Cybersecurity Maturity

Domain 1: Cyber Risk Management and Oversight			
Assessment Factor: Governance			
		Y, N	
OVERSIGHT	**Baseline**		Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. (*FFIEC Information Security Booklet, page 3*) Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. (*FFIEC Information Security Booklet, page 6*) 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. (*FFIEC Information Security Booklet, page 5*) The budgeting process includes information security related expenses and tools. (*FFIEC E-Banking Booklet, page 20*) Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. (*FFIEC Business Continuity Planning Booklet, page J-12*)
	Evolving		At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity. Cybersecurity tools and staff are requested through the budget process. There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.
	Intermediate		The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities. The standard board meeting package includes reports and metrics that go beyond events and incidents to address threat intelligence trends and the institution's security posture. The institution has a cyber risk appetite statement approved by the board or an appropriate board committee. Cyber risks that exceed the risk appetite are escalated to management. The board or an appropriate board committee ensures management's

		annual cybersecurity self-assessment evaluates the institution's ability to meet its cyber risk management standards.
		The board or an appropriate board committee reviews and approves management's prioritization and resource allocation decisions based on the results of the cyber assessments.
		The board or an appropriate board committee ensures management takes appropriate actions to address changing cyber risks or significant cybersecurity issues.
		The budget process for requesting additional cybersecurity staff and tools is integrated into business units' budget processes.
Advanced		The board or board committee approved cyber risk appetite statement is part of the enterprise-wide risk appetite statement.
		Management has a formal process to continuously improve cybersecurity oversight.
		The budget process for requesting additional cybersecurity staff and tools maps current resources and tools to the cybersecurity strategy.
		Management and the board or an appropriate board committee hold business units accountable for effectively managing all cyber risks associated with their activities.
		Management identifies root cause(s) when cyber attacks result in material loss.
		The board or an appropriate board committee ensures that management's actions consider the cyber risks that the institution poses to the financial sector.
Innovative		The board or an appropriate board committee discusses ways for management to develop cybersecurity improvements that may be adopted sector-wide.
		The board or an appropriate board committee verifies that management's actions consider the cyber risks that the institution poses to other critical infrastructures (e.g., telecommunications, energy).

STRATEGY/ POLICIES	**Baseline**		The institution has an information security strategy that integrates technology, policies, procedures, and training to mitigate risk. (*FFIEC Information Security Booklet, page 3*) The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management. (*FFIEC Information Security Booklet, page, 16*) The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing. (*FFIEC E-Banking Booklet, page 28*) The institution has board-approved policies commensurate with its risk and complexity that address information security. (*FFIEC Information Security Booklet, page 16*) The institution has policies commensurate with its risk and complexity that address the concepts of external dependency or third-party management. (*FFIEC Outsourcing Booklet, page 2*) The institution has policies commensurate with its risk and complexity that address the concepts of incident response and resilience. (*FFIEC Information Security Booklet, page 83*) All elements of the information security program are coordinated enterprise-wide. (*FFIEC Information Security Booklet, page 7*)
	Evolving		The institution augmented its information security strategy to incorporate cybersecurity and resilience. The institution has a formal cybersecurity program that is based on technology and security industry standards or benchmarks. A formal process is in place to update policies as the institution's inherent risk profile changes.
	Intermediate		The institution has a comprehensive set of policies commensurate with its risk and complexity that address the concepts of threat intelligence. Management periodically reviews the cybersecurity strategy to address evolving cyber threats and changes to the institution's inherent risk profile. The cybersecurity strategy is incorporated into, or conceptually fits within, the institution's enterprise-wide risk management strategy. Management links strategic cybersecurity objectives to tactical goals. A formal process is in place to cross-reference and simultaneously update all policies related to cyber risks across business lines.

	Advanced	The cybersecurity strategy outlines the institution's future state of cybersecurity with short-term and long-term perspectives. Industry-recognized cybersecurity standards are used as sources during the analysis of cybersecurity program gaps. The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructure in the financial services industry. The risk appetite is informed by the institution's role in critical infrastructure. Management is continuously improving the existing cybersecurity program to adapt as the desired cybersecurity target state changes.
	Innovative	The cybersecurity strategy identifies and communicates the institution's role as it relates to other critical infrastructures.
IT ASSET MANAGEMENT	**Baseline**	An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. *(FFIEC Information Security Booklet, page 9)* Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value. *(FFIEC Information Security Booklet, page 12)* Management assigns accountability for maintaining an inventory of organizational assets. *(FFIEC Information Security Booklet, page 9)* A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools. *(FFIEC Information Security Booklet, page 56)*
	Evolving	The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets. The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards. The institution proactively manages system EOL (e.g., replacement) to limit security risks. Changes are formally approved by an individual or committee with appropriate authority and with separation of duties.

	Intermediate		Baseline configurations cannot be altered without a formal change request, documented approval, and an assessment of security implications. A formal IT change management process requires cybersecurity risk to be evaluated during the analysis, approval, testing, and reporting of changes.
	Advanced		Supply chain risk is reviewed before the acquisition of mission-critical information systems including system components. Automated tools enable tracking, updating, asset prioritizing, and custom reporting of the asset inventory. Automated processes are in place to detect and block unauthorized changes to software and hardware. The change management system uses thresholds to determine when a risk assessment of the impact of the change is required.
	Innovative		A formal change management function governs decentralized or highly distributed change requests and identifies and measures security risks that may cause increased exposure to cyber attack. Comprehensive automated enterprise tools are implemented to detect and block unauthorized changes to software and hardware.
	Assessment Factor: Risk Management		
RISK MANAGEMENT PROGRAM	**Baseline**		An information security and business continuity risk management function(s) exists within the institution. (*FFIEC Information Security Booklet, page 68)*
	Evolving		The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring, and reporting. Management reviews and uses the results of audits to improve existing cybersecurity policies, procedures, and controls. Management monitors moderate and high residual risk issues from the cybersecurity risk assessment until items are addressed.

Intermediate		The cybersecurity function has a clear reporting line that does not present a conflict of interest. The risk management program specifically addresses cyber risks beyond the boundaries of the technological impacts (e.g., financial, strategic, regulatory, compliance). Benchmarks or target performance metrics have been established for showing improvements or regressions of the security posture over time. Management uses the results of independent audits and reviews to improve cybersecurity. There is a process to analyze and assign potential losses and related expenses, by cost center, associated with cybersecurity incidents.
Advanced		Cybersecurity metrics are used to facilitate strategic decision-making and funding in areas of need. Independent risk management sets and monitors cyber-related risk limits for business units. Independent risk management staff escalates to management and the board or an appropriate board committee significant discrepancies from business unit's assessments of cyber-related risk. A process is in place to analyze the financial impact cyber incidents have on the institution's capital. The cyber risk data aggregation and real-time reporting capabilities support the institution's ongoing reporting needs, particularly during cyber incidents.
Innovative		The risk management function identifies and analyzes commonalities in cyber events that occur both at the institution and across other sectors to enable more predictive risk management. A process is in place to analyze the financial impact that a cyber incident at the institution may have across the financial sector.

RISK ASSESSMENT			
	Baseline		A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, and customer information systems. *(FFIEC Information Security Booklet, page 8)* The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls. *(FFIEC Information Security Booklet, page 12)* The risk assessment is updated to address new technologies, products, services, and connections before deployment. *(FFIEC Information Security Booklet, page 13)*
	Evolving		Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships. The focus of the risk assessment has expanded beyond customer information to address all information assets. The risk assessment considers the risk of using EOL software and hardware components.
	Intermediate		The risk assessment is adjusted to consider widely known risks or risk management practices.
	Advanced		An enterprise-wide risk management function incorporates cyber threat analysis and specific risk exposure as part of the enterprise risk assessment.
	Innovative		The risk assessment is updated in real time as changes to the risk profile occur, new applicable standards are released or updated, and new exposures are anticipated. The institution uses information from risk assessments to predict threats and drive real-time responses. Advanced or automated analytics offer predictive information and real-time risk metrics.

AUDIT	**Baseline**		Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems. *(FFIEC Audit Booklet, page 4)* The independent audit function validates controls related to the storage or transmission of confidential data. *(FFIEC Audit Booklet, page 1)* Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance). *(FFIEC Operations Booklet, page 29)* 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. *(FFIEC Information Security Booklet, page 6)*
	Evolving		The independent audit function validates that the risk management function is commensurate with the institution's risk and complexity. The independent audit function validates that the institution's threat information sharing is commensurate with the institution's risk and complexity. The independent audit function validates that the institution's cybersecurity controls function is commensurate with the institution's risk and complexity. The independent audit function validates that the institution's third-party relationship management is commensurate with the institution's risk and complexity. The independent audit function validates that the institution's incident response program and resilience are commensurate with the institution's risk and complexity.
	Intermediate		A formal process is in place for the independent audit function to update its procedures based on changes to the institution's inherent risk profile. The independent audit function validates that the institution's threat intelligence and collaboration are commensurate with the institution's risk and complexity. The independent audit function regularly reviews management's cyber risk appetite statement. Independent audits or reviews are used to identify gaps in existing security capabilities and expertise.

STAFFING	**Advanced**		A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across the sector. The independent audit function regularly reviews the institution's cyber risk appetite statement in comparison to assessment results and incorporates gaps into the audit strategy. Independent audits or reviews are used to identify cybersecurity weaknesses, root causes, and the potential impact to business units.
	Innovative		A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across other sectors the institution depends upon. The independent audit function uses sophisticated data mining tools to perform continuous monitoring of cybersecurity processes or controls.
	Assessment Factor: Resources		
	Baseline		Information security roles and responsibilities have been identified. (*FFIEC Information Security Booklet, page 7*) Processes are in place to identify additional expertise needed to improve information security defenses. (*FFIEC Information Security Work Program, Objective I: 2-8*)
	Evolving		A formal process is used to identify cybersecurity tools and expertise that may be needed. Management with appropriate knowledge and experience leads the institution's cybersecurity efforts. Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position. Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk.
	Intermediate		The institution has a program for talent recruitment, retention, and succession planning for the cybersecurity and resilience staffs.
	Advanced		The institution benchmarks its cybersecurity staffing against peers to identify whether its recruitment, retention, and succession planning are commensurate. Dedicated cybersecurity staff develops, or contributes to developing, integrated enterprise-level security and cyber defense strategies.

TRAINING	**Innovative**	The institution actively partners with industry associations and academia to inform curricula based on future cybersecurity staffing needs of the industry.
	Assessment Factor: Training and Culture	
	Baseline	Annual information security training is provided. (*FFIEC Information Security Booklet*, *page 66*) Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues. (*FFIEC Information Security Booklet*, *page 66*) Situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts. (*FFIEC Information Security Booklet*, *page 7*) Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials). (*FFIEC E-Banking Work Program*, *Objective 6-3*)
	Evolving	The institution has a program for continuing cybersecurity training and skill development for cybersecurity staff. Management is provided cybersecurity training relevant to their job responsibilities. Employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility. Business units are provided cybersecurity training relevant to their particular business risks. The institution validates the effectiveness of training (e.g., social engineering or phishing tests).
	Intermediate	Management incorporates lessons learned from social engineering and phishing exercises to improve the employee awareness programs. Cybersecurity awareness information is provided to retail customers and commercial clients at least annually. Business units are provided cybersecurity training relevant to their particular business risks, over and above what is required of the institution as a whole. The institution routinely updates its training to security staff to adapt to new threats.

CULTURE	**Advanced**		Independent directors are provided with cybersecurity training that addresses how complex products, services, and lines of business affect the institution's cyber risk.
	Innovative		Key performance indicators are used to determine whether training and awareness programs positively influence behavior.
	Baseline		Management holds employees accountable for complying with the information security program. (*FFIEC Information Security Booklet, page 7*)
	Evolving		The institution has formal standards of conduct that hold all employees accountable for complying with cybersecurity policies and procedures. Cyber risks are actively discussed at business unit meetings. Employees have a clear understanding of how to identify and escalate potential cybersecurity issues.
	Intermediate		Management ensures performance plans are tied to compliance with cybersecurity policies and standards in order to hold employees accountable. The risk culture requires formal consideration of cyber risks in all business decisions. Cyber risk reporting is presented and discussed at the independent risk management meetings.
	Advanced		Management ensures continuous improvement of cyber risk cultural awareness.
	Innovative		The institution leads efforts to promote cybersecurity culture across the sector and to other sectors that they depend upon.

Domain 2: Threat Intelligence and Collaboration

Assessment Factor: Threat Intelligence

		Y,N	
THREAT INTELLIGENCE AND INFORMATION	**Baseline**		The institution belongs or subscribes to a threat and vulnerability information sharing source(s) that provides information on threats (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC], U.S. Computer Emergency Readiness Team [US-CERT]). *(FFIEC E-Banking Work Program, page 28)* Threat information is used to monitor threats and vulnerabilities. *(FFIEC Information Security Booklet, page 83)* Threat information is used to enhance internal risk management and controls. *(FFIEC Information Security Booklet, page 4)*
	Evolving		Threat information received by the institution includes analysis of tactics, patterns, and risk mitigation recommendations.
	Intermediate		A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources. Protocols are implemented for collecting information from industry peers and government. A read-only, central repository of cyber threat intelligence is maintained.
	Advanced		A cyber intelligence model is used for gathering threat information. Threat intelligence is automatically received from multiple sources in real time. The institution's threat intelligence includes information related to geopolitical events that could increase cybersecurity threat levels.
	Innovative		A threat analysis system automatically correlates threat data to specific risks and then takes risk-based automated actions while alerting management. The institution is investing in the development of new threat intelligence and collaboration mechanisms (e.g., technologies, business processes) that will transform how information is gathered and shared.

	Assessment Factor: Monitoring and Analyzing		
MONITORING AND ANALYZING	**Baseline**		Audit log records and other security event logs are reviewed and retained in a secure manner. (*FFIEC Information Security Booklet, page 79*) Computer event logs are used for investigations once an event has occurred. (*FFIEC Information Security Booklet, page 83*)
	Evolving		A process is implemented to monitor threat information to discover emerging threats. The threat information and analysis process is assigned to a specific group or individual. Security processes and technology are centralized and coordinated in a Security Operations Center (SOC) or equivalent. Monitoring systems operate continuously with adequate support for efficient incident handling.
	Intermediate		A threat intelligence team is in place that evaluates threat intelligence from multiple sources for credibility, relevance, and exposure. A profile is created for each threat that identifies the likely intent, capability, and target of the threat. Threat information sources that address all components of the threat profile are prioritized and monitored. Threat intelligence is analyzed to develop cyber threat summaries including risks to the institution and specific actions for the institution to consider.
	Advanced		A dedicated cyber threat identification and analysis committee or team exists to centralize and coordinate initiatives and communications. Formal processes have been defined to resolve potential conflicts in information received from sharing and analysis centers or other sources. Emerging internal and external threat intelligence and correlated log analysis are used to predict future attacks. Threat intelligence is viewed within the context of the institution's risk profile and risk appetite to prioritize mitigating actions in anticipation of threats. Threat intelligence is used to update architecture and configuration standards.

Innovative		The institution uses multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and geopolitical events to predict potential future attacks and attack trends. Highest risk scenarios are used to predict threats against specific business targets. IT systems automatically detect configuration weaknesses based on threat intelligence and alert management so actions can be prioritized.
	Assessment Factor: Information Sharing	
Baseline		Information security threats are gathered and shared with applicable internal employees. (*FFIEC Information Security Booklet*, *page 83*) Contact information for law enforcement and the regulator(s) is maintained and updated regularly. (*FFIEC Business Continuity Planning Work Program*, *Objective I: 5-1*) Information about threats is shared with law enforcement and regulators when required or prompted. (*FFIEC Information Security Booklet*, *page 84*)
Evolving		A formal and secure process is in place to share threat and vulnerability information with other entities. A representative from the institution participates in law enforcement or information-sharing organization meetings.
Intermediate		A formal protocol is in place for sharing threat, vulnerability, and incident information to employees based on their specific job function. Information-sharing agreements are used as needed or required to facilitate sharing threat information with other financial sector organizations or third parties. Information is shared proactively with the industry, law enforcement, regulators, and information-sharing forums. A process is in place to communicate and collaborate with the public sector regarding cyber threats.
Advanced		Management communicates threat intelligence with business risk context and specific risk management recommendations to the business units. Relationships exist with employees of peer institutions for sharing cyber threat intelligence. A network of trust relationships (formal and/or informal) has been established to evaluate information about cyber threats.

INFORMATION SHARING (vertical label in left column, spanning Baseline through Advanced rows)

Innovative		A mechanism is in place for sharing cyber threat intelligence with business units in real time including the potential financial and operational impact of inaction. A system automatically informs management of the level of business risk specific to the institution and the progress of recommended steps taken to mitigate the risks. The institution is leading efforts to create new sector-wide information-sharing channels to address gaps in external-facing information-sharing mechanisms.

Domain 3: Cybersecurity Controls

Assessment Factor: Preventative Controls

		Y, N	
INFRASTRUCTURE MANAGEMENT	**Baseline**		Network perimeter defense tools (e.g., border router and firewall) are used. (*FFIEC Information Security Booklet*, *page 33*) Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. (*FFIEC Information Security Booklet*, *page 46*) All ports are monitored. (*FFIEC Information Security Booklet*, *page 50*) Up to date antivirus and anti-malware tools are used. (*FFIEC Information Security Booklet*, *page 78*) Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced. (*FFIEC Information Security Booklet*, *page 56*) Ports, functions, protocols and services are prohibited if no longer needed for business purposes. (*FFIEC Information Security Booklet*, *page 50*) Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. (*FFIEC Information Security Booklet*, *page 56*) Programs that can override system, object, network, virtual machine, and application controls are restricted. (*FFIEC Information Security Booklet*, *page 41*) System sessions are locked after a pre-defined period of inactivity and are terminated after pre-defined conditions are met. (*FFIEC Information Security Booklet*, *page 23*) Wireless network environments require security settings with strong encryption for authentication and transmission. (*N/A if there are no wireless networks.) (*FFIEC Information Security Booklet*, *page 40*)
	Evolving		There is a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and internal network(s). Antivirus and intrusion detection/prevention systems (IDS/IPS) detect and block actual and attempted attacks or intrusions. Technical controls prevent unauthorized devices, including rogue wireless access devices and removable media, from connecting to the internal network(s). A risk-based solution is in place at the institution or Internet hosting

		provider to mitigate disruptive cyber attacks (e.g., DDoS attacks). Guest wireless networks are fully segregated from the internal network(s). (*N/A if there are no wireless networks.) Domain Name System Security Extensions (DNSSEC) is deployed across the enterprise. Critical systems supported by legacy technologies are regularly reviewed to identify for potential vulnerabilities, upgrade opportunities, or new defense layers. Controls for unsupported systems are implemented and tested.
	Intermediate	The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks. Security controls are used for remote access to all administrative consoles, including restricted virtual systems. Wireless network environments have perimeter firewalls that are implemented and configured to restrict unauthorized traffic. (*N/A if there are no wireless networks.) Wireless networks use strong encryption with encryption keys that are changed frequently. (*N/A if there are no wireless networks.) The broadcast range of the wireless network(s) is confined to institution-controlled boundaries. (*N/A if there are no wireless networks.) Technical measures are in place to prevent the execution of unauthorized code on institution owned or managed devices, network infrastructure, and systems components.
	Advanced	Network environments and virtual instances are designed and configured to restrict and monitor traffic between trusted and untrusted zones. Only one primary function is permitted per server to prevent functions that require different security levels from co-existing on the same server. Anti-spoofing measures are in place to detect and block forged source IP addresses from entering the network.
	Innovative	The institution risk scores all of its infrastructure assets and updates in real time based on threats, vulnerabilities, or operational changes. Automated controls are put in place based on risk scores to infrastructure assets, including automatically disconnecting affected assets. The institution proactively seeks to identify control gaps that may be used as part of a zero-day attack.

			Public-facing servers are routinely rotated and restored to a known clean state to limit the window of time a system is exposed to potential threats.
ACCESS AND DATA MANAGEMENT	**Baseline**		Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. (*FFIEC Information Security Booklet, page 19*)

Employee access to systems and confidential data provides for separation of duties. (*FFIEC Information Security Booklet, page 19*)

Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls). (*FFIEC Information Security Booklet, page 19*)

User access reviews are performed periodically for all systems and applications based on the risk to the application or system. (*FFIEC Information Security Booklet, page 18*)

Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel. (*FFIEC Information Security Booklet, page 18*)

Identification and authentication are required and managed for access to systems, applications, and hardware. (*FFIEC Information Security Booklet, page 21*)

Access controls include password complexity and limits to password attempts and reuse. (*FFIEC Information Security Booklet, page 66*)

All default passwords and unnecessary default accounts are changed before system implementation. (*FFIEC Information Security Booklet, page 61*)

Customer access to Internet-based products or services requires authentication controls (e.g., layered controls, multifactor) that are commensurate with the risk. (*FFIEC Information Security Booklet, page 21*)

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.*) (*FFIEC Information Security Booklet, page 64*)

Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems. (*FFIEC Information Security Booklet, page 47*)

All passwords are encrypted in storage and in transit. (*FFIEC Information Security Booklet, page 21*)

		Confidential data are encrypted when transmitted across public or untrusted networks (e.g., Internet). *(FFIEC Information Security Booklet, page 51)* 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.) *(FFIEC Information Security Booklet, page 51)* Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. *(FFIEC Information Security Booklet, page 45)* Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software. *(FFIEC Information Security Booklet, page 25)* Customer service (e.g., the call center) utilizes formal procedures to authenticate customers commensurate with the risk of the transaction or request. *(FFIEC Information Security Booklet, page 19)* Data is disposed of or destroyed according to documented requirements and within expected time frames. *(FFIEC Information Security Booklet, page 66)*
	Evolving	Changes to user access permissions trigger automated notices to appropriate personnel. Administrators have two accounts: one for administrative use and one for general purpose, non-administrative tasks. Use of customer data in non-production environments complies with legal, regulatory, and internal policy requirements for concealing or removing of sensitive data elements. Physical access to high-risk or confidential systems is restricted, logged, and unauthorized access is blocked. Controls are in place to prevent unauthorized access to cryptographic keys.

Intermediate		The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.
		Controls are in place to prevent unauthorized escalation of user privileges.
		Access controls are in place for database administrators to prevent unauthorized downloading or transmission of confidential data.
		All physical and logical access is removed immediately upon notification of involuntary termination and within 24 hours of an employee's voluntary departure.
		Multifactor authentication and/or layered controls have been implemented to secure all third-party access to the institution's network and/or systems and applications.
		Multifactor authentication (e.g., tokens, digital certificates) techniques are used for employee access to high-risk systems as identified in the risk assessment(s). (*N/A if no high risk systems.)
		Confidential data are encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.
		Controls are in place to prevent unauthorized access to collaborative computing devices and applications (e.g., networked white boards, cameras, microphones, online applications such as instant messaging and document sharing). (* N/A if collaborative computing devices are not used.)
Advanced		Encryption of select data at rest is determined by the institution's data classification and risk assessment.
		Customer authentication for high-risk transactions includes methods to prevent malware and man-in-the-middle attacks (e.g., using visual transaction signing).

DEVICE/END-POINT SECURITY	**Innovative**	Adaptive access controls de-provision or isolate an employee, third-party, or customer credentials to minimize potential damage if malicious behavior is suspected. Unstructured confidential data are tracked and secured through an identity-aware, cross-platform storage system that protects against internal threats, monitors user access, and tracks changes. Tokenization is used to substitute unique values for confidential information (e.g., virtual credit card). The institution is leading efforts to create new technologies and processes for managing customer, employee, and third-party authentication and access. Real-time risk mitigation is taken based on automated risk scoring of user credentials.
	Baseline	Controls are in place to restrict the use of removable media to authorized personnel. (*FFIEC Information Security Work Program, Objective I: 4-1*)
	Evolving	Tools automatically block attempted access from unpatched employee and third-party devices. Tools automatically block attempted access by unregistered devices to internal networks. The institution has controls to prevent the unauthorized addition of new connections. Controls are in place to prevent unauthorized individuals from copying confidential data to removable media. Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices). Mobile devices with access to the institution's data are centrally managed for antivirus and patch deployment. (*N/A if mobile devices are not used.) The institution wipes data remotely on mobile devices when a device is missing or stolen. (*N/A if mobile devices are not used.)
	Intermediate	Data loss prevention controls or devices are implemented for inbound and outbound communications (e.g., e-mail, FTP, Telnet, prevention of large file transfers). Mobile device management includes integrity scanning (e.g., jailbreak/rooted detection). (*N/A if mobile devices are not used.) Mobile devices connecting to the corporate network for storing and accessing company information allow for remote software version/patch validation. (*N/A if mobile devices are not used.)

	Advanced	Employees' and third parties' devices (including mobile) without the latest security patches are quarantined and patched before the device is granted access to the network. Confidential data and applications on mobile devices are only accessible via a secure, isolated sandbox or a secure container.
	Innovative	A centralized end-point management tool provides fully integrated patch, configuration, and vulnerability management, while also being able to detect malware upon arrival to prevent an exploit.
SECURE CODING	**Baseline**	Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards. *([FFIEC Information Security Booklet](), page 56)* The security controls of internally developed software are periodically reviewed and tested. (*N/A if there is no software development.) *([FFIEC Information Security Booklet](), page 59)* 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.) *([FFIEC Development and Acquisition Booklet](), page 2)* Intellectual property and production code are held in escrow. (*N/A if there is no production code to hold in escrow.) *([FFIEC Development and Acquisition Booklet](), page 39)*
	Evolving	Security testing occurs at all post-design phases of the SDLC for all applications, including mobile applications. (*N/A if there is no software development.)
	Intermediate	Processes are in place to mitigate vulnerabilities identified as part of the secure development of systems and applications. The security of applications, including Web-based applications connected to the Internet, is tested against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes. Software code executables and scripts are digitally signed to confirm the software author and guarantee that the code has not been altered or corrupted. A risk-based, independent information assurance function evaluates the security of internal applications.
	Advanced	Vulnerabilities identified through a static code analysis are remediated before implementing newly developed or changed applications into production. All interdependencies between applications and services have been

THREAT AND VULNERABILITY DETECTION		identified. Independent code reviews are completed on internally developed or vendor-provided custom applications to ensure there are no security gaps.
	Innovative	Software code is actively scanned by automated tools in the development environment so that security weaknesses can be resolved immediately during the design phase.
	Assessment Factor: Detective Controls	
	Baseline	Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network. *(FFIEC Information Security Booklet, page 61)* Antivirus and anti-malware tools are used to detect attacks. *(FFIEC Information Security Booklet, page 55)* Firewall rules are audited or verified at least quarterly. *(FFIEC Information Security Booklet, page 82)* E-mail protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links). *(FFIEC Information Security Booklet, page 39)*
	Evolving	Independent penetration testing of network boundary and critical Web-facing applications is performed routinely to identify security control gaps. Independent penetration testing is performed on Internet-facing applications or systems before they are launched or undergo significant change. Antivirus and anti-malware tools are updated automatically. Firewall rules are updated routinely. Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices. Processes are in place to monitor potential insider activity that could lead to data theft or destruction.
	Intermediate	Audit or risk management resources review the penetration testing scope and results to help determine the need for rotating companies based on the quality of the work. E-mails and attachments are automatically scanned to detect malware and are blocked when malware is present.

Advanced		Weekly vulnerability scanning is rotated among environments to scan all environments throughout the year. Penetration tests include cyber attack simulations and/or real-world tactics and techniques such as red team testing to detect control gaps in employee behavior, security defenses, policies, and resources. Automated tool(s) proactively identifies high-risk behavior signaling an employee who may pose an insider threat.
Innovative		User tasks and content (e.g., opening an e-mail attachment) are automatically isolated in a secure container or virtual environment so that malware can be analyzed but cannot access vital data, end-point operating systems, or applications on the institution's network. Vulnerability scanning is performed on a weekly basis across all environments.
Baseline		The institution is able to detect anomalous activities through monitoring across the environment. *(FFIEC Information Security Booklet, page 32)* Customer transactions generating anomalous activity alerts are monitored and reviewed. *(FFIEC Wholesale Payments Booklet, page 12)* Logs of physical and/or logical access are reviewed following events. *(FFIEC Information Security Booklet, page 73)* Access to critical systems by third parties is monitored for unauthorized or unusual activity. *(FFIEC Outsourcing Booklet, page 26)* Elevated privileges are monitored. *(FFIEC Information Security Booklet, page 19)*
Evolving		Systems are in place to detect anomalous behavior automatically during customer, employee, and third-party authentication. Security logs are reviewed regularly. Logs provide traceability for all system access by individual users. Thresholds have been established to determine activity within logs that would warrant management response.

The rows for Baseline, Evolving are under the vertical label **ANOMALOUS ACTIVITY DETECTION**.

	Intermediate		Online customer transactions are actively monitored for anomalous behavior. Tools to detect unauthorized data mining are used. Tools actively monitor security logs for anomalous behavior and alert within established parameters. Audit logs are backed up to a centralized log server or media that is difficult to alter. Thresholds for security logging are evaluated periodically. Anomalous activity and other network and system alerts are correlated across business units to detect and prevent multifaceted attacks (e.g., simultaneous account takeover and DDoS attack).
	Advanced		An automated tool triggers system and/or fraud alerts when customer logins occur within a short period of time but from physically distant IP locations. External transfers from customer accounts generate alerts and require review and authorization if anomalous behavior is detected. A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities. An automated tool(s) is in place to detect and prevent data mining by insider threats. Tags on fictitious confidential data or files are used to provide advanced alerts of potential malicious activity when the data is accessed.
	Innovative		The institution has a mechanism for real-time automated risk scoring of threats. The institution is developing new technologies that will detect potential insider threats and block activity in real time.

EVENT DETECTION	Baseline		A normal network activity baseline is established. *(FFIEC Information Security Booklet, page 77)* Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks. *(FFIEC Information Security Booklet, page 78)* Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. *(FFIEC Information Security Work Program, Objective II: M-9)* Responsibilities for monitoring and reporting suspicious systems activity have been assigned. *(FFIEC Information Security Booklet, page 83)* The physical environment is monitored to detect potential unauthorized access. *(FFIEC Information Security Booklet, page 47)*
	Evolving		A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).
	Intermediate		Controls or tools (e.g., data loss prevention) are in place to detect potential unauthorized or unintentional transmissions of confidential data. Event detection processes are proven reliable. Specialized security monitoring is used for critical assets throughout the infrastructure.
	Advanced		Automated tools detect unauthorized changes to critical system files, firewalls, IPS, IDS, or other security devices. Real-time network monitoring and detection is implemented and incorporates sector-wide event information. Real-time alerts are automatically sent when unauthorized software, hardware, or changes occur. Tools are in place to actively correlate event information from multiple sources and send alerts based on established parameters.
	Innovative		The institution is leading efforts to develop event detection systems that will correlate in real time when events are about to occur. The institution is leading the development effort to design new technologies that will detect potential insider threats and block activity in real time.

			Assessment Factor: Corrective Controls
PATCH MANAGEMENT	**Baseline**		A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner. (*FFIEC Information Security Booklet, page 62)* Patches are tested before being applied to systems and/or software. (*FFIEC Operations Booklet, page 22)* Patch management reports are reviewed and reflect missing security patches. (*FFIEC Development and Acquisition Booklet, page 50)*
	Evolving		A formal process is in place to acquire, test, and deploy software patches based on criticality. Systems are configured to retrieve patches automatically. Operational impact is evaluated before deploying security patches. An automated tool(s) is used to identify missing security patches as well as the number of days since each patch became available. Missing patches across all environments are prioritized and tracked.
	Intermediate		Patches for high-risk vulnerabilities are tested and applied when released or the risk is accepted and accountability assigned.
	Advanced		Patch monitoring software is installed on all servers to identify any missing patches for the operating system software, middleware, database, and other key software. The institution monitors patch management reports to ensure security patches are tested and implemented within aggressive time frames (e.g., 0-30 days).
	Innovative		The institution develops security patches or bug fixes or contributes to open source code development for systems it uses. Segregated or separate systems are in place that mirror production systems allowing for rapid testing and implementation of patches and provide for rapid fallback when needed.

REMEDIATION	**Baseline**		Issues identified in assessments are prioritized and resolved based on criticality and within the time frames established in the response to the assessment report. *(FFIEC Information Security Booklet, page 87)*
	Evolving		Data is destroyed or wiped on hardware and portable/mobile media when a device is missing, stolen, or no longer needed. Formal processes are in place to resolve weaknesses identified during penetration testing.
	Intermediate		Remediation efforts are confirmed by conducting a follow-up vulnerability scan. Penetration testing is repeated to confirm that medium- and high-risk, exploitable vulnerabilities have been resolved. Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties. Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action. The maintenance and repair of organizational assets are performed by authorized individuals with approved and controlled tools. The maintenance and repair of organizational assets are logged in a timely manner.
	Advanced		All medium and high risk issues identified in penetration testing, vulnerability scanning, and other independent testing are escalated to the board or an appropriate board committee for risk acceptance if not resolved in a timely manner.
	Innovative		The institution is developing technologies that will remediate systems damaged by zero-day attacks to maintain current recovery time objectives.

Domain 4: External Dependency Management

Assessment Factor: Connections

		Y, N	
CONNECTIONS	**Baseline**		The critical business processes that are dependent on external connectivity have been identified. *(FFIEC Information Security Booklet, page 9)* The institution ensures that third-party connections are authorized. *(FFIEC Information Security Booklet, page 17)* A network diagram is in place and identifies all external connections. *(FFIEC Information Security Booklet, page 9)* Data flow diagrams are in place and document information flow to external parties. *(FFIEC Information Security Booklet, page 10)*
	Evolving		Critical business processes have been mapped to the supporting external connections. The network diagram is updated when connections with third parties change or at least annually. Network and systems diagrams are stored in a secure manner with proper restrictions on access. Controls for primary and backup third-party connections are monitored and tested on a regular basis.
	Intermediate		A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity. Security controls are designed and verified to detect and prevent intrusions from third-party connections. Monitoring controls cover all external connections (e.g., third-party service providers, business partners, customers). Monitoring controls cover all internal network-to-network connections.
	Advanced		The security architecture is validated and documented before network connection infrastructure changes. The institution works closely with third-party service providers to maintain and improve the security of external connections.

DUE DILIGENCE	**Innovative**		Diagram(s) of external connections is interactive, shows real-time changes to the network connection infrastructure, new connections, and volume fluctuations, and alerts when risks arise. The institution's connections can be segmented or severed instantaneously to prevent contagion from cyber attacks.
		Assessment Factor: Relationship Management	
	Baseline		Risk-based due diligence is performed on prospective third parties before contracts are signed, including reviews of their background, reputation, financial condition, stability, and security controls. (*FFIEC Information Security Booklet, page 69*) A list of third-party service providers is maintained. (*FFIEC Outsourcing Booklet, page 19*) A risk assessment is conducted to identify criticality of service providers. (*FFIEC Outsourcing Booklet, page 6*)
	Evolving		A formal process exists to analyze assessments of third-party cybersecurity controls. The board or an appropriate board committee reviews a summary of due diligence results including management's recommendations to use third parties that will affect the institution's inherent risk profile.
	Intermediate		A process is in place to confirm that the institution's third-party service providers conduct due diligence of their third parties (e.g., subcontractors). Pre-contract, physical site visits of high-risk vendors are conducted by the institution or by a qualified third party.
	Advanced		A continuous process improvement program is in place for third-party due diligence activity. Audits of high-risk vendors are conducted on an annual basis.
	Innovative		The institution promotes sector-wide efforts to build due diligence mechanisms that lead to in-depth and efficient security and resilience reviews. The institution is leading efforts to develop new auditable processes and for conducting due diligence and ongoing monitoring of cybersecurity risks posed by third parties.

CONTRACTS	**Baseline**		Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential data or provide critical services. *(FFIEC Information Security Booklet, page 7)* Contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits. *(FFIEC Information Security Booklet, page 12)* Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party. *(FFIEC Information Security Booklet, page 12)* Contracts identify the recourse available to the institution should the third party fail to meet defined security requirements. *(FFIEC Outsourcing Booklet, page 12)* Contracts establish responsibilities for responding to security incidents. *(FFIEC E-Banking Booklet, page 22)* Contracts specify the security requirements for the return or destruction of data upon contract termination. *(FFIEC Outsourcing Booklet, page 15)*
	Evolving		Responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties are formally documented in the contract. Responsibility for notification of direct and indirect security incidents and vulnerabilities is documented in contracts or service-level agreements (SLAs). Contracts stipulate geographic limits on where data can be stored or transmitted.
	Intermediate		Third-party SLAs or similar means are in place that require timely notification of security events.
	Advanced		Contracts require third-party service provider's security policies meet or exceed those of the institution. A third-party termination/exit strategy has been established and validated with management.
	Innovative		The institution promotes a sector-wide effort to influence contractual requirements for critical third parties to the industry.

ONGOING MONITORING			
	Baseline		The third-party risk assessment is updated regularly. (*FFIEC Outsourcing Booklet*, *page 3*) Audits, assessments, and operational performance reports are obtained and reviewed regularly validating security controls for critical third parties. (*FFIEC Information Security Booklet*, *page 86*) Ongoing monitoring practices include reviewing critical third-parties' resilience plans. (*FFIEC Outsourcing Booklet*, *page 19*)
	Evolving		A process to identify new third-party relationships is in place, including identifying new relationships that were established without formal approval. A formal program assigns responsibility for ongoing oversight of third-party access. Monitoring of third parties is scaled, in terms of depth and frequency, according to the risk of the third parties. Automated reminders or ticklers are in place to identify when required third-party information needs to be obtained or analyzed.
	Intermediate		Third-party employee access to the institution's confidential data are tracked actively based on the principles of least privilege. Periodic on-site assessments of high-risk vendors are conducted to ensure appropriate security controls are in place.
	Advanced		Third-party employee access to confidential data on third-party hosted systems is tracked actively via automated reports and alerts.
	Innovative		The institution is leading efforts to develop new auditable processes for ongoing monitoring of cybersecurity risks posed by third parties.

Domain 5: Cyber Incident Management and Resilience

Assessment Factor: Incident Resilience Planning and Strategy

		Y, N	
PLANNING	**Baseline**		The institution has documented how it will react and respond to cyber incidents. (*FFIEC Business Continuity Planning Booklet, page 4*) Communication channels exist to provide employees a means for reporting information security events in a timely manner. (*FFIEC Information Security Booklet, page 83*) Roles and responsibilities for incident response team members are defined. (*FFIEC Information Security Booklet, page 84*) 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). (*FFIEC Information Security Booklet, page 84*) A formal backup and recovery plan exists for all critical business lines. (*FFIEC Business Continuity Planning Booklet, page 4*) The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. (*FFIEC Information Security Booklet, page 71*)
	Evolving		The remediation plan and process outlines the mitigating actions, resources, and time parameters. The corporate disaster recovery, business continuity, and crisis management plans have integrated consideration of cyber incidents. Alternative processes have been established to continue critical activity within a reasonable time period. Business impact analyses have been updated to include cybersecurity. Due diligence has been performed on technical sources, consultants, or forensic service firms that could be called to assist the institution during or following an incident.

	Intermediate		A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.
			Plans are in place to re-route or substitute critical functions and/or services that may be affected by a successful attack on Internet-facing systems.
			A direct cooperative or contractual agreement(s) is in place with an incident response organization(s) or provider(s) to assist rapidly with mitigation efforts.
			Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan.
	Advanced		Methods for responding to and recovering from cyber incidents are tightly woven throughout the business units' disaster recovery, business continuity, and crisis management plans.
			Multiple systems, programs, or processes are implemented into a comprehensive cyber resilience program to sustain, minimize, and recover operations from an array of potentially disruptive and destructive cyber incidents.
			A process is in place to continuously improve the resilience plan.
	Innovative		The incident response plan is designed to ensure recovery from disruption of services, assurance of data integrity, and recovery of lost or corrupted data following a cybersecurity incident.
			The incident response process includes detailed actions and rule-based triggers for automated response.
TESTING	**Baseline**		Scenarios are used to improve incident detection and response. (*FFIEC Information Security Booklet, page 71*)
			Business continuity testing involves collaboration with critical third parties. (*FFIEC Business Continuity Planning Booklet, page J-6*)
			Systems, applications, and data recovery is tested at least annually. (*FFIEC Business Continuity Planning Booklet, page J-7*)
	Evolving		Recovery scenarios include plans to recover from data destruction and impacts to data integrity, data loss, and system and data availability.
			Widely reported events are used to evaluate and improve the institution's response.
			Information backups are tested periodically to verify they are accessible and readable.

Intermediate		Cyber-attack scenarios are analyzed to determine potential impact to critical business processes.
		The institution participates in sector-specific cyber exercises or scenarios (e.g., FS-ISAC Cyber Attack (against) Payment Processors (CAPP)).
		Resilience testing is based on analysis and identification of realistic and highly likely threats as well as new and emerging threats facing the institution.
		The critical online systems and processes are tested to withstand stresses for extended periods (e.g., DDoS).
		The results of cyber event exercises are used to improve the incident response plan and automated triggers.
Advanced		Resilience testing is comprehensive and coordinated across all critical business functions.
		The institution validates that it is able to recover from cyber events similar to by known sophisticated attacks at other organizations.
		Incident response testing evaluates the institution from an attacker's perspective to determine how the institution or its assets at critical third parties may be targeted.
		The institution corrects root causes for problems discovered during cybersecurity resilience testing.
		Cybersecurity incident scenarios involving significant financial loss are used to stress test the institution's risk management.
Innovative		The institution tests the ability to shift business processes or functions between different processing centers or technology systems for cyber incidents without interruption to business or loss of productivity or data.
		The institution has validated that it is able to remediate systems damaged by zero-day attacks to maintain current recovery time objectives.
		The institution is leading the development of more realistic test environments.
		Cyber incident scenarios are used to stress test potential financial losses across the sector.

		Assessment Factor: Detection, Response, and Mitigation	
DETECTION	**Baseline**		Alert parameters are set for detecting information security incidents that prompt mitigating actions. (*FFIEC Information Security Booklet*, *page 43*) System performance reports contain information that can be used as a risk indicator to detect information security incidents. (*FFIEC Information Security Booklet*, *page 86*) Tools and processes are in place to detect, alert, and trigger the incident response program. (*FFIEC Information Security Booklet*, *page 84*)
	Evolving		The institution has processes to detect and alert the incident response team when potential insider activity manifests that could lead to data theft or destruction.
	Intermediate		The incident response program is triggered when anomalous behaviors and attack patterns or signatures are detected. The institution has the ability to discover infiltration, before the attacker traverses across systems, establishes a foothold, steals information, or causes damage to data and systems. Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond. Network and system alerts are correlated across business units to better detect and prevent multifaceted attacks (e.g., simultaneous DDoS attack and account takeover). Incident detection processes are capable of correlating events across the enterprise.
	Advanced		Sophisticated and adaptive technologies are deployed that can detect and alert the incident response team of specific tasks when threat indicators across the enterprise indicate potential external and internal threats. Automated tools are implemented to provide specialized security monitoring based on the risk of the assets to detect and alert incident response teams in real time.
	Innovative		The institution is able to detect and block zero-day attempts and inform management and the incident response team in real time.

RESPONSE AND MITIGATION	**Baseline**		Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information. (*FFIEC Information Security Booklet*, page 84)
	Evolving		The incident response plan is designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities. A process is in place to help contain incidents and restore operations with minimal service disruption. Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware). Procedures include containment strategies and notifying potentially impacted third parties. Processes are in place to trigger the incident response program when an incident occurs at a third party. Records are generated to support incident investigation and mitigation. The institution calls upon third parties, as needed, to provide mitigation services. Analysis of events is used to improve the institution's security measures and policies.
	Intermediate		Analysis of security incidents is performed in the early stages of an intrusion to minimize the impact of the incident. Any changes to systems/applications or to access entitlements necessary for incident management are reviewed by management for formal approval before implementation. Processes are in place to ensure assets affected by a security incident that cannot be returned to operational status are quarantined, removed, disposed of, and/or replaced. Processes are in place to ensure that restored assets are appropriately reconfigured and thoroughly tested before being placed back into operation.
	Advanced		The incident management function collaborates effectively with the cyber threat intelligence function during an incident. Links between threat intelligence, network operations, and incident response allow for proactive response to potential incidents. Technical measures apply defense-in-depth techniques such as deep-packet inspection and black holing for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns and/or DDoS attacks.

	Innovative	The institution's risk management of significant cyber incidents results in limited to no disruptions to critical services. The technology infrastructure has been engineered to limit the effects of a cyber attack on the production environment from migrating to the backup environment (e.g., air-gapped environment and processes).
	Assessment Factor: Escalation and Reporting	
ESCALATION AND REPORTING	**Baseline**	A process exists to contact personnel who are responsible for analyzing and responding to an incident. (*FFIEC Information Security Booklet, page 83)* 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. (*FFIEC Information Security Booklet, page 84)* The institution prepares an annual report of security incidents or violations for the board or an appropriate board committee. (*FFIEC Information Security Booklet, page 5)* Incidents are classified, logged, and tracked. (*FFIEC Operations Booklet, page 28)*
	Evolving	Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk. Regulators, law enforcement, and service providers, as appropriate, are notified when the institution is aware of any unauthorized access to systems or a cyber incident occurs that could result in degradation of services. Tracked cyber incidents are correlated for trend analysis and reporting.
	Intermediate	Employees that are essential to mitigate the risk (e.g., fraud, business resilience) know their role in incident escalation. A communication plan is used to notify other organizations, including third parties, of incidents that may affect them or their customers. An external communication plan is used for notifying media regarding incidents when applicable.
	Advanced	The institution has established quantitative and qualitative metrics for the cybersecurity incident response process. Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the board meeting package.

Innovative		A mechanism is in place to provide instantaneous notification of incidents to management and essential employees through multiple communication channels with tracking and verification of receipt.