Appendix A: Mapping Baseline Statements to FFIEC IT Examination Handbook

The purpose of this appendix is to demonstrate how the FFIEC Cybersecurity Assessment Tool declarative statements at the baseline maturity level correspond with the risk management and control expectations outlined in the *FFIEC Information Technology (IT) Examination Handbook*. The FFIEC will update this appendix to align with new or updated *FFIEC IT Examination Handbook booklets* following their release.

The mapping is by Domain, then by Assessment Factor and Category. Each statement is then sourced to its origin in an applicable *FFIEC IT Examination Handbook*. Refer to the last page of this appendix for the Source reference key.

Yes/No	FFIEC Cybersecurity Assessment Tool
Domain 1 – Cyber Risk Management and Oversight	
	Governance/Oversight: 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. *Source*: IS.I:pg3 The board, or designated board committee, should be responsible for overseeing tThe development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions. IS.I:pg4: The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program. IS.WP.2.3: Determine whether the board holds management accountable for the following: Central oversight and coordination, Assignment of responsibility, Support of the information security program, and Effectiveness of the information security program. MGT.III.C.3:pg28: The board of directors is responsible for overseeing the development, implementation, management, and maintenance of the institution's information security program. This oversight includes assigning specific responsibility and accountability for the program's implementation and reviewing reports from management. MGT.WP.2: Determine whether the board of directors oversees and senior management appropriately establishes an effective governance structure that includes oversight of IT activities. MGT.WP.2.2.g: Review whether the board or a committee of the board appropriately holds management accountable for the identification, measurement, and mitigation of IT risks.
	Governance/Oversight: Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. *Source*: IS.I.B:pg4: Management also should do the following: Participate in assessing the effect of security threats or incidents on the institution and its lines of business and processes. IS.III.A:pg47: Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Governance/Oversight: 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. *Source*: IS.I.B:pg4: The board, or designated board committee, should approve the institution's written information security program; affirm responsibilities for the development, implementation, and maintenance of the program; and review a report on the overall status of the program at least annually. Management should provide a report to the board at least annually that describes the overall status of the program and material matters related to the program, including the following … IS.WP.2.4: Determine whether the board approves a written information security program and receives a report on the effectiveness of the information security program at least annually. MGT.III.C.3(a):pg30: The board should also annually review a written report, prepared by management, regarding the financial institution's actions toward GLBA compliance. MGT.III.C.4:pg30: Management should also provide to the board on an annual basis a written report on the overall status of the business continuity program and the results of testing of the plan and backup systems. MGT.WP.12.7.f: Verify that the board is responsible for annually reviewing management's report on the status of the bank's actions to achieve or maintain compliance with the Information Security Standard. MGT.WP.12.9.a & c: Determine whether the board of directors approved policies and management established and implemented policies, procedures, and responsibilities for an enterprise-wide business continuity program, including the following: Annual review and approval of the business continuity program by the board of directors and annual reports by management of the results of the business continuity and disaster recovery tests to the board of directors.
	Governance/Oversight: The budgeting process includes information security related expenses and tools. *Source:* IS.I.C:pg5: Funding, along with technical and managerial talent, also contributes to the effectiveness of the information security program. Management should provide, and the board should oversee, adequate funding to develop, implement, and maintain a successful information security program. IS.WP.2.9: Determine whether the board provides adequate funding to develop and implement a successful information security function. MGT.I.B.6:pg14: Management should strive to achieve a planning process that constantly adjusts for new risks or opportunities and maximizes IT's value. MGT.I.B.6(c):pg17 When considering new IT projects, management should look at the entry costs of the technology and the post-implementation support costs. MGT.I.B.6(c):pg17: Some institutions budget IT as a separate department. A financial analysis of an IT department should include a comparison of the cost-effectiveness of the in-house operation versus contracting with a third-party provider. The analysis may also include a peer group comparison of operating costs and ratios. MGT.WP.4: Determine the adequacy of the institution's IT operations planning and investment. Assess the adequacy of the risk assessment and the overall alignment with the institution's business strategy, including planning for IT resources and budgeting.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Governance/Oversight: Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. *Source: BCP.B.J-12:* Cyber attacks may also be executed in conjunction with disruptive physical events and may affect multiple critical infrastructure sectors (e.g., the telecommunications and energy sectors). Financial institutions and TSPs should consider their susceptibility to simultaneous attacks in their business resilience planning, recovery, and testing strategies. *BCP.WP.10:* Determine whether the financial institution's and TSP's risk management strategies are designed to achieve resilience, such as the ability to effectively respond to wide-scale disruptions, including cyber attacks and attacks on multiple critical infrastructure sectors.
	Governance/Strategy-Policies: The institution has an information security strategy that integrates technology, policies, procedures, and training to mitigate risk. *Source:* IS.Introduction:pg2: Information security is far more effective when management does the following: Integrates processes, people, and technology to maintain a risk profile that is in accordance with the board's risk appetite. Aligns the information security program with the enterprise risk management program and identifies, measures, mitigates, and monitors risk. IS.WP.6.3: Determine whether the institution continually assesses the capability of technology needed to sustain an appropriate level of information security based on the size, complexity, and risk appetite of the institution. MGT.III.C.1:pg27: Senior management should ensure that policies, standards, and procedures are current, well documented, and integrated with the institution's information security strategy. MGT.WP.4.3: Determine whether the institution has adequate tactical and operational IT plans to support the larger IT strategic plans.
	Governance/Strategy-Policies: The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management. *Source:* IS.II:pg6: Management should develop and implement an information security program that does the following: Supports the institution's IT risk management (ITRM) process by identifying threats, measuring risk, defining information security requirements, and implementing controls. IS.WP.3.1: Determine whether the institution has an effective information security program that supports the ITRM process. MGT.III.C.1:pg27: Institution management should create, document, maintain, and adhere to policies, standards, and procedures to manage and control the institution's IT risk. The level of detail depends on the complexity of the IT environment but should enable management to monitor the identified risk posture. MGT.WP.12.4: Determine whether IT management has developed adequate policies, standards, and procedures to manage the risk from technology and that they are current, documented, and appropriately communicated.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Governance/Strategy-Policies: The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing. *Source:* IS.III.C:pg50: The sharing of attack data through organizations, such as FS-ISAC, also has the potential to benefit the industry at large by enabling other institutions to better assess and respond to current attacks. Management should consider whether to include such information sharing as a part of its strategy to protect the institution. MGT.III.A:pg22: Participation in an information-sharing forum, such as FS–ISAC, should be a component of the risk identification process because sharing information may help the institution identify and evaluate relevant cybersecurity threats and vulnerabilities. MGT.WP.10.1.b: Determine whether management participates in an information sharing forum (such as FS-ISAC).
	Governance/Strategy-Policies: The institution has board-approved policies commensurate with its risk and complexity that address information security. *Source:* IS.I:pg4: Management also should do the following: Implement the board-approved information security program. Establish appropriate policies, standards, and procedures to support the information security program. IS.Wp.6.2: Determine whether the information security policy is annually reviewed and approved by the board.
	Governance/Strategy-Policies: The institution has policies commensurate with its risk and complexity that address the concepts of external dependency or third-party management. *Source:* OT.B.2: Financial institutions should have a comprehensive outsourcing risk management process to govern their TSP relationships.
	Governance/Strategy-Policies: The institution has policies commensurate with its risk and complexity that address the concepts of incident response and resilience. *Source:* IS.II.C.21:pg43: Management should do the following: … Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios. IS.Wp.6.34.c: Determine whether management effectively manages the following information security considerations related to business continuity planning. Review management's ability to do the following: Develop policies that address the concepts of information security incident response and resilience and test information security incident scenarios.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Governance/Strategy-Policies: All elements of the information security program are coordinated enterprise-wide. *Source* IS.Introduction:pg2: Information security programs should have strong board and senior management support, promote integration of security activities and controls throughout the institution's business processes, and establish clear accountability for carrying out security responsibilities. IS.WP.3.2: Determine whether management appropriately integrates the information security program across the institution's lines of business and support functions. Review whether management has the following: Security policies, standards, and procedures that are designed to support and to align with the policies in the lines of business. Incident response programs that include all affected lines of business and support units. Common awareness and enforcement mechanisms between lines of business and information security. Visibility to assess the likelihood of threats and potential damage to the institution. The ability to identify and implement controls over the root causes of an incident. MGT.I.B.2:pg10: The institution should have a comprehensive information security program that addresses all technology and information assets and that complies with the Information Security Standards. The information security program should include appropriate administrative, technical, and physical safeguards based on the inherent risk profile and the individual activities, products, and services of the institution. MGT.III.C.3:pg29: The information security program should be coordinated across the institution. MGT.WP.8.2: Determine whether the institution's management of operational risk incorporates an enterprise-wide view of IT and business processes that are supported by technology.
	Governance/IT Asset Management: An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. *Source*: IS.II.C.5:pg14: Management should inventory and classify assets, including hardware, software, information, and connections. Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections. IS.WP.6.6: Determine whether management effectively maintains an inventory(ies) of hardware, software, information, and connections. Review whether management does the following: Identifies assets that require protection, such as those that store, transmit, or process sensitive customer information, or trade secrets. Classifies assets appropriately. Uses the classification to determine the sensitivity and criticality of assets. Uses the classification to implement controls required to safeguard the institution's assets. Updates the inventory(ies) appropriately. MGT.III.A:pg22: Management should maintain inventories of assets (e.g., hardware, software, and information), event classes (e.g., natural disaster, cyber, and insider abuse or compromise), threats (e.g., theft, malware, and social engineering), and existing controls as an important part of effective risk identification.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Governance/IT Asset Management: Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value. *Source:* IS.II.C.5:pg14: Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections. Management should have policies to govern the inventory and classification of assets both at inception and throughout their life cycle, and wherever the assets are stored, transmitted, or processed. Inventories enable management and staff to identify assets and their functions. Classification enables the institution to determine the sensitivity and criticality of assets. Management should use this classification to implement controls required to safeguard the institution's physical and information assets. IS.WP.6.6: Determine whether management effectively maintains an inventory(ies) of hardware, software, information, and connections. Review whether management does the following: Identifies assets that require protection, such as those that store, transmit, or process sensitive customer information, or trade secrets. Classifies assets appropriately. Uses the classification to determine the sensitivity and criticality of assets. Uses the classification to implement controls required to safeguard the institution's assets. Updates the inventory(ies) appropriately.
	Governance/IT Asset Management: Management assigns accountability for maintaining an inventory of organizational assets. *Source:* IS.II.C.5:pg14: Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections. Management should have policies to govern the inventory and classification of assets both at inception and throughout their life cycle, and wherever the assets are stored, transmitted, or processed. Inventories enable management and staff to identify assets and their functions. Classification enables the institution to determine the sensitivity and criticality of assets. Management should use this classification to implement controls required to safeguard the institution's physical and information assets. IS.WP.6.6: Determine whether management effectively maintains an inventory(ies) of hardware, software, information, and connections. MGT.III.A:pg22: Management should maintain inventories of assets (e.g., hardware, software, and information), event classes (e.g., natural disaster, cyber, and insider abuse or compromise), threats (e.g., theft, malware, and social engineering), and existing controls as an important part of effective risk identification. Inventories should include systems and information hosted or maintained externally.
	Governance/IT Asset Management: A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools. *Source:* IS.II.C.10:pg21: Management should have a process to introduce changes to the environment in a controlled manner. Changes to the IT environment include the following: Configuration management of IT systems and applications. Hardening of systems and applications. Use of standard builds. Patch management. The IT environment consists of operating systems, middleware, applications, file systems, and communications protocols. The institution should have an effective process to introduce application and system changes, including hardware, software, and network devices, into the IT environment. IS.WP.6.11: Determine whether management has a process to introduce changes to the environment (e.g., configuration management of IT systems and applications, hardening of systems and applications, use of standard builds, and patch management) in a controlled manner.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Risk Management/Risk Management Program: An information security and business continuity risk management function(s) exists within the institution. *Source:* IS.II.C.21:pg43: Management should do the following: Identify personnel who will have critical information security roles during a disaster, and train personnel in those roles. Define information security needs for backup sites and alternate communication networks. Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios. *IS.WP.6.34:* Determine whether management effectively manages the following information security considerations related to business continuity planning. MGT.I.B.4:pg12: The business continuity function often resides in the risk management organizational structure. A specific member of management should be assigned responsibility for the oversight of the business continuity function, and both business and technology departments should assign personnel to develop and maintain the individual business unit plans. MGT.WP.3.: As part of the ITRM structure, determine whether financial institution management has defined IT responsibilities and functions. Verify the existence of well-defined responsibilities and expectations between risk management and IT functional areas, such as information security, project management, business continuity, and information systems reporting.
	Risk Management/Risk Assessment: 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. *Source:* IS.I.B:pg4: Management should provide a report to the board at least annually that describes the overall status of the program and material matters related to the program, including the following: Risk assessment process, including threat identification and assessment. IS.WP.2.4: Determine whether the board approves a written information security program and receives a report on the effectiveness of the information security program at least annually. Determine whether the report to the board describes the overall status of the information security program and discusses material matters related to the program such as the following: a. Risk assessment process, including threat identification and assessment. MGT.III.A:pg22: Comprehensive IT risk identification should include identification of cybersecurity risks as well as details gathered during information security risk assessments required under guidelines implementing the GLBA. MGT.WP.7.4: Determine whether the institution maintains a risk assessment process to perform the following: a. Identify risks and threats from both internal and external sources. b. Develop or update policies within the risk management function to guide risk measurement activities. c. Ensure the existence of a process to promote sound understanding and analysis of threats, events, assets, and controls. d. Maintain processes within the risk management function to help make risk mitigation decisions. e. Determine the entities that should have involvement in that decision-making process. f. Ensure that the board and management understand the risk categories.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Risk Management/Risk Assessment: The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls. *Source:* IS.I.B:pg4: Management should provide a report to the board at least annually that describes the overall status of the program and material matters related to the program, including the following: Risk assessment process, including threat identification and assessment. IS.II.C.17:pg38-39: Applications should provide the ability for management to do the following: …Protect web or Internet-facing applications through additional controls, including web application firewalls, regular scanning for new or recurring vulnerabilities, mitigation or remediation of common security weaknesses, and network segregation to limit inappropriate access or connections to the application or other areas of the network. IS.WP.6.27.g: Review whether applications in use provide the following capabilities: Protect web or Internet-facing applications through additional controls, including web application firewalls, regular scanning for new or recurring vulnerabilities, mitigation or remediation of common security weaknesses, and network segregation.
	Risk Management/Risk Assessment: The risk assessment is updated to address new technologies, products, services, and connections before deployment. *Source:* IS.II.A:pg7: External events affecting IT and the institution's ability to meet its operating objectives include natural disasters, cyber attacks, changes in market conditions, new competitors, new technologies, litigation, and new laws or regulations. These events pose risks and opportunities, and the institution should factor them into the risk identification process. IS.II.C:pg11: Additionally, management should develop, maintain, and update a repository of cybersecurity threat and vulnerability information that may be used in conducting risk assessments and provide updates to senior management and the board on cyber risk trends. IS.WP.8.3.d: Determine whether management has effective threat identification and assessment processes, including the following: Using threat knowledge to drive risk assessment and response.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Risk Management/Audit: 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. *Source: AUD.B.4:* The internal audit manager should be responsible for internal control risk assessments, audit plans, audit programs, and audit reports associated with IT. IS.IV.A.2(d):pg56: Independent internal departments or third parties typically perform audits. Audits should review every aspect of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the reasonableness and appropriateness of, and compliance with, policies, standards, and procedures; report on information security activity and control deficiencies to decision makers; identify root causes and recommendations to address deficiencies; and test the effectiveness of controls within the program. MGT.I.B.7(b)pg19: IT auditors should validate that IT controls are designed appropriately to mitigate risk and are operating as management intended. IT audit should be completely independent, should have no role in designing or implementing controls, and should not have primary responsibility for enforcing policy. MGT.WP.6.3: Determine whether the board, or its committee, has appropriate oversight of audit through the following: a. Audit risk assessment and audit plan. b. Audit review activities. c. Audit reports with identified weaknesses. d. Management's responses and corrective actions to audit issues. e. Updates on any audit concerns and the status of issues.
	Risk Management/Audit: The independent audit function validates controls related to the storage or transmission of confidential data. *Source: AUD.B.1:* An effective IT audit program should… promote the confidentiality, integrity, and availability of information systems.
	Risk Management/Audit: Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance). *Source: OPS.B.29:* Operations management should periodically review all logs for completeness and ensure they have not been deleted, modified, overwritten, or compromised. IS.II.C.22:pg43: Logging practices should be reviewed periodically by an independent party to ensure appropriate log management. IS.WP.6.35(c): Review whether management has the following: Independent review of logging practices.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Risk Management/Audit: 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. *Source:* IS.IV.A.2(d):pg56: Internal audit should track the results and the remediation of control deficiencies reported in audits and additional technical reviews, such as penetration tests and vulnerability assessments. IS.WP.2.8: Determine the adequacy of audit coverage and reporting of the information security program by reviewing appropriate audit reports and board or audit committee minutes. AUD.B.8: A risk assessment process to describe and analyze the risks inherent in a given line of business. AUD.WP.I.7.1: Determine the adequacy of the overall audit plan in providing appropriate coverage of IT risks. MGT.I.B.7(b):pg19: Management should also ensure timely and accurate response to audit concerns and exceptions and ensure appropriate and timely corrective action. MGT.WP.1.2: Review management's response to issues raised during, or since, the last examination. Consider the following: a. Adequacy and timing of corrective action. b. Resolution of root causes rather than just specific issues. c. Existence of any outstanding issues. d. Whether management has taken positive action toward correcting exceptions reported in audit and examining reports. e. Independent review of resolution and reporting of resolution to the audit committee. MGT.WP.6.1: Consult with the examiner reviewing audit or IT audit to determine the adequacy of IT audit coverage and management's responsiveness to identified weaknesses.
	Resources/Staffing: Information security roles and responsibilities have been identified. *Source:* IS.II.C.1:pg11: Policies, standards, and procedures guide decisions and activities of users, developers, administrators, and managers and inform those individuals of their information security responsibilities. Policies, standards, and procedures should also specify the mechanisms through which responsibilities can be met. … Policies, standards, and procedures that address the information security program should describe the roles of the information security department, lines of business, and IT organization in administering the information security program. MGT.I:pg4: The governance structure specifies the responsibilities for the board of directors, managers, auditors, and other stakeholders and specifies the level of authority and accountability for decision making. MGT.WP.2.11: Review the institution's structure to determine whether the board established the following: a. The organizational structure provides for effective IT support throughout the institution, from IT management up through senior management and the board. b. Defined roles and responsibilities for key IT positions, including executive management (CEO and COO, and often CIO or CTO), and CISO. e. A CISO or information security officer position responsible for the management and mitigation of information security risks.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Resources/Staffing: Processes are in place to identify additional expertise needed to improve information security defenses. *Source: IS.I.C:pg5: Funding, along with technical and managerial talent, also contributes to the effectiveness of the information security program. Management should provide, and the board should oversee, adequate funding to develop, implement, and maintain a successful information security program. The program should be staffed by sufficient personnel who have skills that are aligned with the institution's technical and managerial needs and commensurate with its size, complexity, and risk profile. Knowledge of technology standards, practices, and risk methodologies is particularly important to the success of the information security program*. MGT.I.B.7(a):pg18: An institution should have programs in place to ensure that staff members have the expertise necessary to perform their jobs and achieve company goals and objectives. The institution may need to look externally to find necessary expertise for specialized areas. MGT.WP.5.2.b: Employees have appropriate qualifications. MGT.WP.5.5: Determine whether the financial institution has a process to ensure that staff has the requisite expertise to fulfill its roles. Review the adequacy of the process.
	Training and Culture/Training: Annual information security training is provided. *Source:* IS.B:pgs4-5: Management also should do the following: … Provide information security and awareness training and ongoing security-related communications to employees, and ensure employees complete such training annually. IS.WP.2.5.l: Determine whether management responsibilities are appropriate and include the following: Facilitation of annual information security and awareness training and ongoing security-related communications to employees. MGT.III.C.2:pg28: The institution should use job descriptions, employment agreements (usually for higher-level or higher-sensitivity positions), training, and awareness programs to promote understanding and increase individual accountability. MGT.WP.12.5.f: Determine whether management has effective hiring and training practices that provide information security awareness and training programs.
	Training and Culture/Training: Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues. *Source:* IS.II.C.7(e):pg17: Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. IS.WP.6.8.f: Determine whether management effectively mitigates risks posed by users. Review whether management does the following: Provides training to support awareness and policy compliance.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Training and Culture/Training: Situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts. *Source:* IS.II.C.7(e):pg17:: Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. IS.WP.6.8.f: Determine whether management effectively mitigates risks posed by users. Review whether management does the following: Provides training to support awareness and policy compliance.
	Training and Culture/Training: Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials). *Source:* IS.II.C.16:pg36: Beyond authentication, remote access controls should include additional layered security controls and may include some combination of the following: Customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk. IS.II.C.16(a): pg37: The institution's customer awareness and education efforts should consider both retail and commercial account holders. IS.WP.6.26: Determine whether management develops customer awareness and education efforts that address both retail (consumer) and commercial account holders.
	Training and Culture/Culture: Management holds employees accountable for complying with the information security program. *Source:* IS.II.C.7(e):pg17: Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected**.** MGT.III.C.2:pg28: Management should require periodic acknowledgement of acceptable use policies for the network, software applications, Internet, e-mail, confidential data, and social media. Information security awareness and training programs help support information security and other management policies. MGT.WP.12.5: Determine whether management has effective hiring and training practices that include the following: d. Requiring periodic acknowledgement of acceptable use policies. e. Obtaining signed confidentiality and nondisclosure agreements. f. Providing information security awareness and training programs.

Yes/No	FFIEC Cybersecurity Assessment Tool
Domain 2 – Threat Intelligence and Collaboration	
	Threat Intelligence/Threat Intelligence and Information: The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (e.g., FS-ISAC, US-CERT). *Source*: IS.II.C:pg11: Management should also obtain, analyze, and respond to information from various sources (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC]) on cyber threats and vulnerabilities that may affect the institution. IS.WP.8.3.f: Determine whether management has effective threat identification and assessment processes, including the following: Developing appropriate processes to evaluate and respond to vulnerability information from external groups or individuals. MGT.III.A:pg22: Participation in an information-sharing forum, such as FS–ISAC, should be a component of the risk identification process because sharing information may help the institution identify and evaluate relevant cybersecurity threats and vulnerabilities. MGT.WP.10.1.b: Determine whether management participates in an information sharing forum (such as FS-ISAC).
	Threat Intelligence/Threat Intelligence and Information: Threat information is used to monitor threats and vulnerabilities. *Source:* IS.III.A:pg47: Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information. The identification of threats involves the sources of threats, their capabilities, and their objectives. Information about threats generally comes from government (e.g., US-CERT), information-sharing organizations (e.g., FS-ISAC), industry sources, the institution, and third parties. IS.WP.8.3.f: Determine whether management has effective threat identification and assessment processes, including the following: Developing appropriate processes to evaluate and respond to vulnerability information from external groups or individuals. MGT.I.A.2:pg6: Establish a formal process to obtain, analyze, and respond to information on threats and vulnerabilities by developing a repeatable threat intelligence and collaboration program. MGT.WP.2.8.f: Establishes a formal process to obtain, analyze, and respond to information on threats and vulnerabilities by developing a repeatable threat intelligence and collaboration program. MGT.III.C.3:pg29: Institution management should: Develop and implement a threat intelligence and collaboration process to identify and respond to information on threats and vulnerabilities. MGT.WP.12.8.c: Determine whether the control structure includes: Using a threat intelligence and collaboration process to identify and respond to information on threats and vulnerabilities.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Threat Intelligence/Threat Intelligence and Information: Threat information is used to enhance internal risk management and controls. *Source:* IS.III.A:pg48: Once a threat is identified and potential vulnerabilities are assessed, the significance of the threat should trigger a response. The response should be commensurate with the risk posed by the threat and should include remediation options. Management should design policies to allow for immediate and consequential threats to be dealt with expeditiously, while less significant threats are addressed as part of a broader risk management process. When management receives vulnerability information from external individuals or groups, management should have appropriate processes and procedures to evaluate the credibility of the information to appropriately address it. IS.WP.8.3.a.d: Determine whether management has effective threat identification and assessment processes, including the following: Maintaining procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information….Using threat knowledge to drive risk assessment and response.
	Monitoring and Analyzing/Monitoring and Analyzing: Audit log records and other security event logs are reviewed and retained in a secure manner. *Source:* IS.II.C.22:pg44: Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs. …Additionally, logging practices should be reviewed periodically by an independent party to ensure appropriate log management. … Regardless of the method of log management, management should develop processes to collect, aggregate, analyze, and correlate security information. IS.WP.6.35: Determine whether management has an effective log management process that involves a central logging repository, timely transmission of log files, and effective log analysis.
	Monitoring and Analyzing/Monitoring and Analyzing: Computer event logs are used for investigations once an event has occurred. *Source:* IS.II.C.22:pg44: Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information… Security information and event management (SIEM) systems can provide a method for management to collect, aggregate, analyze, and correlate information from discrete systems and applications. Management can use SIEM systems to discern trends and identify potential information security incidents. IS.WP.6.35: Determine whether management has an effective log management process that involves a central logging repository, timely transmission of log files, and effective log analysis. Review whether management has the following: (d) Processes to effectively collect, aggregate, analyze, and correlate security event information from discrete systems and applications.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Information Sharing/Information Sharing: Information security threats are gathered and shared with applicable internal employees. *Source:* IS.II.D:pg45: Risk reporting is a process that produces information systems reports that address threats, capabilities, vulnerabilities, and inherent risk changes. Risk reporting should describe any information security events that the institution faces and the effectiveness of management's response and resilience to those events. The reporting process should provide a method of disseminating those reports to appropriate members of management. The contents of the reports should prompt action, if necessary, in a timely manner to maintain appropriate levels of risk. IS.WP.7.1: Determine whether the institution has risk monitoring and reporting processes that address changing threat conditions in both the institution and the greater financial industry. Determine whether these processes address information security events faced by the institution, the effectiveness of management's response, and the institution's resilience to those events. Review whether the reporting process includes a method of disseminating those reports to appropriate members of management.
	Information Sharing/Information Sharing: Contact information for law enforcement and the regulator(s) is maintained and updated regularly. *Source: BCP.WP.I.5.1:* Include(s) emergency preparedness and crisis management plans that…Include an accurate contact tree, as well as primary and emergency contact information, for communicating with employees, service providers, vendors, regulators, municipal authorities, and emergency response personnel. IS.III.D:pg.51: Primary considerations for incident response include the following: Protocols to define when and under what circumstances to notify and involve regulators, customers, and law enforcement, including names and contact information for each group. MGT.III.C.3:pg29: Develop a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulator based on thresholds defined by the financial institution and applicable legal requirements. Relevant thresholds could include significant financial impact, significant operational downtime, operational or system breach, or loss of critical infrastructure. MGT.WP.12.8.i: Developing a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulators based on thresholds defined by the financial institution.
	Information Sharing/Information Sharing: Information about threats is shared with law enforcement and regulators when required or prompted. *Source:* IS.III.D:pg.51: Primary considerations for incident response include the following: How, when, and what to communicate outside of the institution, whether to law enforcement, regulatory agencies, information-sharing organizations, customers, third-party service providers, potential victims, or others. MGT.III.C.3:pg29: Develop a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulator based on thresholds defined by the financial institution and applicable legal requirements. Relevant thresholds could include significant financial impact, significant operational downtime, operational or system breach, or loss of critical infrastructure. *MGT.WP.*12.8.i: Developing a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulators based on thresholds defined by the financial institution.

Yes/No	FFIEC Cybersecurity Assessment Tool
Domain 3 – Cybersecurity Controls	
	Preventive Controls/Infrastructure Management: Network perimeter defense tools (e.g., border router and firewall) are used. *Source:* IS.II.C.9:pg19: Tools used to enforce and detect perimeter protection include routers, firewalls, intrusion detection systems (IDS) and intrusion prevention systems, proxies, gateways, jump boxes, demilitarized zones, virtual private networks (VPN), virtual LANs (VLAN), log monitoring and network traffic inspecting systems, data loss prevention (DLP) systems, and access control lists. IS.WP.8.1.a: Determine whether the institution's security operations activities include the following: Security software and device management (e.g., maintaining the signatures on signature-based devices and firewall rules).
	Preventive Controls/Infrastructure Management: Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. *Source:* IS.II.C.17:pg39: Protect web or Internet-facing applications through additional controls, including web application firewalls, regular scanning for new or recurring vulnerabilities, mitigation or remediation of common security weaknesses, and network segregation to limit inappropriate access or connections to the application or other areas of the network. IS.WP.6.27(g): Review whether applications in use provide the following capabilities: Protect web or Internet-facing applications through additional controls, including web application firewalls, regular scanning for new or recurring vulnerabilities, mitigation or remediation of common security weaknesses, and network segregation. OPS.B.23: Transmission controls should address both physical and logical risks. In large, complex institutions, management should consider segregating wide area networks (WAN) and local area networks (LAN) segments with firewalls that restrict access as well as the content of inbound and outbound traffic. OPS.WP.8.1: Determine whether management has implemented appropriate daily operational controls and processes including… alignment of telecommunication architecture and process with the strategic plan. MGT.III.C.3:pg29: Conduct initial due diligence and ongoing monitoring to fully understand the types of connections and mitigating controls in place between the financial institution and its third- party providers.
	Preventive Controls/Infrastructure Management: All ports are monitored. *Source* IS.II.C.12:pg26: Port monitoring to identify unauthorized network connections. IS.II.C.16:pg37: To prevent or minimize exposure to these incidents, management should do the following: .Limit traffic (e.g., allow valid traffic and block known bad traffic by port or IP address).
	Preventive Controls/Infrastructure Management: Up-to-date anti-virus and anti-malware tools are used. *Source:* IS.II.C.12:pg26: Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. IS.WP.6.17: Determine whether management has implemented defense-in-depth to protect, detect, and respond to malware.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Preventive Controls/Infrastructure Management: Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced. *Source:* IS.II.C.10(c):pg23: The institution should use standard builds, which allow one documented configuration to be applied to multiple computers in a controlled manner. IS.WP.6.14: Determine whether management uses standard builds, allowing one documented configuration to be applied to multiple computers in a controlled manner, to create hardware and software inventories, update or patch systems, restore systems, investigate anomalies, and audit configurations.
	Preventive Controls/Infrastructure Management: Ports, functions, protocols and services are prohibited if no longer needed for business purposes. *Source*: IS.II.C.10(b):pg23: Hardening can include the following actions: …Determining the purpose of the applications and systems and documenting minimum software and hardware requirements and services to be included. Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure. IS.B.6.13: Determine whether management has processes to harden applications and systems (e.g., installing minimum services, installing necessary patches, configuring appropriate security settings, enforcing principle of least privilege, changing default passwords, and enabling logging}.
	Preventive Controls/Infrastructure Management: Access to make changes to systems configurations, (including virtual machines and hypervisors) is controlled and monitored. *Source:* IS.II.C.10:pg21: The institution should have an effective process to introduce application and system changes, including hardware, software, and network devices, into the IT environment…Application and system control considerations for introducing changes to the IT environment before implementation should include the following…Restricting changes to authorized users. IS.WP.6.11: Determine whether management has a process to introduce changes to the environment (e.g., configuration management of IT systems and applications, hardening of systems and applications, use of standard builds, and patch management) in a controlled manner.
	Preventive Controls/Infrastructure Management: Programs that can override system, object, network, virtual machine, and application controls are restricted. *Source:* IS.II.C.15(a):pg32: System and security administrators should restrict and monitor privileged access to operating systems and system utilities. IS.WP.6.21: As part of management's process to secure the operating system and all system components, determine whether management does the following: Limits the number of employees with access to operating system and system utilities and grants only the minimum level of access required to perform job responsibilities.
	Preventive Controls/Infrastructure Management: System sessions are locked after a pre-defined period of inactivity and are terminated after pre-defined conditions are met. *Source:* IS.II.C.16:pg36: Beyond authentication, remote access controls should include additional layered security controls and may include some combination of the following: Application time-outs with mandatory re-authentication.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Preventive Controls/Infrastructure Management: Wireless network environments require security settings with strong encryption for authentication and transmission. (*N/A if there are no wireless networks.) *Source:* IS.II.C.9(a):pg20: Management should use an industry-accepted level of encryption with strength commensurate with the institution's risk profile on the institution's wireless networks. IS.II.C.9(a):pg21: Institutions often provide remote network connectivity for employees or third-party service providers who are not located within or around the institution's facilities. This connectivity presents operational advantages, but steps should be taken to ensure that the connection is encrypted and secured. VPN connections should be used for both broadband networks and wireless air card connections to isolate and encrypt remote traffic to institution networks.
	Preventive Controls/Access and Data Management: Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. *Source*: IS.II.C.7:pg15: Users should be granted access to systems, applications, and databases based on their job responsibilities. IS.II.C.10(b):pg23: Hardening can include the following actions: … Configuring privilege and access controls by first denying all, then granting back the minimum necessary to each user (i.e., enforcing the principle of least privilege). IS.WP.6.13: Determine whether management has processes to harden applications and systems (e.g., installing minimum services, installing necessary patches, configuring appropriate security settings, enforcing principle of least privilege, changing default passwords, and enabling logging). MGT.III.C.2:pg28: Management should document and confirm access privileges for each staff member based on his or her job description.
	Preventive Controls/Access and Data Management: Employee access to systems and confidential data provides for separation of duties. *Source:* IS.II.C.7:pg15: Management should mitigate the risks posed by users by doing the following: Employing segregation of duties. IS.WP.2.5.g: Determine whether management responsibilities are appropriate and include the following: …Establishment of appropriate segregation of duties.
	Preventive Controls/Access and Data Management: Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls). *Source:* IS.II.C.15:pg31: Authorization for privileged access should be tightly controlled. IS.WP.6.20: Determine whether management has an effective process to administer logical security access rights for the network, operating systems, applications, databases, and network devices. Review whether management has the following: A process to control privileged access.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Preventive Controls/Access and Data Management: User access reviews are performed periodically for all systems and applications based on the risk to the application or system. *Source:* IS.II.C.15:pg31: As part of the user access rights monitoring process, management should perform regular reviews to validate user access. Reviews should test whether access rights continue to be appropriate or whether they should be modified or deleted. Management should review access rights on a schedule commensurate with risk. IS.Wp.6.8.c: Determine whether management effectively mitigates risks posed by users. Review whether management does the following:…Establishes and appropriately administers a user access program for physical and logical access. MGT.III.C.2:pg28: Management should establish a timely process to review, update, and remove access privileges associated with any party when appropriate. The lack of such a process may result in unauthorized or inappropriate activity. Failure to remove access privileges when appropriate, particularly for those individuals with high levels of privilege, represents significant
	Preventive Controls/Access and Data Management: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel. *Source:* IS.II.C.7(b):pg16: Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements:…Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel. Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations. IS.WP.6.8: Determine whether management effectively mitigates risks posed by users. Review whether management does the following:…Develops and maintains a culture that fosters responsible and controlled access for users. Establishes and appropriately administers a user access program for physical and logical access.
	Preventive Controls/Access and Data Management: Identification and authentication are required and managed for access to systems, applications, and hardware. *Source*: ISIS.II.C.15(b):pg33: Management should implement effective application access controls by doing the following: Implementing a robust authentication method consistent with the criticality and sensitivity of the application. IS.WP.6.22: Determine whether management controls access to applications. Review whether management does the following: Implements a robust authentication method consistent with the criticality and sensitivity of the application
	Preventive Controls/Access and Data Management: Access controls include password complexity and limits to password attempts and reuse. *Source: IS.II.C.7:pg15:* Access rights should be granted in accordance with the institution's physical and logical access control policies. IS.WP.8.1.k: Determine whether the institution's security operations activities include the following: Enforcement of access controls and logical access control policies.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Preventive Controls/Access and Data Management: All default passwords and unnecessary default accounts are changed before system implementation. *Source:* IS.II.C.15:pg31: Access rights to new software and hardware present a different problem. Typically, hardware and software are shipped with default users and at least one default user has privileged access. Lists of default accounts and passwords are readily available and can enable anyone with access to the system to obtain privileged access. These passwords should be changed, and the accounts should be disabled. IS.WP.6.20: Determine whether management has an effective process to administer logical security access rights for the network, operating systems, applications, databases, and network devices. Review whether management has the following: A process to change or disable default user accounts and passwords.
	Preventive Controls/Access and Data Management: Customer access to Internet-based products or services requires authentication controls (e.g., layered controls, multifactor) that are commensurate with the risk. *Source:* IS.II.C.16:pg36: Institutions increasingly offer services to customers through remotely accessible technology, such as the Internet and mobile financial services. If the institution offers such services, management should implement appropriate authentication techniques commensurate with the risk from remote banking activities. IS.WP.6.22: Determine whether management controls access to applications. Review whether management does the following: Implements a robust authentication method consistent with the criticality and sensitivity of the application.
	Preventive Controls/Access and Data Management: 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.) *Source:* IS.II.C.9:pg19: Management should secure access to computer networks through multiple layers of access controls by doing the following: Establishing zones (e.g., trusted and untrusted) according to the risk profile and criticality of assets contained within the zones and appropriate access requirements within and between each security zone. IS.WP.6.10.a: Determine whether management secures access to its computer networks through multiple layers of access controls. Review whether management does the following: Establishes zones (e.g., trusted and untrusted) according to risk with appropriate access requirements within and between each zone.
	Preventive Controls/Access and Data Management: Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems. *Source:* IS.II.C.8:pg18: Management should implement appropriate preventive, detective, and corrective controls for physical security. Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Management should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones. IS.WP.6.9: Determine whether management applies appropriate physical security controls to protect its premises and more sensitive areas, such as its data center(s).

Yes/No	FFIEC Cybersecurity Assessment Tool
	Preventive Controls/Access and Data Management: All passwords are encrypted in storage and in transit. *Source: IS.II.C.19:pg41: Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information….Passwords should be hashed or encrypted in storage*. IS.WP.6.30: Determine how and where management uses encryption and if the type and strength are sufficient to protect information appropriately.
	Preventive Controls/Access and Data Management: Confidential data are encrypted when transmitted across public or untrusted networks (e.g., Internet). *Source:* IS.II.C.13(b):pg28: When transmitting sensitive information over a public network, information should be encrypted to protect it from interception or eavesdropping. IS.WP.6.30: Determine how and where management uses encryption and if the type and strength are sufficient to protect information appropriately.
	Preventive Controls/Access and Data Management: 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). *Source:* IS.II.C.13(a):pg27: Data storage in portable devices, such as laptops, smart phones, and tablets, poses unique problems….Risk mitigation typically involves data encryption. IS.WP.6.30: Determine how and where management uses encryption and if the type and strength are sufficient to protect information appropriately.
	Preventive Controls/Access and Data Management: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. *Source:* IS.II.C.15(c):pg33: Management should develop policies to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner… Management should employ the following measures: Use robust authentication methods for access and encryption to secure communications. IS.WP.6.23: Review whether management does the following: Provides remote access in a safe and sound manner. Implements the controls necessary to offer remote access securely (e.g., disables unnecessary remote access, obtains approvals for and performs audits of remote access, maintains robust configurations, enables logging and monitoring, secures devices, restricts remote access during specific times, controls applications, enables strong authentication, and uses encryption).
	Preventive Controls/Access and Data Management: Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software. *Source:* IS.II.C.12:pg26: Methods or systems that management should consider include the following:...Monitoring for unauthorized software and disallowing the ability to install unauthorized software. IS.WP.6.11: Determine whether management has a process to introduce changes to the environment (e.g., configuration management of IT systems and applications, hardening of systems and applications, use of standard builds, and patch management) in a controlled manner.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Preventive Controls/Access and Data Management: Customer service (e.g., the call center) utilizes formal procedures to authenticate customers commensurate with the risk of the transaction or request. *Source:* IS.II.C.16:pg36: Beyond authentication, remote access controls should include additional layered security controls and may include some combination of the following: Controls over changes to account maintenance activities (e.g., address or password changes) performed by customers either online or through customer service channels. IS.WP.6.22.a: Determine whether management controls access to applications. Review whether management does the following: Implements a robust authentication method consistent with the criticality and sensitivity of the application.
	Preventive Controls/Access and Data Management: Data are disposed of or destroyed according to documented requirements and within expected time frames. *Source:* IS.II.C.13(c):pg28: The institution should base its disposal policies on the sensitivity of the information. Policies, procedures, and training should inform employees about what actions should be taken to securely dispose of computer-based media and protect the data from the risks of reconstruction. IS.WP.6.18.e: Determine whether management maintains policies and effectively controls and protects access to and transmission of information to avoid loss or damage. Review whether management does the following:…Has appropriate disposal procedures for both paper-based and electronic information.
	Preventive Controls/Device-End Point Security: Controls are in place to restrict the use of removable media to authorized personnel. *Source:* IS.II.C.13(a):pg27: Management should implement appropriate controls (such as the use of a DLP program) over portable devices and the sensitive information contained on them. IS.II.C.13(d):pg29: Management should implement policies for maintaining the security of physical media (including backup tapes) containing sensitive information while in transit, including to off-site storage, or when shared with third parties…. Use of adequate encryption of sensitive information recorded on media that is being physically transported. IS.WP.6.18: Determine whether management maintains policies and effectively controls and protects access to and transmission of information to avoid loss or damage. Review whether management does the following: Requires secure storage of all types of sensitive information, whether on computer systems, portable devices, physical media, or hard-copy documents.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Preventive Controls/Secure Coding: Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards. *Source:* IS.II.C.17:pg38: A secure software development life cycle ensures that Internet- and client-facing applications have the necessary security controls. The institution should ensure that all applications are securely developed…. At institutions that employ third parties to develop applications, management should ensure that the third parties meet the same controls. IS.WP.6.27: Determine whether management uses applications that were developed by following secure development practices and that meet a prudent level of security. MGT.III.C.5:pg31: Management should guide the development or acquisition of software by using a system development life cycle (SDLC) or similar methodology appropriate for the specific IT environment. The extent or use of the SDLC depends on the size and complexity of the institution and the type of development activities performed. If the institution primarily acquires software, management should verify the effective use of an SDLC by the third-party provider. MGT.WP.12.10. Determine whether management assesses and mitigates the operational risks associated with the development or acquisition of software. Appropriate management of the risks should include the following: a. Policies documenting risk management controls for the development and acquisition of systems. b. System development life cycle or similar methodology based on the complexity and type of development performed.
	Preventive Controls/Secure Coding: The security controls of internally developed software are periodically reviewed and tested. (*N/A if there is no software development.). *Source*: IS.II.C.10:pg21: The process for introducing software should encompass securely developing, implementing, and testing changes to both internally developed and acquired software. IS.WP.6.15: Determine whether management has a process to update and patch operating systems, network devices, and software applications, including internally developed software provided to customers, for newly discovered vulnerabilities. MGT.III.C.5:pg31: Testing, which should include tests of security, validates that equipment and systems function properly and produce the desired results. As part of the testing process, management should verify whether new technology systems operate effectively with other technology components, including vendor-supplied technology. Management should conduct retesting periodically to help manage risk exposure on an ongoing basis. MGT.WP.12.10. Determine whether management assesses and mitigates the operational risks associated with the development or acquisition of software. Appropriate management of the risks should include the following: a. Policies documenting risk management controls for the development and acquisition of systems. b. System development life cycle or similar methodology based on the complexity and type of development performed. c. Tests of new technology, systems, and products before deployment to validate functionality, controls, and interoperability.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Preventive Controls/Secure Coding: 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.) *Source:* D&A.B.2: Financial institutions should consider information security requirements and incorporate automated controls into internally developed programs, or ensure the controls are incorporated into acquired software, before the software is implemented. D&A.B.9: Independence – Audit and quality assurance personnel should be independent of the project they are reviewing. D&A.WP.13.1: Evaluate the security and integrity of system and application software by reviewing: the adequacy of quality assurance and testing programs: the adequacy of security and internal- control design standards; the adequacy of involvement by audit and security personnel in software development and acquisition projects; and the adequacy of internal and external security and control audits. MGT.III.C.5:pg31: Audit should review the SDLC to ensure that appropriate controls are incorporated during development. Management should test new technology, systems, and products thoroughly before deployment. MGT.WP.12.10.c: Appropriate management of the risks should include tests of new technology, systems, and products before deployment to validate functionality, controls, and interoperability.
	Preventive Controls/Secure Coding: Intellectual property and production code are held in escrow. (*N/A if there is no production code to hold in escrow.) Source: D&A.B.39: In addition to ensuring access to current documentation, organizations should consider protecting their escrow rights by contractually requiring software vendors to inform the organization if the software vendor pledges the software as loan collateral. D&A.WP.6.1: Assess the adequacy of acquisition activities by evaluating… The adequacy of contract and licensing provisions that address… Source-code accessibility/escrow assertions.
	Detective Controls/Threat and Vulnerability Detection: Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network. *Source:* ISIS.II.C.17:pg38: To verify the controls have been developed and implemented appropriately, management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications. IS.WP.4.2.d: Review whether management has the following: A validation of the risk identification process through audits, self-assessments, penetration tests, and vulnerability assessments. MGT.III.C.3:pg29: Perform penetration tests before launching or making significant changes to critical systems, including Internet- and client-facing applications. Management should review all findings and develop processes to ensure the timely remediation of issues identified by the tests. MGT.WP.12.8.f: Determine whether, as part of the institution's information security program, the board of directors oversees and management establishes a control structure that is intended to specifically address cybersecurity risks and includes the following: Performing penetration tests before launching new or making significant changes to existing Internet- and client-facing applications and remediating findings from the tests.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Detective Controls/Threat and Vulnerability Detection: Anti-virus and anti-malware tools are used to detect attacks. *Source:* IS.II.C.12:pg26: Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. IS.WP.6.17: Determine whether management has implemented defense-in-depth to protect, detect, and respond to malware.
	Detective Controls/Threat and Vulnerability Detection: Firewall rules are audited or verified at least quarterly. *Source:* IS.III:pg46: Security operations activities can include the following: Security software and device management (e.g., maintaining the signatures on signature-based devices and firewall rules). IS.WP.8.1.a: Determine whether the institution's security operations activities include the following: Security software and device management (e.g., maintaining the signatures on signature-based devices and firewall rules).
	Detective Controls/Threat and Vulnerability Detection: E-mail protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links). *Source:* IS.II.C.12:pg26: Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. IS.WP.6.17: Determine whether management has implemented defense-in-depth to protect, detect, and respond to malware.
	Detective Controls/Anomalous Activity Detection: The institution is able to detect anomalous activities through monitoring across the environment. *Source:* IS.II.C.12:pg26: Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. Methods or systems that management should consider include the following: …Monitoring for anomalous activity for malware and polymorphic code. IS.WP.6.17: Determine whether management has implemented defense-in-depth to protect, detect, and respond to malware.
	Detective Controls/Anomalous Activity Detection: Customer transactions generating anomalous activity alerts are monitored and reviewed. *Source:* WPS.B.12: Monitor and log access to funds transfer systems, maintaining an audit trail of all sequential transactions. WPS.WP.II.1.3: Requires its senior management receive and review activity and quality control reports which disclose unusual or unauthorized activities and access attempts.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Detective Controls/Anomalous Activity Detection: Logs of physical and/or logical access are reviewed following events. *Source:* ISIII.C.22:pg44: Institutions maintain event logs to understand an incident or cyber event after it occurs. Monitoring event logs for anomalies and relating that information with other sources of information broadens the institution's ability to understand trends, react to threats, and improve reports to management and the board. IS.WP.6.21(f): As part of management's process to secure the operating system and all system components, determine whether management does the following: Filters and reviews logs for potential security events and provides adequate reports and alerts.
	Detective Controls/Anomalous Activity Detection: Access to critical systems by third parties is monitored for unauthorized or unusual activity. *Source:* OT.B.26: Appropriate access controls and monitoring should be in place between service provider's systems and the institution.
	Detective Controls/Anomalous Activity Detection: Elevated privileges are monitored. *Source:* IS.II.C.15:pg31: Authorization for privileged access should be tightly controlled. IS.WP.8.4.f: Determine whether management has effective threat monitoring processes, including the following: Establishing and documenting a process to independently monitor administrators and other users with higher privileges.
	Detective Controls/Event Detection: A normal network activity baseline is established. *Source:* IS.III.C:pg49: Incident identification involves indicators and analysis. …Examples of technology-based intrusion identification systems and tools include the following:…Network behavior analysis systems. IS.WP.8.4.e: Determine whether management has effective threat monitoring processes, including the following: Monitoring both incoming and outgoing network traffic to identify malicious activity and data exfiltration.
	Detective Controls/Event Detection: Mechanisms (e.g., anti-virus alerts, log event alerts) are in place to alert management to potential attacks. Source: IS.III.B:pg48: Threat monitoring policies should provide for continual and ad hoc monitoring of threat intelligence communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal procedures…. Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies. IS.WP.8.5: Determine whether management has effective incident identification and assessment processes to do the following: e. Escalate the event consistent with the classification. f. Report internally and externally as appropriate.
	Detective Controls/Event Detection: Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. *Source:* IS.Introduction:pg2: Aligns the information security program with the enterprise risk management program and identifies, measures, mitigates, and monitors risk….Management should be able to identify and characterize the threats, assess the risks, make decisions regarding the implementation of appropriate controls, and provide appropriate monitoring and reporting.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Detective Controls/Event Detection: Responsibilities for monitoring and reporting suspicious systems activity have been assigned. *Source*: IS.III.B:pg48: Management should establish the responsibility and authority of security personnel and system administrators for monitoring. Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies. IS.WP.8.4.b: Determine whether management has effective threat monitoring processes, including the following: Establishing responsibility and accountability for security personnel and system administrators for monitoring.
	Detective Controls/Event Detection: The physical environment is monitored to detect potential unauthorized access. *Source:* IS.II.C.8:pg18: Management should implement appropriate preventive, detective, and corrective controls for physical security. IS.WP.6.9: Determine whether management applies appropriate physical security controls to protect its premises and more sensitive areas, such as its data center(s).
	Corrective Controls/Patch Management: A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner. *Source:* IS.II.C.10(d):pg24: Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. IS.WP.6.15: Determine whether management has a process to update and patch operating systems, network devices, and software applications, including internally developed software provided to customers, for newly discovered vulnerabilities. OPS.B.22: Management should establish procedures to stay abreast of patches, to test them in a segregated environment, and to install them when appropriate. OPS.WP.5.1: Determine whether management has implemented and effectively utilizes operational control programs, processes, and tools such as… Project, change, and patch management.
	Corrective Controls/Patch Management: Patches are tested before being applied to systems and/or software. *Source:* OPS.B.22: Management should establish procedures to stay abreast of patches, to test them in a segregated environment, and to install them when appropriate. OPS.WP.5.1: Determine whether management has implemented and effectively utilizes operational control programs, processes, and tools such as… Project, change, and patch management.
	Corrective Controls/Patch Management: Patch management reports are reviewed and reflect missing security patches. *Source:* D&A.B.50: Patch management standards should include procedures for identifying, evaluating, approving, testing, installing, and documenting patches…Organizations should have procedures in place to identify available patches and to acquire them from trusted sources.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Corrective Controls/Remediation: Issues identified in assessments are prioritized and resolved based on criticality and within the time frames established in the response to the assessment report. *Source:* IS.IV.A.4:pg56: The reports should prioritize risk and findings in the order of importance, suggest options for remediation, and highlight repeat issues. Additionally, reports should address root causes. … Reporting should trigger appropriate, timely, and reliable escalation and response procedures. IS.WP.1.2.a: Review management's response to issues raised at, or since, the last examination. Consider the following: Adequacy and timing of corrective action.
Domain 4 – External Dependency Management	
	Connections/Connections: The critical business processes that are dependent on external connectivity have been identified. *Source:* IS.II.C.6:pg14-15: To mitigate interconnectivity risk, management should do the following: Identify connections with third parties, including other financial institutions, financial institution. IS.WP.6.7: Determine whether management comprehensively and effectively identifies, measures, mitigates, monitors, and reports interconnectivity risk.
	Connections/Connections: The institution ensures that third-party connections are authorized. *Source:* IS.II.C.6:pg14-15: To mitigate interconnectivity risk, management should do the following: Identify connections with third parties, including other financial institutions, financial institution intermediaries, and third-party service providers….Assess all connections with third parties that provide remote access capability or control over internal systems. IS.WP.6.7: Determine whether management comprehensively and effectively identifies, measures, mitigates, monitors, and reports interconnectivity risk. Review whether management does the following: Identifies connections with third parties. …Measures the risk associated with connections with third parties with remote access. Implements and assesses the adequacy of appropriate controls to ensure the security of connections.
	Connections/Connections: A network diagram is in place and identifies all external connections. *Source:* IS.II.C.9:pg20: To ensure appropriate network security, management should maintain accurate network and data flow diagrams, and store them securely, providing access only to essential personnel. These diagrams should identify hardware, software, and network components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture. IS.WP.6.10.b: Determine whether management secures access to its computer networks through multiple layers of access controls. Review whether management does the following: Maintains accurate network diagrams and data flow charts.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Connections/Connections: Data flow diagrams are in place and document information flow to external parties. *Source:* IS.II.C.9:pg20: To ensure appropriate network security, management should maintain accurate network and data flow diagrams, and store them securely, providing access only to essential personnel. These diagrams should identify hardware, software, and network components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture. IS.WP.6.10.b: Determine whether management secures access to its computer networks through multiple layers of access controls. Review whether management does the following: Maintains accurate network diagrams and data flow charts.
	Relationship Management/Due Diligence: 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. *Source:* IS.II.C.20:pg42: Management should oversee outsourced operations through the following: Appropriate due diligence in third-party research, selection, and relationship management. IS.WP.6.31: Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. Review the due diligence involved, security controls to mitigate risk, and monitoring capabilities over the institution's third parties. MGT.III.C.8:pg34: An effective third-party management program should provide the framework for management to identify, measure, mitigate, monitor, and report risks associated with the use of third-party providers. Management should develop and implement enterprise-wide policies and procedures to govern the third-party management program, including establishing objectives and strategies, selecting a provider, negotiating the contract, and monitoring the outsourced relationship. MGT.WP.12.14.d: An effective third-party management program should incorporate: Evaluation of prospective third-party providers based on the scope and criticality of services provided.
	Relationship Management/Due Diligence: A list of third-party service providers is maintained. *Source:* OT.B.19: To increase monitoring effectiveness, management should periodically rank service provider relationships according to risk to determine which service providers require closer monitoring. OT.WP.I.1.3: Interview management and review institution information to identify…current outsourcing relationships, including cloud computing relationships, and changes to those relationships since the last examination. Identify any material service provider subcontractors; affiliated service providers; foreign-based third-party providers; current transaction volume in each function outsourced; any material problems experienced with the service provided; and service providers with significant financial- or control-related weaknesses.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Relationship Management/Due Diligence: A risk assessment is conducted to identify criticality of service providers. *Source:* OT.B.6: Management should consider the following factors in evaluating the quantity of risk at the inception of an outsourcing decision, [including]…Risks pertaining to the function outsourced include… [and] Risks pertaining to the technology used. OT.B.23: Financial institutions must also consider which of their critical financial services rely on TSP services, including key telecommunication and network service providers. MGT.III.C.8:pg34: Management should evaluate the quality of service, control environment, and financial condition of the third parties providing the institution with critical IT services. MGT.III.C.8:pg35: Some factors that management should consider or address regarding an effective third-party management program include the following: Tailoring the institution's third-party management program based on an initial and ongoing risk assessment of the institution's third parties and the services they provide. MGT.WP.12.14: An effective third-party management program should incorporate the following: d. Evaluation of prospective third-party providers based on the scope and criticality of services provided. e. Tailoring of the monitoring program based on the initial and ongoing risk assessment of the third party and the services provided..
	Relationship Management/Contracts: 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. *Source:* IS.II.C.20:pg42: If the third-party service provider stores, transmits, processes, or disposes of customer information, management should require third- party service providers by contract to implement appropriate measures designed to meet the Information Security Standards. IS.WP.6.31(c): Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. Review the due diligence involved, security controls to mitigate risk, and monitoring capabilities over the institution's third parties. Review the institution's policies, standards, and procedures related to the use of the following: …Contractual assurances from third-party service providers for security responsibilities, controls, and reporting. MGT.III.C.8:pg35: Third parties should support the responsibilities of their financial institution clients to adhere to all applicable laws, regulations, and supervisory guidance . MGT.III.C.8:pg35: When financial institution management contracts with third-party providers for some or all IT services, it should ensure that controls over outsourced activities provide the institution with the same level of assurance as controls over those activities performed in-house.
	Relationship Management/Contracts: Contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits. *Source:* IS.II.C.20:pg42: Management should oversee outsourced operations through the following: Contractual assurances for security responsibilities, controls, and reporting. IS.WP.6.31(c): Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. … Review the institution's policies, standards, and procedures related to the use of the following: Contractual assurances from third-party service providers for security responsibilities, controls, and reporting.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Relationship Management/Contracts: Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party. *Source:* IS.II.C.20:pg42: Management should verify that third-party service providers implement and maintain controls sufficient to appropriately mitigate risks. The institution's contracts should do the following: …Specify that the institution or an independent auditor has access to the service provider to perform evaluations of the service provider's performance against the Information Security Standards. IS.WP.6.31.e: Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. …Review the institution's policies, standards, and procedures related to the use of the following: Independent review of the third-party service provider's security through appropriate reports from audits and tests.
	Relationship Management/Contracts: Contracts identify the recourse available to the institution should the third party fail to meet defined security requirements. *Source:* OT.B.12: Institutions should include performance standards that define minimum service level requirements and remedies for failure to meet standards in the contract. OT.WP.I.3.4: Evaluate the process for entering into a contract with a service provider. Consider whether the contract contains adequate and measurable service level agreements.
	Relationship Management/Contracts: Contracts establish responsibilities for responding to security incidents. *Source:* IS.II.C.20:pg42: Management should oversee outsourced operations through the following: • Contractual assurances for security responsibilities, controls, and reporting. • Coordination of incident response policies and contractual notification requirements. • Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported. IS.WP.6.31(f) & (g): Review the institution's policies, standards, and procedures related to the use of the following: f. Coordination of incident response policies and contractual notification requirements. g. Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported.
	Relationship Management/Contracts: Contracts specify the security requirements for the return or destruction of data upon contract termination. *Source:* OT.B.15: The contract should establish notification and time frame requirements and provide for the timely return of the institution's data and resources in a machine-readable format upon termination. Any costs associated with conversion assistance should also be clearly stated.
	Relationship Management/Ongoing Monitoring: The third-party risk assessment is updated regularly. *Source:* OT.B.3: Factors institutions should consider include…tailoring the enterprise-wide, service provider monitoring program based on initial and ongoing risk assessments of outsourced services.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Relationship Management/Ongoing Monitoring: Audits, assessments, and operational performance reports are obtained and reviewed regularly validating security controls for critical third parties. *Source:* IS.II.C.20:pg42: Management should oversee outsourced operations through the following: …Independent review of the third party's security through appropriate reports from audits and tests. IS.WP.6.31.e: Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers…. Review the institution's policies, standards, and procedures related to the use of the following:…Independent review of the third-party service provider's security through appropriate reports from audits and tests. MGT.III.C.8:pg34 As part of a financial institution's third-party management program, management should ensure that third-party providers effectively provide support by doing the following: Reviewing results of independent audits of IT controls at third-party providers. MGT.WP.12.18: When reviewing information provided by the institution's third party providers, determine the quality of management's follow-up and resolution of customer concerns and problems with its third-party providers.
	Relationship Management/Ongoing Monitoring: Ongoing monitoring practices include reviewing critical third-parties' resilience plans. *Source:* OT.B.19: The program should monitor the service provider environment including its security controls, financial strength, and the impact of any external events. OT.WP.I.3.6: Evaluate the institution's process for monitoring the risk presented by the service provider relationship. Ascertain that monitoring addresses general control environment of the service provider through the receipt and review of appropriate audit and regulatory reports; service provider's disaster recovery program and testing; information security. MGT.WP.4.7.c: Determine whether management has an effective ongoing monitoring process of its third-party providers.
Domain 5 – Cyber Incident Management and Resilience	
	Incident Resilience Planning and Strategy/Planning: The institution has documented how it will react and respond to cyber incidents. *Source:* BCP.B.4: Business continuity planning involves the development of an enterprise-wide business continuity plan (BCP) and the prioritization of business objectives and critical operations that are essential for recovery…focused on the impact of various threats that could potentially disrupt operations rather than on specific events. BCP.WP.7.5: Determine the existence of an appropriate enterprise-wide BCP. BCP.WP.10: Determine whether the financial institution's and TSP's risk management strategies are designed to achieve resilience, such as the ability to effectively respond to wide-scale disruptions, including cyber attacks and attacks on multiple critical infrastructure sectors. MGT.III.C.3:pg29: Institution management should develop, implement, and periodically test incident response procedures, which should address escalation, remediation, and reporting of events and incidents. MGT.III.C.3(b):pg30: To address cybersecurity risk, the information security program should consider the following: Cyber incident management and resilience. MGT.WP.12.8.a: Determine whether a control structure includes: Developing and implementing processes to identify, protect against, detect, respond to, and recover from security events and incidents.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Incident Resilience Planning and Strategy/Planning: Communication channels exist to provide employees a means for reporting information security events in a timely manner. *Source:* IS.III:pg46: Management should establish defined processes and appropriate governance to facilitate the performance of security operations. Policies should address the timing and extent of the security operations activities, reporting, escalation triggers, and response actions. IS.WP.2.7: Determine whether security officers and employees know, understand, and are accountable for fulfilling their security responsibilities.
	Incident Resilience Planning and Strategy/Planning: Roles and responsibilities for incident response team members are defined. *Source:* IS.III.D:pg51: Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals…. IS.WP.8.6.e: Determine whether management has effective incident response processes, including the following:…Policies and procedures to guide the response, assigning responsibilities to individuals;…
	Incident Resilience Planning and Strategy/Planning: 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). *Source:* IS.III.D:pg52: Because of the wide range of technical and nontechnical issues posed by an intrusion, typical SIRT membership includes individuals with a wide range of backgrounds and expertise from different areas within the institution. Those areas include management, legal, and public relations, as well as IT staff. IS.WP.8.6.c: Determine whether management has effective incident response processes, including the following:…Appropriate balance of adequate people and technologies in the response.
	Incident Resilience Planning and Strategy/Planning: A formal backup and recovery plan exists for all critical business lines. *Source:* BCP.B.4: The business continuity planning process should include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components. BCP.WP.3.1: Determine whether the work flow analysis was performed to ensure that all departments and business processes are covered.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Incident Resilience Planning and Strategy/Planning: The institution plans to use business continuity, disaster recovery, and data back-up programs to recover operations following an incident. *Source:* IS.II.C.21:pg43: Business continuity plans should be reviewed as an integral part of the security process. Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution if continuity plans must be implemented. Management should train personnel regarding their security roles during a disaster. Additionally, management should update technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of the business continuity plan. IS.WP.6.34: Determine whether management effectively manages the following information security considerations related to business continuity planning. BCP.B.8: The risk assessment is the second step in the business continuity planning process. It should include: evaluating the business impact analysis (BIA) assumptions using various threat scenarios. BCP.WP.I.4: Determine whether appropriate risk management over the business continuity process is in place and if the financial institution's and TSP's risk management strategies consider wide-scale recovery scenarios designed to achieve industry-wide resilience.
	Incident Resilience Planning and Strategy/Testing: Scenarios are used to improve incident detection and response. *Source:* IS.II.C.21:pg43: Management should do the following:… Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios. BCP.B.J-13: Cyber threats will continue to challenge business continuity preparedness. Financial institutions should remain aware of emerging cyber threats and scenarios and consider their potential impact to operational resilience. BCP.WP.II.1.1: Determine whether the testing strategy addresses various event scenarios, including potential issues encountered during a wide-scale disruption.
	Incident Resilience Planning and Strategy/Testing: Business continuity testing involves collaboration with critical third parties. *Source*: BCP.B.J-6: Testing with third parties should disclose the adequacy of both organizations' ability to recover, restore, resume, and maintain operations after disruptions, consistent with business and contractual requirements. BCP.WP.I.9.3: Assess whether the third-party TSP's contract provides for the following elements to ensure business resiliency…Testing requirements with the TSP.
	Incident Resilience Planning and Strategy/Testing: Systems, applications, and data recovery is tested at least annually. *Source:* BCP.B.J-7: For critical services, annual or more frequent tests of the contingency plan are required. As with all BCP testing, the frequency should be driven by the financial institution's risk assessment, risk rating, and any significant changes to the operating environment. BCP.WP.I.11.4: Determine whether the testing strategy includes guidelines for the frequency of testing that are consistent with the criticality of business functions, recovery time objectives (RTOs), recovery point objectives (RPOs), and recovery of the critical path, as defined in the business impact analysis (BIA) and risk assessment, corporate policy, and regulatory guidelines.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Detection, Response & Mitigation/Detection: Alert parameters are set for detecting information security incidents that prompt mitigating actions. *Source:* IS.II.C.15(a):pg32: To prevent unauthorized access to or inappropriate activity on the operating system and system utilities, management should do the following:…Filter and review logs for potential security events and provide adequate reports and alerts. IS.II.C.15(b):pg33: Management should implement effective application access controls by doing the following:…Logging access and events, defining alerts for significant events, and developing processes to monitor and respond to anomalies and alerts. IS.WP.6.21.f: As part of management's process to secure the operating system and all system components, determine whether management does the following:…Filters and reviews logs for potential security events and provides adequate reports and alerts. IS.WP.6.22.f: Determine whether management controls access to applications. Review whether management does the following:…Logs access and events, defines alerts for significant events, and develops processes to monitor and respond to anomalies and alerts.
	Detection, Response & Mitigation/Detection: System performance reports contain information that can be used as a risk indicator to detect information security incidents. *IS.II.D:pg45: Risk reporting is a process that produces information systems reports that address threats, capabilities, vulnerabilities, and inherent risk changes. Risk reporting should describe any information security events that the institution faces and the effectiveness of management's response and resilience to those events*. IS.WP.7.1: Determine whether the institution has risk monitoring and reporting processes that address changing threat conditions in both the institution and the greater financial industry. Determine whether these processes address information security events faced by the institution, the effectiveness of management's response, and the institution's resilience to those events.
	Detection, Response & Mitigation/Detection: Tools and processes are in place to detect, alert, and trigger the incident response program. *Source:* IS.III.D:pg50: The institution's program should have defined protocols to declare and respond to an identified incident. IS.WP.8.6.a: Determine whether management has effective incident response processes, including the following: Protocols defined in the incident response policy to declare and respond to an incident once identified.
	Detection, Response & Mitigation/Response and Mitigation: Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information. *Source:* IS.III.D:pg52: While containment strategies between institutions can vary, they typically include the following broad elements: Isolation of compromised systems or enhanced monitoring of intruder activities. Search for additional compromised systems. Collection and preservation of evidence. Communication with affected parties and often the primary regulator, information-sharing organizations (e.g., FS-ISAC), or law enforcement. IS.WP.8.6.b: Determine whether management has effective incident response processes, including the following: Procedures to minimize damage through the containment of the incident, restoration of systems, preservation of data and evidence, and notification, as appropriate, to customers and others as needed.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Escalation and Reporting/Escalation and Reporting: A process exists to contact personnel who are responsible for analyzing and responding to an incident. *Source:* IS.III.C:pg50: Escalation policies should address when different personnel within the organization will be contacted and the responsibility those personnel have in incident analysis and response. IS.WP.8.5.h: Determine whether management has effective incident identification and assessment processes to do the following: Develop procedures to test the incident escalation, response, and reporting processes. MGT.WP.2.8.f: Determine whether management establishes a formal process to obtain, analyze, and respond to information on threats and vulnerabilities by developing a repeatable threat intelligence and collaboration program.
	Escalation and Reporting/Escalation and Reporting: 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. *Source:* IS.III.D:pg51: Additionally, management should define thresholds for reporting significant security incidents, and consider developing processes for when the institution should notify its regulators of incidents that may affect the institution's operations, reputation, or sensitive customer information. IS.III.D:pg51: Protocols to define when and under what circumstances to notify and involve regulators, customers, and law enforcement, including names and contact information for each group. IS.WP.8.6.f: Determine whether management has effective incident response processes, including the following: Thresholds for reporting significant security incidents and processes to notify, as appropriate, the institution's regulators of those incidents that may affect the institution or the financial system. MGT.III.C.3:pg29: Develop a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulator based on thresholds defined by the financial institution and applicable legal requirements. Relevant thresholds could include significant financial impact, significant operational downtime, operational or system breach, or loss of critical infrastructure. MGT.WP.2.2.f: Review whether the board approves a policy to escalate and report significant security incidents to the board, steering committee, government agencies, and law enforcement, as appropriate.
	Escalation and Reporting/Escalation and Reporting: The institution prepares an annual report of security incidents or violations for the board or an appropriate board committee. *Source:* IS.I.B:pg4: Management should provide a report to the board at least annually that describes the overall status of the program and material matters related to the program, including the following:…Security breaches or violations of law or regulation and management's responses to such incidents. IS.WP.2.4.e:...Determine whether the report to the board describes the overall status of the information security program and discusses material matters related to the program such as the following:… Security breaches or violations and management's responses.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Escalation and Reporting/Escalation and Reporting: Incidents are classified, logged, and tracked. *Source:* OPS.B.28: Event/problem management plans should cover hardware, operating systems, applications, and security devices and should address at a minimum: event/problem identification and rating of severity based on risk; event/problem impact and root cause analysis; documentation and tracking of the status of identified problems; the process for escalation; event/problem resolution; management reporting. OPS.WP.10.1: Describe and assess the event/problem management program's ability to identify, analyze, and resolve issues and events.

Explanation of FFIEC IT Examination Handbook References

Each statement from the FFIEC IT Examination Handbook has a unique identifier that begins with the document, followed by the section.

Below is a list of the unique identifiers used to reference the all the documents and the sections in the older references.

Document	Section
Audit (AUD)	Work Program (WP) or Booklet (B) for older references or Chapter.section.sub-section for Information Security and Management Booklets
Business Continuity Planning (BCP)	
Development and Acquisition (D&A)	
Information Security (IS)	
Management (MGT)	
Operations (OPS)	
Outsourcing Technology Services	
Retail Payment Systems (RPS)	
Wholesale Payment Systems (WPS)	

Older references:
If it is a booklet, then the page number is listed. If it is from a work program, the tier, objective reference, and statement number is listed. Each portion of the unique identifier is separated by a period.

Therefore, if the reference is from the Audit Booklet page 15, it is referenced as "AUD.B.15."

If the reference is from the Business Continuity Planning Work Program Tier I, Objective 4, statement 10, it is referenced as "BCP.WP.I.4.10."

Newer references (Information Security and Management Booklets**):**
If it is from a booklet, then the booklet Chapter, Section and Sub-Section are list, followed by the page number. Chapter, Section and Sub-Section are separated by a period, Page number is separated by colons.

Therefore, if the reference is from the Information Security Booklet, Chapter I. Governance of the Information Security Program, Section B. Responsibility and Accountability, page 4. It is referenced as "IS.I.B:pg4:"

If the reference is from the Management Work Program, Objective 4, Statement 3, it is referenced as "MGT.WP.4.3:"