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.B.3:* Financial institutions should implement an ongoing security process and institute appropriate governance for the security function, assigning clear and appropriate roles and responsibilities to the board of directors, management, and employees. *Additional reference:*[1] *Information Security and Management Booklets.*
	Governance/Oversight: Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. *Source: IS.B.6:* Senior management should clearly support all aspects of the information security program… participate in assessing the effect of security issues on the financial institution and its business lines and processes.
	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.B.5:* The board should approve written information security policies and the written report on the effectiveness of the information security program at least annually. ** Information Security, Management*
	Governance/Oversight: The budgeting process includes information security related expenses and tools. *Source: EB.B.20:* Financial institutions should base any decision to implement e-banking products and services on a thorough analysis of the costs and benefits associated with such action. The individuals conducting the cost-benefit analysis should clearly understand the risks associated with e-banking so that cost considerations fully incorporate appropriate risk mitigation controls. *EB.WP.2.2:* Determine the adequacy of board and management oversight of e-banking activities with respect to strategy, planning, management reporting, and audit. Determine whether e-banking guidance and risk considerations have been incorporated into the institution's operating policies to an extent appropriate for the size of the financial institution and the nature and scope of its e-

[1] Other IT Examination Handbook booklets serve as additional reference – this is noted with an asterisk.

Yes/No	FFIEC Cybersecurity Assessment Tool
	banking activities.
	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.B.3:* The Information Security Strategy (plan to mitigate risk that integrates technology, policies, procedures, and training) should be reviewed and approved by the board of directors. *IS.WP.I.3.2:* Determine whether the risk assessment provides adequate support for the security strategy, controls, and monitoring that the financial institution has implemented. *IS.WP.II.L.1:* Obtain an understanding of the data security strategy (approach to protecting data, risk assessment, policies and procedures, and review data sensitivity/update assessments). * *Management*
	Governance/Strategy-Policies: The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management. *Source: IS.B.16:* Institutions generally should establish defenses that address the network and application layers at external connections, whether from the Internet or service providers. *IS.WP.I.3:* Determine the adequacy of the risk assessment process. *IS.WP.I.6:* Determine the adequacy of security monitoring.
	Governance/Strategy-Policies: The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing. *Source: EB.B.28:* Each financial institution with external connectivity should ensure the following controls exist internally or at their TSP. Financial institutions should maintain an ongoing awareness of attack threats through membership in information-sharing entities such as the Financial Services - Information Sharing and Analysis Center (FS-ISAC), Infragard, the CERT Coordination Center, private mailing lists, and other security information sources. *EB.WP.4.2:* Discuss the institution's e-banking environment with management as applicable.
	Governance/Strategy-Policies: The institution has board-approved policies commensurate with its risk and complexity that address information security. *Source: IS.B.16:* Financial institutions are required to establish an information security program that meets the requirements of the 501(b) guidelines. Information security policies and procedures are some of the institution's measures and means by which the objectives of the information security program are achieved. *IS.WP.I.4:* Evaluate the adequacy of security policies and standards relative to the risk to the institution.

Yes/No	FFIEC Cybersecurity Assessment Tool
	** Operations, Wholesale Payments, Retail Payments*
	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. ** E-Banking*
	Governance/Strategy-Policies: The institution has policies commensurate with its risk and complexity that address the concepts of incident response and resilience. *Source: IS.B.83:* The security response center should be governed by policies and procedures that address security incidents. *IS.WP.II.M.15:* Evaluate the appropriateness of the security policy in addressing the review of compromised systems. ** E-Banking, Operations*
	Governance/Strategy-Policies: All elements of the information security program are coordinated enterprise-wide. *Source: IS.B.7:* 12 CFR 30 II.A. "Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated." *IS.WP.I.7.3:* Evaluate the effectiveness of enterprise-wide security administration. Review security guidance and training provided to ensure awareness among employees and contractors, including annual certification that personnel understand their responsibilities. ** E-Banking, Management, Operations, Wholesale Payments*
	Governance/IT Asset Management: An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. *Source: IS.B.9:* A risk assessment should include an identification of information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information and information systems can be both paper-based and electronic-based. *IS.WP.I.3.1:* Consider whether the institution has identified and ranked information assets (e.g., data, systems, physical locations) according to a rigorous and consistent methodology that considers the risks to customer non-public information as well as the risks to the institution. ** E-Banking, Management, Operations*
	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.B.12:* Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation. *IS.WP.II.M.22:* Determine whether an effective process exists to respond in an appropriate and timely manner to newly discovered vulnerabilities.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Governance/IT Asset Management: Management assigns accountability for maintaining an inventory of organizational assets. *Source: IS.B.9:* A risk assessment should include an identification of information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information and information systems can be both paper-based and electronic-based. *IS.WP.I.3.1:* Consider whether the institution has identified and ranked information assets (e.g., data, systems, physical locations) according to a rigorous and consistent methodology that considers the risks to customer non-public information as well as the risks to the institution.
	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.B.56:* Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. *IS.WP.I.4.1:* Review and evaluate security policies and standards to ensure that they sufficiently address the following area when considering the risks identified by the institution: software development and acquisition, including processes that evaluate the security features and software trustworthiness of code being developed or acquired, as well as change control and configuration management. ** Operations, Wholesale Payments*
	Risk Management/Risk Management Program: An information security and business continuity risk management function(s) exists within the institution. *Source: IS.B.68:* Policies regarding media handling, disposal, and transit should be implemented to enable the use of protection profiles and otherwise mitigate risks to data. *IS.WP.I.4:* Evaluate the adequacy of security policies and standards relative to the risk to the institution. Physical controls over access to hardware, software, storage media, paper records, and facilities. Media handling procedures and restrictions, including procedures for securing, transmitting and disposing of paper and electronic information.
	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.B.8:* Risk managers should incorporate security issues into their risk assessment process for each risk category. Financial institutions should ensure that security risk assessments adequately consider potential risk in all business lines and risk categories. An adequate risk assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities. *IS.WP.I.3.1:* Determine the adequacy of the risk assessment process. Review the risk assessment to determine whether the institution has characterized its systems properly and assessed the risks to information assets. ** Information Security, E-Banking, Operations, Wholesale Payments, Outsourcing, Retail Payments*
	Risk Management/Risk Assessment: The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls. *Source: IS.B.12:* Prioritizes the risks present due to threats and vulnerabilities to determine the

Yes/No	FFIEC Cybersecurity Assessment Tool
	appropriate level of training, controls, and assurance necessary for effective mitigation. *IS.WP.II.M.22:* Determine whether an effective process exists to respond in an appropriate and timely manner to newly discovered vulnerabilities. ** E-Banking, Management, Wholesale Payments, Outsourcing, Retail Payments*
	Risk Management/Risk Assessment: The risk assessment is updated to address new technologies, products, services, and connections before deployment. *Source: IS.B.13:* Risk assessments should be updated as new information affecting information security risks is identified (e.g., a new threat, vulnerability, adverse test result, hardware change, software change, or configuration change). *IS.WP.I.3.3:* Determine the adequacy of the risk assessment process. ** Information Security, E-Banking, Management, Wholesale Payments*
	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. ** E-Banking, Management, Operations, Retail Payments*
	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.
	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.B.6:* The annual approval should consider the results of management assessments and reviews, internal and external audit activity related to information security, third-party reviews of the information security program and information security measures, and other internal or external reviews designed to assess the adequacy of information security controls. *IS.WP.II.L.2:* Review audit and security review reports that summarize if data is protected consistent with the risk assessment. *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.
	Resources/Staffing: Information security roles and responsibilities have been identified. *Source: IS.B.7:* Employees should know, understand, and be held accountable for fulfilling their security responsibilities. Financial institutions should define these responsibilities in their security

Yes/No	FFIEC Cybersecurity Assessment Tool
	policy. ** Information Security, E-Banking, Management*
	Resources/Staffing: Processes are in place to identify additional expertise needed to improve information security defenses. *Source: IS.WP.I.2.8:* Determine the size and quality of the institution's security staff. Consider … adequacy of staffing levels and impact of any turnover.
	Training and Culture/Training: Annual information security training is provided. *Source: IS.B.66:* Providing training to support awareness and policy compliance. *IS.WP.I.7.3:* Review security guidance and training provided to ensure awareness among employees and contractors, including annual certification that personnel understand their responsibilities. ** E-Banking, Operations*
	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.B.66:* Providing training to support awareness and policy compliance… Training should also address social engineering and the policies and procedures that protect against social engineering attacks. *IS.WP.I.7.3:* Review security guidance and training provided to ensure awareness among employees and contractors, including annual certification that personnel understand their responsibilities. ** Operations*
	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.B.7:* Ensure an effective information security awareness program has been implemented throughout the organization. *IS.WP.I.7.3:* Review security guidance and training provided to ensure awareness among employees and contractors, including annual certification that personnel understand their responsibilities.
	Training and Culture/Training: Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials). *Source: EB.WP.6.3:* Review the Web site content for inclusion of the following information which institutions should consider to avoid customer confusion and communicate customer responsibilities … Security policies and customer usage responsibilities (including security disclosures and Internet banking agreements).
	Training and Culture/Culture: Management holds employees accountable for complying with the information security program. *Source: IS.B.7:* Employees should know, understand, and be held accountable for fulfilling their security responsibilities. Financial institutions should define these responsibilities in their security policy**.** ** Information Security, Management*

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: EB.B.28:* Financial institutions should maintain an ongoing awareness of attack threats through membership in information-sharing entities such as the Financial Services - Information Sharing and Analysis Center (FS-ISAC), Infragard, the CERT Coordination Center, private mailing lists, and other security information sources. *IS.B.83:* Sources of external threat information include industry information sharing and analysis centers (ISACs), Infragard, mailing lists, and commercial reporting services. *IS.WP.I.6.3:* Information should include external information on threats and vulnerabilities (ISAC and other reports) and internal information related to controls and activities.
	Threat Intelligence/Threat Intelligence and Information: Threat information is used to monitor threats and vulnerabilities. *Source: IS.B.83:* The security response center should consider, evaluate, and respond to both external threats and internal vulnerabilities. Sources of external threat information include industry information sharing and analysis centers (ISACs), Infragard, mailing lists, and commercial reporting services. *IS.WP.I.6.1:* Evaluate the adequacy of information used by the security response center. Information should include external information on threats and vulnerabilities (ISAC and other reports) and internal information related to controls and activities.
	Threat Intelligence/Threat Intelligence and Information: Threat information is used to enhance internal risk management and controls. *Source: IS.B.4:* Security Process Monitoring and Updating …. This information is used to update the risk assessment, strategy, and controls. *IS.WP.I.3.3:* Evaluate the risk assessment process for the effectiveness of the following key practices: multidisciplinary and knowledge-based approach; systematic and centrally controlled; integrated process; accountable activities; documented; knowledge enhancing; and regularly updated.
	Monitoring and Analyzing/Monitoring and Analyzing: Audit log records and other security event logs are reviewed and retained in a secure manner. *Source: IS.B.79:* Institutions should strictly control and monitor access to log files whether on the host or in a centralized logging facility. *IS.WP.II.B.13:* Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period and that reporting to those logs is adequately protected. ** E-Banking, Operations, Retail Payments*
	Monitoring and Analyzing/Monitoring and Analyzing: Computer event logs are used for investigations once an event has occurred. *Source: IS.B.83:* Because the identification of incidents requires monitoring and management, response centers frequently use SIM (security information management) tools to assist in the data collection, analysis, classification, and reporting of activities related to security incidents.

Yes/No	FFIEC Cybersecurity Assessment Tool
	IS.WP.II.G.7: Determine whether appropriate logs are maintained and available to support incident detection and response efforts.
	Information Sharing/Information Sharing: Information security threats are gathered and shared with applicable internal employees. *Source: IS.B.83:* Reporting policies should address internal and external reporting. *IS.WP.I.6.4:* Obtain and evaluate the policies governing security response center functions, including monitoring, classification, escalation, and reporting.
	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.
	Information Sharing/Information Sharing: Information about threats is shared with law enforcement and regulators when required or prompted. *Source: IS.B.84:* Preparation … involves defining the policies and procedures that guide the response, assigning responsibilities to individuals, providing appropriate training, formalizing information flows, and selecting, installing, and understanding the tools used in the response effort. Key considerations …include… When and under what circumstances to notify and involve regulators, customers, and law enforcement. This consideration drives certain monitoring decisions, decisions regarding evidence gathering and preservation, and communications considerations.
Domain 3 – Cybersecurity Controls	
	Preventive Controls/Infrastructure Management: Network perimeter defense tools (e.g., border router and firewall) are used. *Source: IS.B.33:* Typical perimeter controls include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as domain name service (DNS). Institutions internally hosting Internet-accessible services should consider implementing additional firewall components that include application-level screening. *IS.WP.I.4.1:* Evaluate the appropriateness of technical controls mediating access between security domains. ** Information Security, E-Banking, Operations, Wholesale Payments*
	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.B.46:* Management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems. *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. *IS.WP.I.4:* Review security policies and standards to ensure that they sufficiently address the following areas when considering the risks identified by the institution…. Network Access - Remote

Yes/No	FFIEC Cybersecurity Assessment Tool
	Access Controls (including wireless, virtual private network [VPN], modems, and Internet-based). *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. ** E-Banking, Wholesale Payments*
	Preventive Controls/Infrastructure Management: All ports are monitored. *Source: IS.B.50:* Institutions should consider securing PCs to workstations, locking or removing disk drives and unnecessary physical ports, and using screensaver passwords or automatic timeouts.
	Preventive Controls/Infrastructure Management: Up-to-date anti-virus and anti-malware tools are used. *Source: IS.B.78:* Host-based intrusion detection systems are recommended by the NIST for all mission-critical systems, even those that should not allow external access. *IS.WP.II.M.9:* Determine whether appropriate detection capabilities exist related to… anti-virus, anti-spyware, and other malware identification alerts. ** Outsourcing*
	Preventive Controls/Infrastructure Management: Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced. *Source: IS.B.56:* Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. *IS.WP.II.H:* Determine whether management explicitly follows a recognized security standard development process, or adheres to widely recognized industry standards. ** E-Banking, Operations, Wholesale Payments, Outsourcing*
	Preventive Controls/Infrastructure Management: Ports, functions, protocols and services are prohibited if no longer needed for business purposes. *Source: IS.B.50:* Institutions should consider securing PCs to workstations, locking or removing disk drives and unnecessary physical ports, and using screensaver passwords or automatic timeouts. *IS.WP.II.C.1:* Determine whether hosts are hardened through the removal of unnecessary software and services, consistent with the needs identified in the risk assessment, that configuration takes advantage of available object, device, and file access controls, and that necessary software updates are applied.
	Preventive Controls/Infrastructure Management: Access to make changes to systems configurations, (including virtual machines and hypervisors) is controlled and monitored. *Source: IS.B.56:* Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. The steps include… Maintaining appropriately robust configuration management and change control processes. *IS.WP.II.H:* Determine whether management explicitly follows a recognized security standard development process, or adheres to widely recognized industry standards. ** E-Banking, Operations, Wholesale Payments, Outsourcing*

Yes/No	FFIEC Cybersecurity Assessment Tool
	Preventive Controls/Infrastructure Management: Programs that can override system, object, network, virtual machine, and application controls are restricted. *Source: IS.B.41:* Financial institutions should secure access to the operating systems of all system components by…Securing access to system utilities. *IS.WP.II.B.4:* Determine whether effective procedures and practices are in place to secure network services, utilities, and diagnostic ports, consistent with the overall risk assessment.
	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.B.23:* Controls against these attacks are account lockout mechanisms, which commonly lock out access to the account after a risk-based number of failed login attempts. *IS.WP.II.A.4:* Evaluate the effectiveness of password and shared-secret administration for employees and customers considering the complexity of the processing environment and type of information accessed. ** E-Banking, Wholesale Payments*
	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.B.40:* If a financial institution uses a wireless network, it should carefully evaluate the risk and implement appropriate additional controls. *IS.WP.I.4.1:* Determine whether appropriate device and session authentication takes place, particularly for remote and wireless machines.
	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.B.19:* Access rights should be based upon the needs of the applicable user to carry out legitimate and approved activities on the financial institution's information systems. *IS.WP.I.4.1:* Review security policies and standards to ensure that they sufficiently address administration of access rights at enrollment, when duties change, and at employee separation.
	Preventive Controls/Access and Data Management: Employee access to systems and confidential data provides for separation of duties. *Source: IS.B.19:* Access rights should be based upon the needs of the applicable user to carry out legitimate and approved activities on the financial institution's information systems. *IS.WP.I.4.1:* Review security policies and standards to ensure that they sufficiently address administration of access rights at enrollment, when duties change, and at employee separation.
	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.B.19:* Authorization for privileged access should be tightly controlled. *IS-WP-II-A.1:* Determine whether access to system administrator level is adequately controlled and monitored. ** E-Banking, Operations, Wholesale Payments, Outsourcing*

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.B.18:* Reviewing periodically users' access rights at an appropriate frequency based on the risk to the application or system. *IS.WP.I.7.6:* Evaluate the process used to monitor and enforce policy compliance (e.g., granting and revocation of user rights). ** Wholesale Payments*
	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.B.18:* Financial institutions should have an effective process to administer access rights including: assigning users and devices only the access required to perform their required functions and updating access rights based on personnel or system changes. *IS.WP.I.4.1:* Review security policies and standards to ensure that they sufficiently address administration of access rights at enrollment, when duties change, and at employee separation. ** Information Security, Wholesale Payments*
	Preventive Controls/Access and Data Management: Identification and authentication are required and managed for access to systems, applications, and hardware. *Source: IS.B.21:* Financial institutions should use effective authentication methods appropriate to the level of risk by…selecting authentication mechanisms based on the risk associated with the particular application or services. *IS-WP-II-A.3:* Authentication - Evaluate whether the authentication method selected and implemented is appropriately supported by a risk assessment. ** Information Security, E-Banking, Operations, Wholesale Payments, Retail Payments*
	Preventive Controls/Access and Data Management: Access controls include password complexity and limits to password attempts and reuse. *Source: IS.B.66:* Financial institutions should control and protect access to paper, film and computer-based media to avoid loss or damage. *IS-WP-II-A.4:* Evaluate the effectiveness of password and shared-secret administration… Password composition in terms of length and type of characters (new or changed passwords should result in a password whose strength and reuse agrees with the security policy). ** Wholesale Payments*
	Preventive Controls/Access and Data Management: All default passwords and unnecessary default accounts are changed before system implementation. *Source: IS.B.61:* When deploying off-the-shelf software, management should harden the resulting system. Hardening includes the following actions… Changing all default passwords. *IS.WP.II.A.1:* Determine whether the financial institution has removed or reset default profiles and passwords from new systems and equipment. ** Wholesale Payments*
	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

Yes/No	FFIEC Cybersecurity Assessment Tool
	with the risk. *Source: IS.B.21:* Considering whether multi-factor authentication is appropriate for each application, taking into account that multi-factor authentication is increasingly necessary for many forms of electronic banking and electronic payment activities. *IS.WP.II.A.3:* Evaluate whether the authentication method selected and implemented is appropriately supported by a risk assessment. ** Information Security, E-Banking, Wholesale Payments, Retail Payments*
	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.B.64:* Isolated software libraries should be used for the creation and maintenance of software. Typically, separate libraries exist for development, test, and production. *IS.WP.II.H.6:* Evaluate the adequacy of the change control process.
	Preventive Controls/Access and Data Management: Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems. *Source: IS.B.47:* Financial institutions should define physical security zones and implement appropriate preventative and detective controls in each zone to protect against risks. *IS.WP.I.4.1:* Evaluate the adequacy of security policies and standards relative to…physical controls over access to hardware, software, storage media, paper records, and facilities. ** E-Banking, Operations, Wholesale Payments, Retail Payments*
	Preventive Controls/Access and Data Management: All passwords are encrypted in storage and in transit. *Source: IS.B.21:* Encrypting the transmission and storage of authenticators (e.g., passwords, personal identification numbers (PINs), digital certificates, and biometric templates).
	Preventive Controls/Access and Data Management: Confidential data are encrypted when transmitted across public or untrusted networks (e.g., Internet). *Source: IS.B.51:* Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. *IS.WP.II.B.15:* Determine whether appropriate controls exist over the confidentiality and integrity of data transmitted over the network (e.g., encryption, parity checks, message authentication). ** E-Banking, Operations, Wholesale Payments, Outsourcing, Retail Payments*
	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.B.51:* Financial institutions should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit. *IS.WP.II.K.1:* Review the information security risk assessment and identify those items and areas classified as requiring encryption.
	Preventive Controls/Access and Data Management: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Source: IS.B.45: Financial institutions should secure remote access to and from their systems… securing remote access devices, and using strong authentication and encryption to secure communications. *IS.WP.II.B.17:* Determine whether remote access devices and network access points for remote equipment are appropriately controlled. For example, authentication is of appropriate strength (e.g., two-factor for sensitive components); and remote access devices are appropriately secured and controlled by the institution. ** Information Security, Operations*
	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.B.25:* Examples of Acceptable Use Policy (AUP) elements for internal network and stand-alone users include… hardware and software changes the user can make to their access device. *IS.WP.II.D.3:* Determine whether adequate inspection for, and removal of, unauthorized hardware and software takes place.
	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.B.19:* Customers may be granted access based on their relationship with the institution. *IS.WP.II.A.3:* Evaluate whether the authentication method selected and implemented is appropriately supported by a risk assessment.
	Preventive Controls/Access and Data Management: Data are disposed of or destroyed according to documented requirements and within expected time frames. *Source: IS.B.66:* Financial institutions should control and protect access to paper, film and computer-based media to avoid loss or damage. Institutions should … ensure safe and secure disposal of sensitive media. *IS.WP.I.4:* Evaluate the adequacy of security policies and standards relative to the risk to the institution. Physical controls over access to hardware, software, storage media, paper records, and facilities. Media handling procedures and restrictions, including procedures for securing, transmitting and disposing of paper and electronic information. ** Information Security, Operations*
	Preventive Controls/Device-End Point Security: Controls are in place to restrict the use of removable media to authorized personnel. *Source: IS.WP.I.4.1:* Review security policies and standards to ensure that they sufficiently address the following areas when considering the risks identified by the institution… Media handling procedures and restrictions.
	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.B.56:* Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. *IS.WP.II.H.2:* Determine whether management explicitly follows a recognized security standard development process, or adheres to widely recognized industry standards.

Yes/No	FFIEC Cybersecurity Assessment Tool
	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.B.59:* Ongoing risk assessments should consider the adequacy of application level controls in light of changing threat, network, and host environments. *IS.WP.III.H.8:* Inquire about the method used to test the newly developed or acquired software for vulnerabilities.
	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.
	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: IS.B.61:* Hardening includes the following actions… Testing the system to ensure a secure configuration… [and] Testing the resulting systems. *IS.WP.II.M.12:* Evaluate independent tests, including penetration tests, audits, and assessments.
	Detective Controls/Threat and Vulnerability Detection: Anti-virus and anti-malware tools are used to detect attacks. *Source: IS.B.55:* Typical controls to protect against malicious code use technology, policies and procedures, and training, all applied in a layered manner from perimeters inward to hosts and data. The controls are of the preventative and detective/corrective variety. *IS.WP.I.4.1:* Review security policies and standards to ensure that they sufficiently address [Malicious Code Prevention] when considering the risks identified by the institution. ** E-Banking*
	Detective Controls/Threat and Vulnerability Detection: Firewall rules are audited or verified at least quarterly.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Source: IS.B.82: Firewall policies and other policies addressing access control between the financial institution's network and other networks should be audited and verified at least quarterly. *IS.WP.II.B.10:* Confirm that routing tables are regularly reviewed for appropriateness on a schedule commensurate with risk.
	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.B.39:* Enforcement of malicious code filtering is through anti-virus, anti-spyware, and anti-spam filtering, the blocking of downloading of executable files, and other actions. *IS.WP.II.B.10:* Confirm that malicious code is effectively filtered.
	Detective Controls/Anomalous Activity Detection: The institution is able to detect anomalous activities through monitoring across the environment. *Source: IS.B.32:* Financial institutions should secure access to their computer networks through multiple layers of access controls to protect against unauthorized access. Institutions should…monitor cross-domain access for security policy violations and anomalous activity.
	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.
	Detective Controls/Anomalous Activity Detection: Logs of physical and/or logical access are reviewed following events. *Source: IS.B.73:* Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by… Monitoring network and host activity to identify policy violations and anomalous behavior. *IS.WP.II.M.1:* Review security procedures for report monitoring to identify unauthorized or unusual activities.
	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.B.19:* Authorization for privileged access should be tightly controlled. *IS-WP-II-A.1:* Determine whether access to system administrator level is adequately controlled and monitored. ** E-Banking, Operations, Wholesale Payments, Outsourcing*
	Detective Controls/Event Detection: A normal network activity baseline is established. *Source: IS.B.77:* The behavior-based anomaly detection method creates a statistical profile of normal activity on the host or network. Normal activity generally is measured based on the volume of traffic, protocols in use, and connection patterns between various devices.

Yes/No	FFIEC Cybersecurity Assessment Tool
	IS-WP-II-M: Determine whether appropriate detection capabilities exist related to network-related anomalies. ** E-Banking*
	Detective Controls/Event Detection: Mechanisms (e.g., anti-virus alerts, log event alerts) are in place to alert management to potential attacks. *Source: IS.B.78:* Host intrusion detection systems (hIDSs) include anti-virus and anti-spyware programs… Host-based intrusion detection systems are recommended by the NIST for all mission-critical systems, even those that should not allow external access
	Detective Controls/Event Detection: Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. *Source: IS.WP.II.M.9:* Determine whether appropriate detection capabilities exist.
	Detective Controls/Event Detection: Responsibilities for monitoring and reporting suspicious systems activity have been assigned. *Source: IS.B.83:* The responsibility and authority of security personnel and system administrators for monitoring should be established, and the tools used should be reviewed and approved by appropriate management with appropriate conditions for use. *IS.WP.II.M.15:* Evaluate the appropriateness of the security policy in addressing the review of compromised systems. Consider documentation of the roles, responsibilities and authority of employees and contractors.
	Detective Controls/Event Detection: The physical environment is monitored to detect potential unauthorized access. *Source: IS.B.47:* Implement appropriate preventative and detective controls to protect against physical penetration by malicious or unauthorized people, damage from environmental contaminants, and electronic penetration through active or passive electronic emissions.
	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.B.62:* Software support should incorporate a process to update and patch operating system and application software for new 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. *IS.WP.II.C.3:* Determine whether adequate processes exist to apply host security updates, such as patches and anti-virus signatures, and that such updating takes place. *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

Yes/No	FFIEC Cybersecurity Assessment Tool
	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.
	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.B.87:* Senior management should require periodic self-assessments to provide an ongoing assessment of policy adequacy and compliance and ensure prompt corrective action of significant deficiencies. *IS.WP.I.6.9:* Determine the timeliness of identification of vulnerabilities and anomalies, and evaluate the 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.B.9:* The institution's system architecture diagram should include a system characterization and data flow analysis of networks (where feasible), computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems. *IS.WP.I.2.3:* Determine the extent of network connectivity internally and externally, and the boundaries and functions of security domains. * *Operations*
	Connections/Connections: The institution ensures that third-party connections are authorized. *Source: IS.B.17:* The selection of where to put which control is a function of the risk assessment. Institutions generally should establish defenses that address the network and application layers at external connections, whether from the Internet or service providers. *IS.WP.II.B.2:* Evaluate controls that are in place to install new or change existing network infrastructure and to prevent unauthorized connections to the financial institution's network.
	Connections/Connections: A network diagram is in place and identifies all external connections. *Source: IS.B.9:* The institution's system architecture diagram and related documentation should identify service provider relationships, where and how data is passed between systems, and the relevant controls that are in place. *IS.WP.I.2.3:* Determine the extent of network connectivity internally and externally, and the boundaries and functions of security domains. * *Operations*
	Connections/Connections: Data flow diagrams are in place and document information flow to external parties. *Source: IS.B.10:* Financial institutions outsourcing strategy also should be considered in identifying relevant data flows and information processing activities. The financial institution's system architecture diagram and related documentation should identify service provider relationships,

Yes/No	FFIEC Cybersecurity Assessment Tool
	where and how data is passed between systems, and the relevant controls that are in place. *IS.B.1.3:* Identify changes to the technology infrastructure or new products and services that might increase the institution's risk from information security issues. Consider…network topology including changes to configuration or components. ** E-Banking*
	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.B.69:* Financial institutions should exercise their security responsibilities for outsourced operations through appropriate due diligence in service provider research and selection. *IS.WP.I.5:* Evaluate the sufficiency of security-related due diligence in service provider research and selection. ** Operations, Outsourcing, E-Banking, Retail Payments*
	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.
	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.
	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.B.7:* Management also should consider and monitor the roles and responsibilities of external parties. The security responsibilities of technology service providers (TSPs), contractors, customers, and others who have access to the institution's systems and data should be clearly delineated and documented in contracts. *IS.WP.I.5.2:* Evaluate the security-related controls embedded in vendor management. Evaluate the adequacy of contractual assurances regarding security responsibilities, controls, and reporting. ** Outsourcing, E-Banking, Retail Payments*
	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.

Yes/No	FFIEC Cybersecurity Assessment Tool
	Source: IS.B.12: An institution's contract with the service provider should contain language that establishes standards the service provider should meet and provide for periodic reporting against those standards. ** E-Banking, Retail Payments*
	Relationship Management/Contracts: Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party. *Source: IS.B.12:* The contract should include a provision for the independent review of internal controls at service providers and vendors, require that timely action be taken to address identified vulnerabilities, and require a reporting to the institution of the review, its findings, and the actions taken in response to the findings. *IS.WP.I.5.4:* Determine that the scope, completeness, frequency, and timeliness of third-party audits and tests of the service provider's security are supported by the financial institution's risk assessment. ** Audit, Outsourcing*
	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. ** Retail Payments*
	Relationship Management/Contracts: Contracts establish responsibilities for responding to security incidents. *Source: EB.B.22:* The board and senior management must provide effective oversight of third-party vendors providing e-banking services and support. Effective oversight requires that institutions ensure the following practices are in place…Monitoring reports and expectations including incidence response and notification. ** Retail Payments*
	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. ** Information Security, Audit, E-Banking*
	Relationship Management/Ongoing Monitoring: Audits, assessments, and operational performance reports are obtained and reviewed regularly validating security controls for critical third parties. *Source: IS.B.86:* Where indicated by the institution's risk assessment, management is responsible

Yes/No	FFIEC Cybersecurity Assessment Tool
	for monitoring the service provider's activities through review of timely audits and test results or other equivalent evaluations. *IS.WP.II.J.2-4:* Determine whether the institution has assessed the service provider's ability to meet contractual security requirements. Determine whether appropriate security testing is required and performed on any code, system, or service delivered under the contract. ** Outsourcing, E-Banking, Retail Payments*
	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.
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. ** E-Banking*
	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.B.83:* Reporting policies should address internal and external reporting, including coordination with service providers and reporting to industry ISACs. *IS.WP.I.6.4:* Obtain and evaluate the policies governing security response center functions, including monitoring, classification, escalation, and reporting. ** Business Continuity Planning*
	Incident Resilience Planning and Strategy/Planning: Roles and responsibilities for incident response team members are defined. *Source: IS.B.84:* Define policies and procedures that guide the response, assigning responsibilities to individuals, providing appropriate training, formalizing information flows, and selecting, installing, and understanding the tools used in the response effort. *IS.WP.I.6.2:* Identify the organizational unit and personnel responsible for performing the functions of a security response center. ** Business Continuity Planning, Operations*

Yes/No	FFIEC Cybersecurity Assessment Tool
	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.B.84:* Preparation – [Define] which personnel have authority to perform what actions. This consideration affects the internal communications strategy, the commitment of personnel, and procedures that escalate involvement and decisions within the organization. *IS.WP.II.M.14:* Determine whether an intrusion response team… contains appropriate membership.
	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. ** E-Banking, Operations, Retail Payments*
	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.B.71:* Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution in the event the continuity plans must be implemented. *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. ** Retail Payments*
	Incident Resilience Planning and Strategy/Testing: Scenarios are used to improve incident detection and response. *Source: IS.B.71:* Risk assessments should consider the changing risks that appear in business continuity scenarios and the different security posture that may be established. *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.

Yes/No	FFIEC Cybersecurity Assessment Tool
	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. ** Outsourcing, Retail Payments*
	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. ** Retail Payments*
	Detection, Response & Mitigation/Detection: Alert parameters are set for detecting information security incidents that prompt mitigating actions. *Source: IS.B.43:* Management has the capability to filter logs for potential security events and provide adequate reporting and alerting capabilities. *IS.WP.II.H.4:* Evaluate whether the software acquired incorporates appropriate security controls, audit trails, and activity logs and that appropriate and timely audit trail and log reviews and alerts can take place. ** Business Continuity Planning*
	Detection, Response & Mitigation/Detection: System performance reports contain information that can be used as a risk indicator to detect information security incidents. *Source: IS.B.86:* Security personnel should monitor the information technology environment and review performance reports to identify trends, new threats, or control deficiencies. Specific activities could include reviewing security and activity logs, investigating operational anomalies, and routinely reviewing system and application access levels. *IS.WP.II.M.1:* Identify the monitoring performed to identify non-compliance with institution security policies and potential intrusions... Review security procedures for report monitoring to identify unauthorized or unusual activities.
	Detection, Response & Mitigation/Detection: Tools and processes are in place to detect, alert, and trigger the incident response program. *Source: IS.B.84:* Define policies and procedures that guide the response, assigning responsibilities to individuals, providing appropriate training, formalizing information flows, and selecting, installing, and understanding the tools used in the response effort.
	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.B.84:* While containment strategies between institutions can vary, they typically contain the following broad elements: isolation of compromised systems, or enhanced monitoring of intruder activities; search for additional compromised systems; collection and preservation of evidence; and communication with effected parties, the primary regulator, and law enforcement. *IS.WP.II.M.14:* Determine whether an intrusion response team: contains appropriate membership; Is available at all times; has appropriate training to investigate and report findings; has access to

Yes/No	FFIEC Cybersecurity Assessment Tool
	back-up data and systems, an inventory of all approved hardware and software, and monitored access to systems (as appropriate); has appropriate authority and timely access to decision makers for actions that require higher approvals; and have procedures for submitting appropriate incidents to the industry ** E-Banking, Business Continuity Planning, Retail Payments*
	Escalation and Reporting/Escalation and Reporting: A process exists to contact personnel who are responsible for analyzing and responding to an incident. *Source: IS.B.83:* Escalation policies should address when different personnel within the organization will be contacted about the incident, and the responsibility those personnel have in incident analysis and response. *IS.WP.I.6.4:* Obtain and evaluate the policies governing security response center functions, including monitoring, classification, escalation, and reporting. ** Business Continuity Planning, Operations*
	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.B.84:* Key considerations that directly affect the institution's policies and procedures include the following: when and under what circumstances to notify and involve regulators, customers, and law enforcement. This consideration drives certain monitoring decisions, decisions regarding evidence gathering and preservation, and communications considerations. *IS.WP.II.M.21:* Determine whether response policies and training appropriately address unauthorized disclosures of customer information, including notifying customers when warranted [and] appropriately notifying its primary federal regulator. Evaluate coordination of incident response policies and contractual notification requirements. ** Business Continuity Planning, Retail Payments*
	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.B.5:* Oversight requires the board to provide management with guidance; approve information security plans, policies and programs; and review reports on the effectiveness of the information security program. *IS.WP.I.7.1:* Review board and committee minutes and reports to determine the level of senior management support of and commitment to security.
	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. 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.

Below is a list of the unique identifiers used to reference the documents and the section.

Document	Section
Audit (AUD)	Booklet (B) or Work Program (WP)
Business Continuity Planning (BCP)	
Development and Acquisition (D&A)	
E-Banking (EB)	
Information Security (IS)	
Management (MGT)	
Operations (OPS)	
Outsourcing Technology Services (OT)	
Retail Payment Systems (RPS)	
Wholesale Payment Systems (WPS)	

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.”