place that mirror production systems allowing for rapid testing and implementation of patches and provide for rapid fallback when needed. | Financial institutions should have a patch management program requiring patch testing as quickly as patches are received for systems (e.g., desktops, servers, tablets, mobile device, and switches). They should be configured similar to the production systems. These systems should be segregated from the production environment. While rapid fallback may only be needed for installations on live systems, a process should be in place for fallback when necessary to reverse instability or compatibility issues with installing patches. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Patch Management and determine if the financial Institution has documented a process to acquire, test, and deploy software patches in a segregated environment from production. |
| 350 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Baseline | Issues identified in assessments are prioritized and resolved based on criticality and within the time frames established in the response to the assessment report. | Gramm-Leach-Bliley Act (GLBA) guidelines direct financial institutions to test key information security program controls. Senior management should require periodic self-assessments to provide an ongoing assessment of policy adequacy and compliance and ensure timely corrective action of significant deficiencies.<br><br>Performing a risk assessment of threats to customer information is a regulatory requirement, set forth in GLBA Guidelines. Findings should be ranked in priority and mitigated based upon the risk to the financial institution. Results from the risk assessment should be formally presented to senior management and the board of directors at least annually. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Risk Management to determine if the financial Institution has a process for determining the criticality of risk for issues identified during assessments.<br><br>Discuss with management the methodology for prioritizing and tracking issues identified in assessments.<br><br>Review recent risk assessments and audits, including management responses and corrective actions, to determine that issues are prioritized and discuss with management if these issues are being tracked and resolved based on established timeframes. |
| 351 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Evolving | Data is destroyed or wiped on hardware and portable/mobile media when a device is missing, stolen, or no longer needed. | Financial institutions should have a formal data destruction policy and procedures to handle the various types of data outlined within their data classification policy.<br><br>This includes paper and electronic data on computer hard drives, including data stored in all potential electronic repositories such as copy machine hard drives, printer hard drives, fax machine hard drives, and mobile devices (i.e., phones and tablets). | Review the Financial Institution's Policy, Standards and Guidelines specific to: Data Destruction or Media Sanitization and determine if the financial Institution has a process for data and media destruction. |
| 352 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Evolving | Formal processes are in place to resolve weaknesses identified during penetration testing. | Financial institutions should engage in penetration testing conducted by a qualified third-party. Results from those exercises identify weaknesses in key controls, design, and operating environment. The financial institution should have a process to track all significant weaknesses to resolution. | Review results of penetration tests, risk assessments and audits.<br><br>Review management's plan for remediation and current status. |
| 353 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Intermediate | Remediation efforts are confirmed by conducting a follow-up vulnerability scan. | As the financial institution remediates vulnerabilities from scans, additional scans should be completed to ensure the patches and other corrective actions are actually addressing the vulnerabilities. Many vulnerabilities are not fixed by simply applying a patch to a system or application, but by a series of tasks in addition to applying the patch. For example, a patch to correct a vulnerability in the Microsoft Operating system may incorporate multiple steps: applying a patch to the systems in addition to implementing changes within an Active Directory group policy object. | Discuss with management any audit issues or findings identified as resolved or remediated.<br><br>Review the latest vulnerability scan to confirm remediation efforts as resolved. |
| 354 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Intermediate | Penetration testing is repeated to confirm that medium- and high-risk, exploitable vulnerabilities have been resolved. | Medium and high risk weaknesses identified in the course of vulnerability testing can pose a significant risk to the financial institution. As the financial institution remediates these vulnerabilities, additional testing should be performed to provide assurance those weaknesses are fully remediated. Effective patch management is a systematic and repeatable process which includes comprehensive monitoring processes, assessing and prioritizing vulnerabilities, performing testing, deploying patches, and documenting installed patches and remediation. | Review penetration test results to verify remediated activities are addressed according to the remediation activities report. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 355 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Intermediate | Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties. | Financial institutions often outsource security investigations and forensic analysis to a skilled and qualified third-party. Only highly qualified personnel experienced with preserving this type of information should conduct forensic analysis. The financial institution should have an appropriate due diligence process in place to ensure any third-party is fully qualified to performed services contracted. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution has a methodology for conducting security investigations and forensic analysis of events.<br><br>Discuss with management the methodology for identifying and selecting qualified staff or third parties for conducting security investigations, analysis and remediation activities. |
| 356 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Intermediate | Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action. | Financial institutions often outsource security investigations and forensic analysis to a skilled and qualified third-party. Only highly qualified personnel experienced with preserving this type of information should conduct forensic analysis. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution's methodology for conducting security investigations and forensic analysis of events includes generally accepted and appropriate forensic procedures are used to gather and present evidence to support potential legal action. |
| 357 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Intermediate | The maintenance and repair of organizational assets are performed by authorized individuals with approved and controlled tools. | A financial institution's IT staff should be commensurate with the types of systems and infrastructure. For example, staff responsible for making changes to firewalls should be sufficiently qualified to do so, such as by receiving certification in the specific technology and ongoing training. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Asset Management, Change Management and determine the financial Institution has a process for approving and monitoring the maintenance and repair of assets. |
| 358 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Intermediate | The maintenance and repair of organizational assets are logged in a timely manner. | Any change to a mission critical or critical asset should be formally documented within the Change Management process. Changes should be logged, reviewed, tested, and approved prior to release into production. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Asset Management, Change Management and determine the financial Institution has a process for approving and monitoring the maintenance and repair of assets. |
| 359 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Advanced | All medium and high risk issues identified in penetration testing, vulnerability scanning, and other independent testing are escalated to the board or an appropriate board committee for risk acceptance if not resolved in a timely manner. | Different testing processes (e.g., penetration, vulnerability, social engineering) potentially will identify significant findings. All significant findings should be reported to senior management and the Board with a valid remediation timeline. Some findings/risk elements (e.g., water-based sprinkler systems, legacy systems scheduled for replacement) may not be cost effective to repair. It is important that the board or assigned committee reviews all findings. Decisions to mitigate or accept risk should be documented to achieve accountability for risk decisions. | Review the vulnerability and penetration results and determine whether tracking of findings from audits have been documented and have a management response and corrective action plan. |
| 360 | 3: Cybersecurity Controls | 3: Corrective Controls | 2: Remediation | Innovative | The institution is developing technologies that will remediate systems damaged by zero-day attacks to maintain current recovery time objectives. | Financial institutions should have a recovery time objective (RTO) as determined by completing a BCP BIA. The BIA determines critical systems/services and their RTO. Depending on their impact, zero-day attacks may necessitate higher BCP capabilities such as full systems failover and/or the ability to quickly reconstitute or restore systems and data to their pre-attack state. | Review the business impact analysis (BIA) recovery time objectives (RTO) and discuss with management efforts or technologies under development to remediate systems damaged by zero-day attacks to maintain the financial Institution's current RTOs. |
| 361 | 4: External Dependency Management | 1: Connections | 1: Connections | Baseline | The critical business processes that are dependent on external connectivity have been identified. | Management should prepare a listing of all critical services (and the respective third-party vendor) where an external connection is necessary for the service to be provided (e.g., core system, mortgage processing, Bank Secrecy Act monitoring). | Review the list of critical services dependent on external service providers identified in the business impact analysis (BIA) and review network topology diagram(s) to validate the external service provider connections are properly identified. |
| 362 | 4: External Dependency Management | 1: Connections | 1: Connections | Baseline | The institution ensures that third-party connections are authorized. | There should be evidence that each third-party service (through an external connection) has been formally approved. The authorization can be provided by an authority such as senior management, an IT steering committee, or the board of directors. The evidence will likely come from minutes or signed contracts. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management to determine if processes are defined for approving Third-Party vendors.<br><br>Discuss with management their methodology for performing due diligence on Third-Party connections prior to signing a contract. |
| 363 | 4: External Dependency Management | 1: Connections | 1: Connections | Baseline | A network diagram is in place and identifies all external connections. | To ensure appropriate network security, institutions should maintain accurate network and data flow diagrams that 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. Management should be able to produce a visual depiction (i.e. diagram or topology map) of all external vendor connections. This could be a stand-alone document or part of the overall network topology. | Review the list of all service providers and identify all service providers that provide a service that requires an external connect.<br><br>Review the network topology diagram(s) to make sure all external vendor connections are identified. |
| 364 | 4: External Dependency Management | 1: Connections | 1: Connections | Baseline | Data flow diagrams are in place and document information flow to external parties. | This is similar to the diagram of external vendor connections; however, this is one step further. The data flow diagram is an extension of the connections and shows the direction of information flowing in and out of the financial institution's network. | Review (if available) a data flow diagram which explains how data flows to and from vendors outside of the financial Institution's network. |
| 365 | 4: External Dependency Management | 1: Connections | 1: Connections | Evolving | Critical business processes have been mapped to the supporting external connections. | Critical services are defined and any associated external connectivity is reflected in a network diagram or topology. | Review the network topology diagram(s) and verify critical services that require an external connection are identified. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 366 | 4: External Dependency Management | 1: Connections | 1: Connections | Evolving | The network diagram is updated when connections with third parties change or at least annually. | Financial institutions should identify changes to technology infrastructure or new products and services that might increase the financial institution's risk. 'Each time third-party connections change, the pertinent network diagram(s) are updated as soon as possible, or at a minimum, via an annual update process. | Review the network topology diagram(s) and verify external connections are identified.<br><br>Discuss with management the methodology for updating network topology diagram(s) when a third party connection changes, or at least annually. |
| 367 | 4: External Dependency Management | 1: Connections | 1: Connections | Evolving | Network and systems diagrams are stored in a secure manner with proper restrictions on access. | Diagrams containing sensitive information are stored within secure file shares and/or encrypted folders on the network. These files should be restricted based upon role or need-to-know (e.g., senior IT staff). | Discuss with management their practice for storing these diagrams and the access restrictions around their storage.<br><br>Review the file share permissions (authorized access) within Active Directory for the specific domain folder storing the network diagrams. |
| 368 | 4: External Dependency Management | 1: Connections | 1: Connections | Evolving | Controls for primary and backup third-party connections are monitored and tested on a regular basis. | Management should control and monitor all third-party connections. Controls can include network segmentation, inline IDS/IPS and SIEM or log aggregation tools.<br><br>Further, back up connections should be tested to ensure resiliency and limit outage risk. | Discuss with management how third party access to the financial institution's network is controlled and monitored. |
| 369 | 4: External Dependency Management | 1: Connections | 1: Connections | Intermediate | A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity. | A physical inventory should validate the accuracy of an automated asset inventory tool. Network diagrams should be comprehensive, and up-to-date, including all inventoried assets. | Review the validated IT asset inventory of hardware and software.<br><br>Review network, data flow and connectivity diagrams and compare against the IT asset inventory to validate the accuracy of the asset inventory. |
| 370 | 4: External Dependency Management | 1: Connections | 1: Connections | Intermediate | Security controls are designed and verified to detect and prevent intrusions from third-party connections. | Security devices such as intrusion detection systems (IDS) or intrusion prevention systems (IPS) are in place to alert management of an intrusion. Penetration tests are conducted to simulate an intrusion or other anomalous activity originating from third-party connections. | Review third party testing (reports) and determine the scope of the pen test (which IP addresses are tested). |
| 371 | 4: External Dependency Management | 1: Connections | 1: Connections | Intermediate | Monitoring controls cover all external connections (e.g., third-party service providers, business partners, customers). | Controls can include intrusion detection systems (IDS), intrusion prevention systems (IPS) and Security information and event management (SIEM) tools. A baseline should establish normal activity or traffic. Monitoring controls identify anomalous activity that may require incident response or other corrective actions. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Network Management to determine if the financial institution has a process for monitoring external network connections.<br><br>Discuss with management if the financial institution has established a network activity baseline to identify typical utilization patterns so that significant deviations can be detected.<br><br>Review the network topology diagram(s) and data flow diagram(s) to determine if they identify hardware, software, and network components, internal and external connections, and types of information passed between systems. |
| 372 | 4: External Dependency Management | 1: Connections | 1: Connections | Intermediate | Monitoring controls cover all internal network-to-network connections. | Controls can include intrusion detection systems (IDS), intrusion prevention systems (IPS) and Security information and event management (SIEM) tools. A baseline should establish normal activity or traffic. Monitoring controls identify anomalous activity that may require incident response or other corrective actions. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Network Management to determine if the financial institution has a process for monitoring internal network traffic.<br><br>Discuss with management if the financial institution has established a network activity baseline to identify typical utilization patterns so that significant deviations can be detected.<br><br>Review the network topology diagram(s) and data flow diagram(s) to determine if they identify hardware, software, and network components, internal and external connections, and types of information passed between systems. |
| 373 | 4: External Dependency Management | 1: Connections | 1: Connections | Advanced | The security architecture is validated and documented before network connection infrastructure changes. | 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. All network changes should be tested and validated to ensure key controls are effective and not inadvertently broken. Validation can include review of network and data flow diagrams, security configuration reviews, and network scanning or even penetration testing. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and discuss with management the methodology for validating the financial institution's security architecture before implementing network changes. |
| 374 | 4: External Dependency Management | 1: Connections | 1: Connections | Advanced | The institution works closely with third-party service providers to maintain and improve the security of external connections. | Examples include requiring each vendor to use a single remote access solution, ensuring that vendors do not share credentials, multifactor authentication, and enforcing the concept of least access or privilege. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Identity and Access Management and Third-Party Service Provider Management to determine if the financial Institution has documented external vendor access practices. |
| 375 | 4: External Dependency Management | 1: Connections | 1: Connections | Innovative | Diagram(s) of external connections is interactive, shows real-time changes to the network connection infrastructure, new connections, and volume fluctuations, and alerts when risks arise. | Automated tools are in place that collect live network data to generate updated network diagrams and associated information on demand and in real-time. | Discuss with management the financial Institution's automated tool/process to capture and reflect real-time changes to the network infrastructure. |
| 376 | 4: External Dependency Management | 1: Connections | 1: Connections | Innovative | The institution's connections can be segmented or severed instantaneously to prevent contagion from cyber attacks. | This may be accomplished through advanced intrusion prevention system technology. | Review the financial Institution's process to automatically terminate vendor access, if warranted. Determine if this has been tested and, if so, review the documentation from the test for appropriateness. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 377 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Baseline | Risk-based due diligence is performed on prospective third parties before contracts are signed, including reviews of their background, reputation, financial condition, stability, and security controls. | A financial institution's board and management should conduct appropriate due diligence on all potential third parties before selecting and entering into contracts or relationships. A financial institution should not rely solely on experience with or prior knowledge of the third-party as a proxy for an objective, in-depth assessment of the third-party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner.<br><br>The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. More extensive due diligence is appropriate when a third-party relationship involves critical activities. On-site visits may be useful to understand fully the third-party's operations and capacity. If the institution uncovers information that warrants additional scrutiny, it should broaden the scope or assessment methods of the due diligence as appropriate. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management and discuss with management methodology for conducting the appropriate due diligence in third-party research, selection, and relationship management. |
| 378 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Baseline | A list of third-party service providers is maintained. | Management should maintain a current listing of all third-party service providers. This list should be all-inclusive (i.e. Services/products delivered in-house at the financial institution as well as services provided via external connection to the internet). | Review management's listing of all third party service providers and verify all services provided via a third-party connection are captured (e.g. list is current, all critical and/or high risk vendors are included). |
| 379 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Baseline | A risk assessment is conducted to identify criticality of service providers. | Financial institution management should review the list of all third-party vendors to assess/define the criticality of each vendor (e.g., high, medium, low risk OR critical, non-critical, etc.). This list should be based on criticality to drive the frequency (and the corresponding level of detail) of ongoing due diligence reviews by management. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management and discuss with management the methodology for determining the criticality of each vendor.<br><br>Review the risk assessment to determine if the criticality of each vendor is presented (e.g. high, medium, low risk OR critical, non-critical, etc.). |
| 380 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Evolving | A formal process exists to analyze assessments of third-party cybersecurity controls. | Financial institutions should include the types of assessments and audit reports it is entitled to receive (e.g., financial, internal control, and security reviews) from a third-party in the contract. The contract should specify the audit frequency, any charges for obtaining the audits, as well as the rights of the institution and its regulatory agencies to obtain the results of the audits in a timely manner. Management has established formal policy assigning accountability for ongoing monitoring of third-party service providers throughout the life of the contract. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management to determine if the financial Institution has a formal process for reviewing and analyzing the assessments of third-party service providers' cybersecurity controls. |
| 381 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Evolving | The board or an appropriate board committee reviews a summary of due diligence results including management's recommendations to use third parties that will affect the institution's inherent risk profile. | Third parties that can affect the risk profile include those with access to internal systems or nonpublic customer information, those storing and/or processing information that support critical activities, and cloud computing providers that support critical activities. | Review the Board report, or an appropriate board committee report, for discussion of due diligence results to determine if the Board receives information on the financial Institution's exposure from third parties. |
| 382 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Intermediate | A process is in place to confirm that the institution's third-party service providers conduct due diligence of their third parties (e.g., subcontractors). | Critical vendors often have third-party relationships that can present risk to their clients if not properly managed. These vendors should have effective third-party risk management programs in place and appropriate methods for demonstrating due diligence over their third-party relationships. | Request and review the risk assessments completed for all critical vendors (or a sampling). |
| 383 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Intermediate | Pre-contract, physical site visits of high-risk vendors are conducted by the institution or by a qualified third party. | Financial institutions may rely on their own site visits or that of a qualified third-party such as an auditor performing a Service Organization Control (SOC) audit. | Request and review the risk assessments completed for all critical vendors (or a sampling). |
| 384 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Advanced | A continuous process improvement program is in place for third-party due diligence activity. | Management conducts reviews of the due diligence program to determine if any gaps exist and work towards self-improvement of the program. | Discuss with management if, and how, reviews of the due diligence program take place in order to determine if any gaps exist within the documentation. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 385 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Advanced | Audits of high-risk vendors are conducted on an annual basis. | Critical (high risk) vendors should provide an annual audit report of their control structure to ensure effectiveness. Per American Institute of Certified Public Accountants (AICPA) guidelines, a Service Organization Controls (SOC) 1 report or Statement on Standards for Attestation Engagements 16 (SSAE 16) audit report is the standard for in-house vendor services (e.g., core system maintained by the financial institution). A SOC 2 audit is the standard for a cloud service provider because the vendor processes or stores customer personally identifiable information (PII) outside of the financial institution's network. In some cases, a financial institution may supply a bridge letter. A bridge letter that describes updates or changes in its controls since the previous type 1 or type 2 report. However, there are no provisions in SSAE No. 16 for auditors to report on such a letter. | Review Third-Party Service Provider Audit Reports and verify the financial Institution conducted an audit or has a "bridge" letter (where applicable) for all critical service providers or high risk vendors. |
| 386 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Innovative | The institution promotes sector-wide efforts to build due diligence mechanisms that lead to in-depth and efficient security and resilience reviews. | The financial institution works with other external institutions and business partners to seek methods to improve overall due diligence practices (e.g., advisory boards). | Determine if, and how, the financial Institution works with other institutions and business partners to seek methods to improve overall due diligence practices (e.g. advisory boards). |
| 387 | 4: External Dependency Management | 2: Relationship Management | 1: Due Diligence | Innovative | The institution is leading efforts to develop new auditable processes and for conducting due diligence and ongoing monitoring of cybersecurity risks posed by third parties. | Techniques may include limiting access to an as needed basis and/or for maintenance purposes and auditing of all third-party access credentials. Technology solutions include use of VPNs, multifactor authentication, geolocation, time, IP, and device restrictions. | Discuss with management any efforts to develop new auditable processes and for conducting due diligence and ongoing monitoring of cybersecurity risks posed by third parties. |
| 388 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Baseline | Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential data or provide critical services. | Financial institution management may rely on third-parties to provide critical services; management, however, remains responsible for ensuring the confidentiality, integrity and availability of the financial institution's systems and information by overseeing the effectiveness of the services provided by third-party service providers. Management must require its service providers by contract to implement appropriate measures designed to meet the objectives of regulatory guidelines for safeguarding member information (GLBA guidelines). Management should verify that third-party service providers implement and maintain controls sufficient to appropriately mitigate risks. The financial institution's contracts customarily would:<br>• Include minimum control and reporting standards;<br>• Provide for the right to require changes to standards as external and internal environments change; and<br>• Specify that the financial 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 set forth in the GLBA guidelines. | Review the list of Third-Party service providers against the list of Third-Party service provider contracts and determine if a contract is in place for all third parties that process, store, or transmit confidential data or provide critical services. |
| 389 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Baseline | Contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits. | Financial institution management may rely on third-parties to provide critical services; management, however, remains responsible for ensuring the confidentiality, integrity and availability of the financial institution's systems and information by overseeing the effectiveness of the services provided by third-party service providers. Management must require its service providers by contract to implement appropriate measures designed to meet the objectives of regulatory guidelines for safeguarding member information (GLBA guidelines). Management should verify that third-party service providers implement and maintain controls sufficient to appropriately mitigate risks. The financial institution's contracts customarily would:<br>• Include minimum control and reporting standards;<br>• Provide for the right to require changes to standards as external and internal environments change; and<br>• Specify that the financial 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 set forth in the GLBA guidelines. | Review the third party service provider contracts and determine if the contracts acknowledge that the third party is responsible for the security of the financial Institution's confidential data that it possesses, stores, processes, or transmits. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 390 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Baseline | Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party. | Financial institution management may rely on third-parties to provide critical services; management, however, remains responsible for ensuring the confidentiality, integrity and availability of the financial institution's systems and information by overseeing the effectiveness of the services provided by third-party service providers. Management customarily oversees outsourced operations through:<br>• Appropriate due diligence in third-party research, selection, and relationship management;<br>• Contractual assurances for security responsibilities, controls, and reporting;<br>• Nondisclosure agreements regarding the financial institution's systems and data;<br>• Independent review of the third-party's security through appropriate reports from audits and tests;<br>• Coordination of incident response policies and contractual notification requirements; and<br>• Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported. | Review the third party service provider contracts determine if the contracts acknowledge that the third party is responsible for having their controls independently reviewed and validated regularly. |
| 391 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Baseline | Contracts identify the recourse available to the institution should the third party fail to meet defined security requirements. | Financial institution management may rely on third-parties to provide critical services; management, however, remains responsible for ensuring the confidentiality, integrity and availability of the financial institution's systems and information by overseeing the effectiveness of the services provided by third-party service providers. Management should oversee outsourced operations through contractual assurances for security responsibilities, controls, and reporting. Management should include service level agreements (SLAs) in its outsourcing contracts to specify and clarify performance expectations, as well as establish accountability. These SLAs formalize the performance criteria against which the quantity and quality of service should be measured. Management should closely monitor the service provider's compliance with key service level agreements. | Review the third party service provider contracts and determine if the contracts include a recourse and termination process for non-performance. |
| 392 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Baseline | Contracts establish responsibilities for responding to security incidents. | Management may rely on third parties to provide critical services; management, however, remains responsible for ensuring the confidentiality, integrity and availability of the financial institution's systems and information by overseeing the effectiveness of the services provided by third-party service providers. Management should oversee outsourced operations through contractual assurances for security responsibilities, controls, and reporting. Management should include service level agreements (SLAs) in its outsourcing contracts to specify and clarify performance expectations, as well as establish accountability. These SLAs formalize the performance criteria against which the quantity and quality of service should be measured. Management should closely monitor the service provider's compliance with key service level agreements. | Review the third party service provider contracts and determine if the contracts include responsibilities for responding to security incidents. |
| 393 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Baseline | Contracts specify the security requirements for the return or destruction of data upon contract termination. | Financial institution management should assess the timeliness and expense of contract termination provisions. The extent and flexibility of termination rights can vary depending upon the service. Management should consider including termination rights for a variety of conditions. Contracts should include provisions for timely return or destruction of the financial institution's data and resources. | Review the third party service provider contracts and determine if the contracts include notification and timeframe requirements for the timely return or destruction of the institution's data and resources. |
| 394 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Evolving | Responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties are formally documented in the contract. | Financial institutions should have a clear understanding of service provider roles and responsibilities. This understanding enables management to determine whether additional security is necessary on third-party owned, managed, or maintained devices that may reside in their data center. | Review the third party service provider contracts and determine if the contracts formally document responsibilities for managing devices. |
| 395 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Evolving | Responsibility for notification of direct and indirect security incidents and vulnerabilities is documented in contracts or service-level agreements (SLAs). | An indirect security incident would be one which affected another client directly with potential for more widespread impact pending full investigation, containment, and eradication. | Review the third party service provider contracts and determine if the contracts establish processes and accountability for identifying, reporting, investigating, and escalating incidents. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 396 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Evolving | Contracts stipulate geographic limits on where data can be stored or transmitted. | Financial institutions should be aware of and approve where their customer data is being processed and/or stored by their third parties. Contracts should specifically define where this will take place. Storing data outside of the U.S. can present different legal concerns due to laws that may be dissimilar to U.S. laws. | Review the third party service provider contracts and determine if the contracts stipulate geographic limits on where data can be stored or transmitted. |
| 397 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Intermediate | Third-party SLAs or similar means are in place that require timely notification of security events. | Contracts should require timely notice for conditions that can materially affect a financial institution and its customers. Contracts should stipulate incident reporting requirements to ensure there are clearly documented processes and accountability for identifying, reporting, investigating, and escalating incidents in a timely manner. | Review the third party service provider contracts and determine if the contracts establish processes and accountability for identifying, reporting, investigating, and escalating incidents. |
| 398 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Advanced | Contracts require third-party service provider's security policies meet or<br>exceed those of the institution. | Under the Gramm Leach Bliley Act (GLBA) guidelines, service provider contracts are required to have a provision agreeing to implement appropriate measures designed to meet the objectives of the guidelines. Before entering into outsourcing contracts, and throughout the life of the relationship, institutions should ensure the third-party service provider's physical and data security standards meet or exceed standards required by the financial institution. | Review the third party service provider contracts and determine if the contracts require third-party service provider's security policies meet or exceed those of the financial Institution. |
| 399 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Advanced | A third-party termination/exit strategy has been established and validated with management. | Management should have an exit strategy in the event a third-party would happen to breach contract or not perform according to service level agreements. The strategy should explain what the financial institution expects to be done both internally and by the vendor as well as identify potential vendor replacements. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management to determine if there are provisions regarding an exit strategy in the event a Third-Party would happen to breach contract or not perform according to service level agreements. The strategy should explain what the financial Institution expects to be done both internally and by the vendor as well as consideration for potential vendor replacements. |
| 400 | 4: External Dependency Management | 2: Relationship Management | 2: Contracts | Innovative | The institution promotes a sector-wide effort to influence contractual requirements for critical third parties to the industry. | Management participates in advisory boards of some kind to improve contract provisions in standard vendor contracts. | Discuss with management their participation in Third-Party service provider advisory boards or similar co-op situations to improve contract provisions in standard vendor contracts. |
| 401 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Baseline | The third-party risk assessment is updated regularly. | The GLBA guidelines include at least annual reporting to the board or an appropriate committee of the board on material matters related to the information security program required therein, such as on the risk assessment and service provider arrangements. Where indicated by the financial institution's risk assessment, these guidelines obligate financial institutions to monitor service providers for compliance with their contractual requirement to implement appropriate measures designed to meet the objectives of the guidelines. | Request evidence regarding annual reporting to the board or an appropriate committee of the board on material matters such as risk assessment and service provider arrangements. This may be included in the Annual Security Report, within ongoing Information Security reports (or minutes) to a committee of the board or the board directly, etc. |
| 402 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Baseline | Audits, assessments, and operational performance reports are obtained and reviewed regularly validating security controls for critical third parties. | Management obtains various materials to demonstrate their ongoing oversight of critical vendors. These typically include items such as audited financial reports, SSAE-16 or SOC 2 audits, and key performance metrics as stipulated in contractual service level agreements. | Request and review audited financial reports, SSAE-16 or SOC 2 audits, and key performance metrics (if available) as stipulated in contract service level agreements. |
| 403 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Baseline | Ongoing monitoring practices include reviewing critical third-parties' resilience plans. | This pertains to the vendor's BCP/DR program. This is often addressed in SSAE-16 (SOC 1) and SOC 2 audits at a high level. A separate request may be necessary to review the vendor's BCP/DR program and/or processes in more detail. | Review Third-Party Service Provider Audit Reports as a part of ongoing monitoring of service providers. |
| 404 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Evolving | A process to identify new third-party relationships is in place, including identifying new relationships that were established without formal approval. | All vendors should be identified and categorized with respect to risk. One means to detect new relationships which bypassed the formal approval process is review of the accounts payable listing. | Review the financial Institution's process of onboarding new vendors (how they are identified and reported to risk management, etc.) |
| 405 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Evolving | A formal program assigns responsibility for ongoing oversight of third- party access. | A Vendor Management Policy may assign specific responsibility to manage and/or provide ongoing oversight of third-party access to the financial institution's network | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management and determine if responsibility is assigned to manage and/or provide oversight of Third-Party access to the financial institution's network. |
| 406 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Evolving | Monitoring of third parties is scaled, in terms of depth and frequency, according to the risk of the third parties. | Ongoing review of vendors occurs on a flow basis, based upon risk, to ensure all vendors obtain ongoing periodic due diligence reviews. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management regarding continual oversight of vendors. If practical, request a demo of Third-Party Service Provider Management software and review output reports from the program. |
| 407 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Evolving | Automated reminders or ticklers are in place to identify when required third-party information needs to be obtained or analyzed. | A process is in place to notify management when due diligence monitoring items (e.g., financial statements, audit reports, contract expiration dates) are due for review. | Discuss with management the financial Institution's process to notify management when due diligence monitoring items (e.g. financial statements, audit reports, contract expiration dates) are due for review. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 408 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Intermediate | Third-party employee access to the institution's confidential data are tracked actively based on the principles of least privilege. | For smaller institutions, a port is generally opened on the firewall to allow access. Upon the vendor's completion of their work, the port is then closed. In effect, this provides the active tracking of access. For larger institutions, log data is generally produced and reviewed periodically for appropriateness. Some large institutions have also implemented an automated log aggregation and alerting tool (known as a SIEM). | Determine institution's process to allow access by third parties into the FI network (discussion, policy, demonstration). For large institutions, review sampling of logs showing access. IT staff should be able to explain the log data. |
| 409 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Intermediate | Periodic on-site assessments of high-risk vendors are conducted to ensure appropriate security controls are in place. | High-risk vendors may necessitate a more frequent and detailed level of due diligence of their physical and data center security environment. This is especially true if audit activity appears to be infrequent, superficial, or otherwise inadequate. | Review reports of on-site assessments of Third-Party service provider security controls. |
| 410 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Advanced | Third-party employee access to confidential data on third-party hosted systems is tracked actively via automated reports and alerts. | The vendor is able to provide access reports (logs, management summaries, etc.) to provide assurance of appropriate access to client data on the vendor systems. | Request and review a sampling of vendor access reports (logs, management summaries, etc.) to provide assurance of appropriate access to client data on the vendor systems. |
| 411 | 4: External Dependency Management | 2: Relationship Management | 3: Ongoing Monitoring | Innovative | The institution is leading efforts to develop new auditable processes for ongoing monitoring of cybersecurity risks posed by third parties. | Techniques may include limiting access to an as needed basis and/or for maintenance purposes and auditing of all third-party access credentials. Technology solutions include use of VPNs, multifactor authentication, geolocation, time, IP, and device restrictions. | If practical, request a demonstration by IT staff on their process for access restrictions and controls. |
| 412 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Baseline | The institution has documented how it will react and respond to cyber incidents. | Financial institution management should develop an incident response plan that properly integrates into the BCP. A key element of incident response involves assigning responsibility for evaluating, responding, and managing security incidents and developing procedures for employees to follow for escalating and reporting incidents. The ultimate goal should be to minimize damage to the financial institution and its customers by containing the incident and properly restoring information systems. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Business Continuity Planning (BCP) and Disaster Recovery (DR) to determine if the financial Institution has a business continuity plan that provides for the recovery of critical systems after a Cyber incident. |
| 413 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Baseline | Communication channels exist to provide employees a means for reporting information security events in a timely manner. | A financial institution's policies and procedures should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the financial institution, and system owners. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution's incident response plan specifies which incidents must be reported, when they must be reported, and to whom. |
| 414 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Baseline | Roles and responsibilities for incident response team members are defined. | Policies and procedures often exist 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. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institutions has defined roles and responsibilities for incident response team members. |
| 415 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Baseline | The response team includes individuals with a wide range of backgrounds and expertise, from many different areas within the institution (e.g., management, legal, public relations, as well as information technology). | Incident response can involve a wide range of responses such as customer notification, media communications, and incident containment and eradication. | Review the resumes of incident response team members to determine their level of skill and expertise in relation to the roles and responsibilities.<br><br>Discuss with management the incident response team members and their backgrounds and expertise. |
| 416 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Baseline | A formal backup and recovery plan exists for all critical business lines. | A formal backup and recovery plan describes how critical systems are backed up and restored in the event of loss or corruption of production data. Critical systems' data is typically backed up at least daily, and recovery from backups should be periodically tested to ensure the backup process is functioning properly. Business unit staff should test data after it is recovered for usability. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Business Continuity Planning (BCP) and Disaster Recovery (DR) to determine if a formal backup and recovery plan exists for the financial Institution's critical business lines listed in the business impact analysis. |
| 417 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Baseline | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | The financial institution should have a board-approved business continuity, disaster recovery, and data backup program to recover operations following an incident. The BCP should address:<br>1) Business impact analysis and risk assessment;<br>2) Alternate processing for critical business functions while systems/applications and facilities are unavailable;<br>3) Recovery strategies and procedures for critical systems/applications;<br>4) Roles and responsibilities; and<br>5) BCP and disaster recovery testing. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Disaster Recovery and Business Continuity to determine if the financial Institution has implemented a business continuity, disaster recovery, and data backup program to recover operations following an incident.<br><br>Review the business impact analysis (BIA) and verify it is updated at least annually. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 418 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Evolving | The remediation plan and process outlines the mitigating actions, resources, and time parameters. | According to NIST 800-61r2, containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack. Organizations should create separate containment strategies for each major incident type. Clearly documenting criteria can facilitate decision-making. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Disaster Recovery (DR) and Business Continuity Planning (BCP) to determine if the financial Institution has detailed remediation plans for each major incident type. |
| 419 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Evolving | The corporate disaster recovery, business continuity, and crisis management plans have integrated consideration of cyber incidents. | Cyber incidents can impact business continuity by interrupting critical services, destroying data, or disrupting communications. As a result, the impact of cyber incidents should be addressed in BCP. Crisis management plans may also need to be enacted to contain and control incidents and properly manage public communications. | Discuss with management how the financial Institution's recovery plans are integrated and address cyber incidents that may disrupt critical services. |
| 420 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Evolving | Alternative processes have been established to continue critical activity within a reasonable time period. | Financial institutions typically identify acceptable downtimes by establishing RTOs for each critical business function. Ideally, recovery time objectives are derived from a business impact analysis or similar method to estimate the dollar cost of downtime over various timeframes (e.g., short, medium, and longer term). In the event that critical activities cannot be recovered within defined RTO, the financial institution should have in place alternative processes for resumption of critical activities. | Review the Business Continuity Test results to determine if alternative processing for all critical systems are tested and comply with the requirements in the Business Impact Analysis. |
| 421 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Evolving | Business impact analyses have been updated to include cybersecurity. | A BIA should describe the relative impact of various types of cyber-threats on the financial institution's business activities. The BIA should assess the consequences of disruption of a business function as the result of cyber incidents such as malware, insider threats, data/systems corruption or destruction, and data communication infrastructure disruption | Review the Financial Institution's Policy, Standards and Guidelines specific to: Business Continuity Planning (BCP) and Disaster Recovery (DR) discuss with management how cybersecurity is incorporated into business impact analysis. |
| 422 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Evolving | Due diligence has been performed on technical sources, consultants, or forensic service firms that could be called to assist the institution during or following an incident. | Both different expertise types and a rapid response may be necessary, depending on the severity of the incident. Therefore, institutions should consider vetting multiple response resources in their incident planning to have primary and backup resources available. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management, Incident Response and determine if it addresses due diligence for third-party service providers called to assist following incidents.<br><br>Discuss the third-party service provider due diligence performed on all critical vendors that assist the financial Institution during or following an incident. |
| 423 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Intermediate | A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack. | Internal stakeholders of a financial institution can include employees, managers, corporate leaders, and owners/stockholders. External stakeholders include customers, the media, regulators, and law enforcement. This also includes Customer Notification procedures under Gramm Leach Bliley Act (GLBA) guidance. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if there is a documented strategy in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack. |
| 424 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Intermediate | Plans are in place to re-route or substitute critical functions and/or services that may be affected by a successful attack on Internet-facing systems. | For example, the financial institution maintains excess capacity on its mobile banking channel to mitigate the impact of a DDoS attack to its online banking website. Or, the online banking website traffic can be readily re-routed to an alternative website to avoid the malicious traffic. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Business Continuity Planning (BCP) and Disaster Recovery (DR), Incident Response, Cyber Resilience to determine if they contain alternate processing or rerouting of critical services in the event of an attack on internet facing systems.<br><br>Discuss with management how critical functions and/or services would be re-routed or substituted if the financial Institution suffers a successful attack on Internet-facing systems. |
| 425 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Intermediate | A direct cooperative or contractual agreement(s) is in place with an incident response organization(s) or provider(s) to assist rapidly with mitigation efforts. | Incident response is a complex process and institutions may benefit from engaging with a managed security service provider (MSSP). When outsourcing components of the Incident Response function to MSSPs, the Outsourcing Technology Services Booklet of the FFIEC IT Handbook offers additional guidance for examiners. The incident response function should to be coordinated and clearly defined between the financial institution and MSSP. Notification and escalation requirements regarding incident response should be clearly documented and aligned between the financial institution and MSSP. The definition of a reportable event should be clear and unambiguous. | Discuss with management if the financial Institution has direct cooperative or contractual agreement(s) in place with a third-party service provider to assist with mitigation efforts following an incident. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 426 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Intermediate | Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan. | It is rarely enough to simply document a significant incident without analyzing what went wrong and what could have prevented it. This enables root cause analysis to determine whether controls or processes failed or were absent. Lesson learned analysis is a key element of continuous improvement in cybersecurity preparedness. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if incident response plans are updated as a result of lessons learned from incidents that occurred at the financial Institution and other organizations.<br><br>Review after action reports to determine if Incident information is analyzed and tracked. |
| 427 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Advanced | Methods for responding to and recovering from cyber incidents are tightly woven throughout the business units' disaster recovery, business continuity, and crisis management plans. | Each business unit has a different level of cyber incident risk exposure and potential impact to its operations. Therefore, each business unit should consider its unique cybersecurity risks and address those in the pertinent plans or programs that reside at the business unit level. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Disaster Recovery (DR), Business Continuity Planning (BCP) and Crisis Management and discuss with management the methodology for integrating incident response into each business unit's business continuity planning process. |
| 428 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Advanced | Multiple systems, programs, or processes are implemented into a comprehensive cyber resilience program to sustain, minimize, and recover operations from an array of potentially disruptive and destructive cyber incidents. | The financial institution has a dedicated and formalized cyber resilience program that adequately addresses currently known and potentially pertinent cyber threats or incident sources. The program includes technical and physical safeguards and controls as well as policy requirements. The cyber resilience program includes input and validation from the financial institution's technology experts, information security experts, risk management and the critical business units. | Review the Institution's policy, standards and guidelines specific to: Cyber Resilience, Incident Response and determine if the financial Institution has a formal cyber resilience program that covers the various types of attacks and how the financial Institution should react to them. |
| 429 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Advanced | A process is in place to continuously improve the resilience plan. | Resilience is comparable to other major business functions or risk management activities in that it is supported by a strategy, objectives, and tactical plans. Progress is benchmarked or measured over time towards achieving process improvement. Systems and processes should be periodically tested for their ability to be resilient and be able to recover from intrusions and attacks. Resiliency plans are integrated with risk management activities and system recovery strategies that are periodically re-evaluated. | Discuss with management the methodology for continuously improving the financial Institution's ability to respond and recover quickly from an attack or cyber incident. |
| 430 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Innovative | The incident response plan is designed to ensure recovery from disruption of services, assurance of data integrity, and recovery of lost or corrupted data following a cybersecurity incident. | An incident response plan should contain provisions for preparation, detection, containment, eradication, remediation and follow-up. At a minimum, each financial institution must have a response program for unauthorized access to customer information as required by Gramm Leach Bliley Act (GLBA). Specifically, the response program must contain provisions to:<br>• Identify what customer information has been compromised;<br>• Notify the applicable regulatory offices (primary supervisor and insurer);<br>• File a suspicious activity report if required or in situations where voluntary reporting is encouraged;<br>• Contain and control the incident;<br>• Monitor, freeze, or close affected accounts;<br>• Preserve records and other evidence; and<br>• Notify customers when warranted. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if it contains provisions for preparation, detection, containment, eradication, remediation and follow-up. |
| 431 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 1: Planning | Innovative | The incident response process includes detailed actions and rule- based triggers for automated response. | A combination of technologies such as the use of security information and event management (SIEM), endpoint security and intrusion detection tools can identify a pattern or sequence of activities, such as serial attempts associated with a domain user attempting to connect to a system across the network and take action. | Discuss with management the rule-based triggers that generate automated responses. |
| 432 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Baseline | Scenarios are used to improve incident detection and response. | Depending on the event, some or all of the elements of the security environment may change. Different people may be involved in operations, at different physical locations, using similar but different machines and software which may communicate over different communications lines. Understanding the possible scenarios improves the response. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and verify the financial Institution uses scenarios in incident response exercises and updates the incident response plan as result. |
| 433 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Baseline | Business continuity testing involves collaboration with critical third parties. | A financial institution's management should ensure the institution is an active participant in its TSPs' testing programs and that the TSPs have a testing strategy that includes testing for significant disruptive events. The testing program should be based on a financial institution's established recovery priorities for critical systems and business processes as well as specific threat scenarios. | Review the business continuity plan test results and verify the collaboration between the financial Institution and its key service provides is documented in the financial Institution's test results. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 434 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Baseline | Systems, applications, and data recovery is tested at least annually. | The typical expectation is to test recovery of critical systems at least once per year. All systems need not be tested simultaneously, but a comprehensive rotation of testing coverage should be followed. Additionally, business units should evaluate the usability of the recovered data. | Review the business continuity plan test results and determine that the recovery of critical systems listed in the business impact analysis is included in the annual testing of the financial institution's systems, applications and data |
| 435 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Evolving | Recovery scenarios include plans to recover from data destruction and impacts to data integrity, data loss, and system and data availability. | A cyber-attack may simultaneously target production data and online backups for destruction or corruption. It may also target the destruction of hardware. Data destruction occurs when data are erased or rendered unusable. Data corruption occurs when data are altered without authorization. | Review the business continuity plan test results and verify the recovery from cyber-attacks which destroys data, systems and data availability is tested. |
| 436 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Evolving | Widely reported events are used to evaluate and improve the institution's response. | Examples of widely reported events include large scale retail data breaches, large scale financial institution breaches, DDoS attacks targeting the financial industry, data destructive attacks, and cryptographic malware such as Crypto Locker or Crypto Wall. | Discuss with management how lessons learned from actual data breaches throughout the financial industry are used to improve the financial Institutions incident response plan. |
| 437 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Evolving | Information backups are tested periodically to verify they are accessible and readable. | Backup media can degrade over time and backup processes or routines can fail due to human or technical errors. Therefore, there should be a process to restore and test backups. Backup equipment and media should not be used past any defined end of life horizons. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Data Backup to determine if the financial institution has a process for periodically testing information backups.<br><br>Review the results of backup tests to determine if they were been tested for accessibility. |
| 438 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Intermediate | Cyber-attack scenarios are analyzed to determine potential impact to critical business processes. | Scenarios to consider include cyber events demonstrating the financial institution's and third-party provider's ability to respond quickly and efficiently to such an event. For example, a financial institution's ability to recover from a disruption of critical functions because of a distributed denial of service (DDoS) attack or the ability to recover from a data corruption event should be subject to testing. A financial institution may consider working with an outside party, such as other financial institutions or an industry group, to test these types of events. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if various cyber attack scenarios are documented and analyzed for impact. |
| 439 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Intermediate | The institution participates in sector-specific cyber exercises or scenarios (e.g., FS-ISAC Cyber Attack (against) Payment Processors (CAPP)). | Opportunities to participate on cyber exercises are offered on a voluntary basis with the objective of a high level of participation from institutions. Sources of sector-wide exercises include public-private partnerships (i.e., FBIIC, FS-ISAC and FSSCC). | Discuss with management the financial Institutions participation in sector-specific cyber exercises or scenarios [e.g., FS-ISAC Cyber Attack (against) Payment Processors (CAPP)]. |
| 440 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Intermediate | Resilience testing is based on analysis and identification of realistic and highly likely threats as well as new and emerging threats facing the institution. | Monitoring of new and emerging threats typically includes active multi-source threat intelligence analysis and awareness of geopolitical events or threats. | Discuss with management if the financial Institution has a process is in-place to monitor new and emerging threats using active multi-source threat intelligence. |
| 441 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Intermediate | The critical online systems and processes are tested to withstand stresses for extended periods (e.g., DDoS). | Cyber-attack campaigns may occur over extended periods of time, whether continuous or sporadic. Ongoing campaigns may also affect an increasing number of financial institutions serviced by the same service provider. This can pose increased risk of service outages due to capacity limitations of the service provider. | Review the business continuity plan test results and determine if the critical systems listed in the business impact analysis are tested to determine if they can be run from the backup and recovery site for an extended period of time. |
| 442 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Intermediate | The results of cyber event exercises are used to improve the incident response plan and automated triggers. | Automated triggers may result in an alert or action taken (e.g., an IPS blocking traffic from a suspicious IP address). Triggers may include changes to administrator accounts, database access, lateral network movement outside of normal baseline activity, and remote connections or logons. | Review the after-action report for lessons learned and determine if the incident response plan is updated as a result. |
| 443 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Advanced | Resilience testing is comprehensive and coordinated across all critical business functions. | Business line management should have ownership and accountability for testing continuity of business operations, including applications and processes. While business line management has overall responsibility for testing their business processes and related interdependencies, they should coordinate with the enterprise-wide BCP testing function and support areas, such as IT and facilities management. The critical business functions should be identified in the BIA. | Discuss with management the methodology for developing and coordinating cyber resilience testing across business units. |
| 444 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Advanced | The institution validates that it is able to recover from cyber events similar to by known sophisticated attacks at other organizations. | Validation can be viewed as falling under testing of key controls that should be conducted by a qualified, independent reviewer (e.g., internal and/or third-party audit). | Review results of independent audits of the financial institution's business continuity program to determine if the financial Institution has identified any gaps in their existing defenses. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 445 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Advanced | Incident response testing evaluates the institution from an attacker's perspective to determine how the institution or its assets at critical third parties may be targeted. | Considering the attacker's perspective can be performed in conjunction with the development of threat profiles. According to SANs Institute, threat profiles will provide incident management teams with threat intelligence information that they can use to analyze individual threat scenarios or threat scenario campaigns and enable them to anticipate and mitigate future attacks based on this detailed knowledge about the threats. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution incorporates attacker perspectives in its incident response testing. |
| 446 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Advanced | The institution corrects root causes for problems discovered during cybersecurity resilience testing. | Root cause analysis involves identifying the underlying reason(s) why processes failed. Root causes should be identified and tracked through remediation to facilitate continuous improvement in business resilience. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution has a documented process implemented to identify and track root causes from identification through remediation. |
| 447 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Advanced | Cybersecurity incident scenarios involving significant financial loss are used to stress test the institution's risk management. | Cyber incidents can potentially cause significant financial loss due to business interruptions, reputational damage, data breaches, theft of corporate or customer funds, and compromise of strategic plans or other critical intellectual property.<br><br>An effective stress testing framework provides a comprehensive, integrated, and forward looking set of activities for a financial institution to employ along with other practices to assist in the identification and measurement of its material risks and vulnerabilities. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if cybersecurity incident scenarios include anticipated financial loss. |
| 448 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Innovative | The institution tests the ability to shift business processes or functions between different processing centers or technology systems for cyber incidents without interruption to business or loss of productivity or data. | Testing should demonstrate not only the ability to failover to a secondary site but also the ability to restore normal operations. High availability refers to business continuity capability very near to 100%. Either failover or high availability may be sufficient depending on business requirements. An organization should have their critical services/processes (as determined by the business impact analysis) returned to 100% to have an effective testing process. | Review business continuity test results to determine if the financial Institution has the ability to failover to a secondary site and the ability to restore critical services/processes as determined by the business impact analysis. |
| 449 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Innovative | The institution has validated that it is able to remediate systems damaged by zero-day attacks to maintain current recovery time objectives. | Validation could include a risk assessment to identify susceptible systems and development of an incident response protocol and/or playbook for remediation of zero-day attacks. Testing can consist of real-life incidents as well as tabletop exercises of potential incidents. | Discuss with management methods or activities used to validate the financial Institution's ability to remediate systems damaged by zero-day attacks to maintain current recovery time objectives. |
| 450 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Innovative | The institution is leading the development of more realistic test environments. | The development environment may not scale to and therefore fully reflect the complexities (e.g., interconnectivity, interoperability, data flows) of the production environment. | Discuss with management if the incident response team explores different test environments to mirror its production environment process. |
| 451 | 5: Cyber Incident Management and Resilience | 1: Incident Resilience Planning and Strategy | 2: Testing | Innovative | Cyber incident scenarios are used to stress test potential financial losses across the sector. | A financial institution may provide services or support applications and/or system connections that have the potential to materially impact other institutions systems. | Discuss with management how the financial Institution uses or participates in Cyber incident scenarios to stress test potential financial losses across the sector. |
| 452 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Baseline | Alert parameters are set for detecting information security incidents that prompt mitigating actions. | Monitoring systems (firewall, intrusion detection system, intrusion prevention system, security information and event management and data loss prevention) should be set to alert or perform and/or prevent specified actions. For example, DLP should detect and take pre-defined actions on sensitive data being transmitted external to the financial institution. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution defines the alert parameters for detecting information security incidents that require mitigating actions. |
| 453 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Baseline | System performance reports contain information that can be used as a risk indicator to detect information security incidents. | The financial institution's system performance reports should include risk indicators to detect possible information security incidents. Types of reports used may include system and network log files, network message traffic, user files, results produced by intrusion detection tools, and system administrator console logs. | Review the available system performance reports and determine whether they contain or identify risk indicators to detect security incidents.<br><br>Discuss with management the methodology for developing cybersecurity risk indicators. |
| 454 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Baseline | Tools and processes are in place to detect, alert, and trigger the incident response program. | The financial institution may use active and or passive monitoring tools that will generate an alert when it detects any deviation from normal or expected operation. The security team based on their analysis of the alert may invoke the incident response program.<br><br>Active monitoring tools poll key configuration items to determine their status and availability. Passive monitoring tools detect and correlate operational alerts generated by configuration items. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution has a documented process for detecting, alerting and triggering the incident response program.<br><br>Discuss with management or demonstrate the tools in place to detect, alert and trigger the incident response program. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 455 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Evolving | The institution has processes to detect and alert the incident response team when potential insider activity manifests that could lead to data theft or destruction. | An insider can have levels of authorization that increase their ability to access a financial institution's internal systems and resources. A financial institution's processes should help detect and alert the incident response team of potential insider activity that may manifest into a security violation. Incidents that may relate to insider threat activity include:<br>• Failed log-in attempts;<br>• Transfers of large amounts of data;<br>• Altered coding on sensitive files; and<br>• Personnel issues such as unfriendly terminations.<br><br>The financial institution may use network-monitoring software and implement reporting mechanisms for employees and supervisors to report suspicious activity. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution has a documented process for detecting potential insider activity manifests that could lead to data theft or destruction. |
| 456 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Intermediate | The incident response program is triggered when anomalous behaviors and attack patterns or signatures are detected. | The financial institution uses network-monitoring software to detect internal and external cyber threats. To determine what kinds of patterns are anomalous and therefore potentially suspicious, institutions should establish a network activity baseline.<br><br>After the baseline is established and the monitoring software is implemented, designated personnel should monitor the network for anomalous activity, such as unfamiliar IP addresses attempting to access the network, unusually large data transfers, failed login attempts, and large printing jobs or data transfers of privileged files.<br><br>When anomalous activity is identified, personnel should first investigate to see whether a legitimate explanation for the activity exists (e.g., forgotten passwords or training activities requiring printing of privileged materials). If no legitimate explanation is uncovered, the appropriate security personnel should determine whether the incident response program needs to be invoked. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if there is a process in place to detect anomalous activity, such as unfamiliar IP addresses attempting to access the network, unusually large data transfers, failed login attempts, and large printing jobs or data transfers of privileged files.<br><br>Discuss with management the actions taken when the incident response program is triggered due to anomalous behaviors and attack patterns or signatures being detected. |
| 457 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Intermediate | The institution has the ability to discover infiltration, before the attacker traverses across systems, establishes a foothold, steals information, or causes damage to data and systems. | Detection solutions and logging are utilized to identify and alert to unauthorized activity. Once alerts occur the logs for the affected servers or systems can be reviewed to identify locations of access and remediation steps taken to close access or remove unauthorized applications (malware). | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if there is a process in place to detect anomalous activity. |
| 458 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Intermediate | Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond. | Monitoring solutions send alerts to designated incident response staff through SMS (text) or email when alerts are triggered. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if there is a process in place to detect anomalous activity in real-time.<br><br>Review a sample of automated alerts notifying personnel of security incidents. |
| 459 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Intermediate | Network and system alerts are correlated across business units to better detect and prevent multifaceted attacks (e.g., simultaneous DDoS attack and account takeover). | System logs and events can be correlated across business units by using technologies such as security Information and event management (SIEM) tools. A SIEM can collect logs from a variety of systems and correlate data to determine if a single or multiple event is active based on the alerting. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution has the capability to correlate alerts to determine if multifaceted attacks (e.g., simultaneous DDoS attack and account takeover) occurred. |
| 460 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Intermediate | Incident detection processes are capable of correlating events across the enterprise. | The incident detection process includes human intelligence, as well as the use of intelligent monitoring systems that perform event correlation for internal and external security events and analysis that includes spending the time to research false positives and building a database of events for comparison and correlation. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution has the capability to correlate alerts to determine if multifaceted attacks (e.g., simultaneous DDoS attack and account takeover) occurred. |
| 461 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Advanced | Sophisticated and adaptive technologies are deployed that can detect and alert the incident response team of specific tasks when threat indicators across the enterprise indicate potential external and internal threats. | Monitoring and alerting systems can use adaptive processes that identify when network behavior is suspicious based on previously identified behavior. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution has the capability to correlate alerts to determine if multifaceted attacks (e.g., simultaneous DDoS attack and account takeover) occurred. |
| 462 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Advanced | Automated tools are implemented to provide specialized security monitoring based on the risk of the assets to detect and alert incident response teams in real time. | Accurately assessing threats and identifying vulnerabilities is critical to understanding the risk to assets. For example, an intrusion detection systems (IDS) can be positioned in front of critical assets to detect and alert personnel of anomalous network activity to or from the assets. | Review the results of the vulnerability scanner run on the internal and external networks based on the management's risk analysis. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 463 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 1: Detection | Innovative | The institution is able to detect and block zero-day attempts and inform management and the incident response team in real time. | The financial institution has an effective process that can detect and block zero-day attempts and inform management and the incident response team in real-time.<br><br>A zero-day vulnerability is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. A zero-day exploit leaves no opportunity for detection at first. Attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability. | Discuss with management if the financial Institution has a process implemented that can detect and block zero-day attempts and inform management and the incident response team in real-time. |
| 464 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Baseline | Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information. | The incident response plan should include procedures to contain and control an incident. At a minimum, the procedures should include steps that identify and isolate the compromised systems, search for additional compromised systems and collect and preserve the compromised information. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to verify it identifies each phase of the process which includes Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.<br><br>Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if it identifies the Computer Incident Response Team (CIRT) members. |
| 465 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Evolving | The incident response plan is designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities. | The incident response plan should be reviewed to determine if it includes appropriate steps for assessing the root cause of the incident, and whether it includes appropriate guidance for performing analysis and for determining management's actions and operational steps that would minimize the relative impact of the incident on the financial institution's systems, information, and business. The incident response plan and measures should detail specific objectives for recovery of the affected systems with minimum service disruption on customers and the business. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution has a process implemented to prioritize incidents based on the relevant factors, such as the functional impact of the incident (e.g., current and likely future negative impact to business functions), the information impact of the incident (e.g., effect on the confidentiality, integrity, and availability of the organization's information), and the recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident). |
| 466 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Evolving | A process is in place to help contain incidents and restore operations with minimal service disruption. | Processes should identify and contain incidents that might impact the financial institution's systems, eradicate malware from the affected systems, and restore the compromised systems to an operational and secure state. The primary purpose of the containment phase is to limit and prevent further damage. The eradication phase deals with the actual removal of the malware and restoration of the affected systems. The systems restoration phase addresses recovery of any affected systems or services within BCP RTOs. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution has a process implemented to define acceptable risks in containing incidents.<br><br>Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution has containment strategies based on the type of incident. |
| 467 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Evolving | Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware). | The financial institution's incident response plan identifies containment and mitigation strategies for various types of incidents that might impact the financial institution's systems and/or information. Types of incidents might include: unauthorized access to systems and information, denial of services, malicious code injections, unauthorized use of system resources, unauthorized system scans and attempted access, ransomware, social engineering attempts and spear phishing. Containment strategies vary based on the type of incident. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution's incident response plan identifies containment and mitigation strategies for various incident types, like unauthorized access, denial of service, malicious code, improper usage, scans/probes and attempted access. |
| 468 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Evolving | Procedures include containment strategies and notifying potentially impacted third parties. | In addition to implementing containment strategy, the incident response procedures should address how and when third-party vendors are notified, if the compromise affects their systems. For example, the Federal Reserve Board (FRB) Operating Circular #5 requires notification of the FRB in the event a Fedline system is affected. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the financial Institution's incident response plan includes detailed containment strategies and describe the process of notifying potentially impacted third parties and there sub-contractors. |
| 469 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Evolving | Processes are in place to trigger the incident response program when an incident occurs at a third party. | The financial institution's incident response program should address notification and communication with third-parties, regarding incidents at the third-party that might impact the financial institution. The processes should also address how the financial institution handles incidents at "fourth-party vendors", as well. Fourth-party vendors are vendors used by the financial institution's third-party vendor. Once it is determined that the incident impacts the financial institution's systems, information, and operations, an agreed-upon protocol should be established between the financial institution and the third-party for communicating and determining how the incident will be contained and recovery measures implemented. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Third-Party Service Provider Management and Incident Response and discuss with management the process managing incidents that occur at Third-Party service providers. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 470 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Evolving | Records are generated to support incident investigation and mitigation. | Where feasible, every step taken, from the time the incident was detected to its final resolution, should be documented and timestamped. Recording the steps performed can also lead to more efficient, systematic, and less error-prone forensic and recovery efforts.<br><br>Records often contain sensitive information regarding such things as vulnerabilities, security breaches, and users that may have performed inappropriate actions. An incident response team or designated personnel should ensure that access to incident data is restricted properly, both logically and physically.<br><br>Records of incidents, whether electronic logs or other records, cannot be altered or otherwise manipulated. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution generates records to support incident investigations and mitigation. |
| 471 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Evolving | The institution calls upon third parties, as needed, to provide mitigation services | The incident response program should identify the use of third-party security experts when handling an incident. This is needed if the financial institution's incident response team does not have people with a certain set of skills and technical expertise, and with abilities that enable them to respond to incidents, perform analysis tasks, and communicate effectively with customers and other external contacts, including law enforcement. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution identifies third party service providers who will assist in the incident response process. |
| 472 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Evolving | Analysis of events is used to improve the institution's security measures and policies. | One of the most important parts of incident response is also the most often omitted: learning and improving. Holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself.<br><br>Another important post-incident activity is creating a follow-up report for each incident, which can be quite valuable for future use. The report provides a reference that can be used to assist in handling similar incidents. Creating a formal chronology of events (including timestamped information such as log data from systems) is important, as is creating a monetary estimate of the amount of damage the incident caused. Follow-up reports should be kept for a period as specified in record retention policies. | Discuss with management how the analysis of events are used to improve the financial Institution's security measures and policies.<br><br>Review after-action reports for incident response plan and process recommendations following simulated and actual events. |
| 473 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Intermediate | Analysis of security incidents is performed in the early stages of an intrusion to minimize the impact of the incident. | The incident response team should operate with the authority to collect information and subsequently inform the business of changes that should occur to further secure the financial institution. The incident response team should escalate the more significant issues that require major changes in systems and business practices to senior management to request the necessary resources to support corrective action. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response.<br><br>Review a sampling of Incident Reports (Including After-Action Report). |
| 474 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Intermediate | Any changes to systems/applications or to access entitlements necessary for incident management are reviewed by management for formal approval before implementation. | An Emergency Change Control process may ensure that all changes requested by the incident response team are formally reviewed, approved and made in an expedited manner. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response, Change Management and discuss with management the process for requesting and approving changes necessary for incident management are reviewed and approved before implementation. |
| 475 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Intermediate | Processes are in place to ensure assets affected by a security incident that cannot be returned to operational status are quarantined, removed, disposed of, and/or replaced. | The incident response plan should follow an Incident Response Life Cycle (Containment, Eradication, and Recovery). Procedures should be developed for each life cycle stage. If the recovery procedures identify an asset that cannot be returned to production, Data Classification and Handling procedures may address retiring the asset from production. | Review the Financial Institution's Policy, Standards Guidelines specific to: Incident Response and Data Classification and Handling to ensure they address containment, eradication, and recovery of affected assets and possibly retirement of an affected asset from production. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 476 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Intermediate | Processes are in place to ensure that restored assets are appropriately reconfigured and thoroughly tested before being placed back into operation. | The financial institution has procedures in place to restore system functionality once the infected devices have been restored or replaced. Procedures should also address when the temporary containment or restrictive security measures will be terminated. In all cases, the devices or operating system should be restored so that they are no longer vulnerable to the malware threat. The procedures should address restoration of single or few devices as well as the rebuilding of a large number of the financial institution's IT devices and systems.<br><br>Business continuity testing should be aligned with the incident response processes. Business units should perform the validation function pursuant to operational use. However, even though the incident response team should assess the risks of restoring the service, management should ultimately be responsible for determining what should be done based on the incident response team's recommendations and management's understanding of the business impact of maintaining the containment measures. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Business Continuity to determine the financial Institution has processes in place that require testing and validation of assets before deploying into production after an incident. |
| 477 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Advanced | The incident management function collaborates effectively with the cyber threat intelligence function during an incident. | The financial institution may have an Incident Management and Cyber Threat Intelligence department. The two departments may also be one department but the information they handle varies and must be coordinated.<br><br>Incident Management department deals with "raw information" and the Cyber Threat Intelligence department deals with "intelligence information." "Raw information" differs from "intelligence information" as follows:<br>• Raw Information is raw unfiltered feed; unevaluated when delivered; aggregated from virtually every source; maybe true, false, misleading, incomplete, relevant or irrelevant; and is not actionable; and<br>• Cyber Threat Intelligence is information that is processed and sorted; evaluated and interpreted by trained intelligence analysts; aggregated from reliable sources and cross correlated for accuracy; accurate; timely; complete (as possible); assessed for relevancy and is actionable. | Discuss with management the collaboration between the Incident response team and any cyber threat capabilities at the financial Institution. |
| 478 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Advanced | Links between threat intelligence, network operations, and incident response allow for proactive response to potential incidents. | To enhance incident response actions and bolster cyber defenses, institutions should harness the collective wisdom of incident response functions within the financial institution and the collective wisdom of peer organizations through information sharing and coordinated incident response.<br><br>Organizations should acquire cyber threat intelligence from both internal and external sources and use it to disrupt the adversary's cyber-attack life cycle. | Discuss with management the collaboration between the Incident response team and the threat intelligence and network operations capabilities at the financial Institution. |
| 479 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Advanced | Technical measures apply defense-in-depth techniques such as deep- packet inspection and black holing for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns and/or DDoS attacks. | The financial institution follows a defense-in-depth strategy. "Defense-in-Depth" relies on the intelligent application of techniques and technologies and overlay of controls. Defense-in-depth methodologies and techniques might include:<br>• Implementation of firewalls and intrusion detection/prevention systems at various layers of the network, as well as implementation of firewalls that inspect network traffic and data packets, and intrusion detection systems (IDS)/intrusion prevention systems (IPS) that block unwanted traffic and detect intrusion attempts and data traffic anomalies.<br>• Re-routing of malicious or suspect data traffic to dead-end devices (i.e. black holing) for investigation, or dropping suspected malicious traffic and preventing it from entering the financial institution's network. | Discuss with management the financial Institution's defense-in-depth strategy and techniques for detecting network based attacks.<br><br>Review the network topology diagram(s) and discuss with management if the financial Institution has implemented defense mechanisms in layers across the financial Institution's network. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 480 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Innovative | The institution's risk management of significant cyber incidents results in limited to no disruptions to critical services. | Financial Institutions should have the people, processes and technology in place to safeguard critical assets and services. Business continuity and disaster recovery plans should address significant cyber events and not just business disruptions caused by system failures and natural disasters. . By correlating intelligence on cyber events and institution can quickly detect and remediate a potential issue before it spreads, resulting in reduced damage and cost. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Cyber Resilience, Business Continuity to determine if the financial Institution has implemented a process to correlate information or intelligence on cyber incidents.<br><br>Discuss with management how information or intelligence is used to build a cyber resilience strategy that allows the financial Institution to quickly prepare, protect, and respond to significant cyber attacks. |
| 481 | 5: Cyber Incident Management and Resilience | 2: Detection, Response, and Mitigation | 2: Response and Mitigation | Innovative | The technology infrastructure has been engineered to limit the effects of a cyber attack on the production environment from migrating to the backup environment (e.g., air-gapped environment and processes). | Isolating backup environments used to recover data adds a layer of protection in preventing and recovering from cyber-attacks. The network architecture may use an air-gapped environment to isolate the production and backup environment. Air gapping is a security measure that involves isolating a computer or network and preventing it from establishing an external connection. An air-gapped computer is physically segregated and incapable of connecting wirelessly or physically with other computers or network devices. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security and network topology diagram(s) to determine the financial Institution's strategy for network segmentation.<br><br>Discuss with management what controls or measures are in place to prevent the propagation of cyber attacks from spreading from production to the backup environment. |
| 482 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Baseline | A process exists to contact personnel who are responsible for analyzing and responding to an incident. | The goal of incident response is to minimize damage to the financial institution and its customers. The financial 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 enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the financial institution. The program plan should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the financial institution, and system owners. | Review the Institution's policy, standards and guidelines specific to: Incident Response and determine if the financial Institution defines the Incident Response Team roles and responsibilities and include triggers to notify contact personnel to respond to an incident. |
| 483 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Baseline | Procedures exist to notify customers, regulators, and law enforcement as required or necessary when the institution becomes aware of an incident involving the unauthorized access to or use of sensitive customer information. | An incident response plan should contain provisions for preparation, detection, containment, eradication, remediation and follow-up. Each institution should have a response program to address incidents of unauthorized access to customer information under Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Response program components:<br>• Identify what customer information or systems have been compromised;<br>• Notify the primary regulator of incidents involving sensitive customer information;<br>• Notify law enforcement and file a suspicious activity report if required;<br>• Take appropriate steps to contain and control the incident; and<br>• Notify customers when warranted. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if it complies with Gramm-Leach-Bliley Act [Gramm Leach Bliley Act (GLBA)] guidelines. |
| 484 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Baseline | The institution prepares an annual report of security incidents or violations for the board or an appropriate board committee. | The board should receive annual reports on the overall status of the financial institution's information security program, as well as the financial institution's compliance with the GLBA guidelines for safeguarding customer information. External incident sources also should be part of an ongoing reporting process. | Review the Annual Security Report to the board of directors to determine if the institution prepares an annual report of security incidents or violations. |
| 485 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Baseline | Incidents are classified, logged, and tracked. | Incidents should be classified based upon common attack vectors and be used as a basis for defining more specific handling procedures. An issue tracking system should be in place for tracking incident information including remediation. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial Institution has a process or procedures for the management of incidents to include classification, logging and tracking.<br><br>Review the incident reports to verify incidents are classified and logged into a database. |
| 486 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Evolving | Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk. | Establishing objective criteria ensures that the board and senior management is apprised of material cyber incidents. For example, a severity rating system such as 1-5, Low-Medium-High, or Mild-Moderate-Catastrophic. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if there are documented processes for escalating cyber incidents or vulnerabilities to the board and senior management based on criticality of the risk.<br><br>Discuss with management the methodology for assigning a criticality of risk to cyber incidents and vulnerabilities. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 487 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Evolving | Regulators, law enforcement, and service providers, as appropriate, are notified when the institution is aware of any unauthorized access to systems or a cyber incident occurs that could result in degradation of services. | The incident response program includes incident reporting procedures that ensure the financial institution promptly reports incident information to appropriate authorities and service providers, if appropriate.<br><br>The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if the financial institution has a process to promptly report incident information to appropriate authorities and service providers, if appropriate. |
| 488 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Evolving | Tracked cyber incidents are correlated for trend analysis and reporting. | Reviewing cyber incident information collectively provides a more complete picture of the incident and assists in answering the "who, what, when, where, and why's" of an attack. Security events should be analyzed from as many sources as possible to evaluate threats and formulate appropriate responses. Incident data can help highlight trends in the evolving attack landscape and possibly help associate a pattern of attacks with a larger "campaign" – e.g., a broad effort by a crime syndicate to acquire data that could be used to perpetuate financial fraud. | Discuss with management the process for correlating cyber incidents for trend analysis. |
| 489 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Intermediate | Employees that are essential to mitigate the risk (e.g., fraud, business resilience) know their role in incident escalation. | Organizational structure, roles, responsibilities, and levels of authority should be defined. When responding to an incident, financial institutions need strategies to enhance communication, coordination and cooperation within each impacted business unit and across the enterprise. | Discuss with management how employees are educated and held accountable for knowing their role and responsibility in incident escalation. |
| 490 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Intermediate | A communication plan is used to notify other organizations, including third parties, of incidents that may affect them or their customers. | According to Ready.gov, understanding the audiences that a business needs to reach during an emergency is one of the first steps in the development of a crisis communications plan. There are many potential audiences that will want information during and following an incident and each has its own needs for information. The challenge is to identify potential audiences, determine their need for information and then identify who within the business is best able to communicate with that audience. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if it includes a communication strategy in the event of an incident.<br><br>Discuss with management the communication plan or strategy on how, when, and what to communicate outside of the financial Institution, whether to law enforcement, regulatory agencies, information-sharing organizations, customers, third-party service providers, potential victims, or others. |
| 491 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Intermediate | An external communication plan is used for notifying media regarding incidents when applicable. | The incident handling team should establish media communications procedures that comply with the financial institution's policies on media interaction and information disclosure. For discussing incidents with the media, organizations often find it beneficial to designate a single point of contact (POC) and at least one backup contact. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response to determine if it includes a communication strategy in the event of an incident.<br><br>Discuss with management the communication plan or strategy on how, when, and what to communicate outside of the financial Institution, whether to law enforcement, regulatory agencies, information-sharing organizations, customers, third-party service providers, potential victims, or others. |
| 492 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Advanced | The institution has established quantitative and qualitative metrics for the cybersecurity incident response process. | Quantitative examples include elapsed time from the beginning of the incident to incident discovery, to the initial impact assessment, and to each stage of the incident handling process (e.g., containment, recovery).<br><br>Qualitative assessment metrics can include asking incident response team members to assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked, to determine if the owner thinks the incident was handled efficiently and if the outcome was satisfactory. | Review the Financial Institution's Policy, Standards and Guidelines specific to: Incident Response and determine if the Incident Response Plan includes quantitative and qualitative metrics for the cybersecurity incident response process. |
| 493 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Advanced | Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the board meeting package. | Reporting items to consider include number of incidents handled, severity, time spent per incident, and estimated monetary damage from the incident (e.g., information and critical business processes negatively affected by the incident). | Review the Annual Security Report to the board of directors to determine the cybersecurity metrics on cyber incidents presented to the board or senior management. |
| 494 | 5: Cyber Incident Management and Resilience | 3: Escalation and Reporting | 1: Escalation and Reporting | Innovative | A mechanism is in place to provide instantaneous notification of incidents to management and essential employees through multiple communication channels with tracking and verification of receipt. | Mechanisms and channels can include phone numbers, secure email, online forms, and secure instant messaging systems that users can use to report suspected incidents. At least one mechanism should be in place to allow people to report incidents anonymously. | Discuss with management the mechanisms in place to provide instantaneous notification of incidents. |