

FFIEC Cybersecurity Assessment Tool

Overview for Chief Executive Officers and Boards of Directors

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council¹ (FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time. The Assessment incorporates cybersecurity-related principles from the *FFIEC Information Technology (IT) Examination Handbook* and regulatory guidance, and concepts from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.²

Benefits to the Institution

For institutions using the Assessment, management will be able to enhance their oversight and management of the institution's cybersecurity by doing the following:

- Identifying factors contributing to and determining the institution's overall cyber risk.
- Assessing the institution's cybersecurity preparedness.
- Evaluating whether the institution's cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies.

CEO and Board of Directors

The role of the chief executive officer (CEO), with management's support, may include the responsibility to do the following:

- Develop a plan to conduct the Assessment.
- Lead employee efforts during the Assessment to facilitate timely responses from across the institution.
- Set the target state of cybersecurity preparedness that best aligns to the board of directors' (board) stated (or approved) risk appetite.
- Review, approve, and support plans to address risk management and control weaknesses.
- Analyze and present results for executive oversight, including key stakeholders and the board, or an appropriate board committee.

¹ The FFIEC comprises the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

² A mapping is available in [Appendix B: Mapping Cybersecurity Assessment Tool to the NIST Cybersecurity Framework](#). NIST reviewed and provided input on the mapping to ensure consistency with Framework principles and to highlight the complementary nature of the two resources.

- Oversee the performance of ongoing monitoring to remain nimble and agile in addressing evolving areas of cybersecurity risk.
- Oversee changes to maintain or increase the desired cybersecurity preparedness.

The role of the board, or an appropriate board committee, may include the responsibility to do the following:

- Engage management in establishing the institution’s vision, risk appetite, and overall strategic direction.
- Approve plans to use the Assessment.
- Review management’s analysis of the Assessment results, inclusive of any reviews or opinions on the results issued by independent risk management or internal audit functions regarding those results.
- Review management’s determination of whether the institution’s cybersecurity preparedness is aligned with its risks.
- Review and approve plans to address any risk management or control weaknesses.
- Review the results of management’s ongoing monitoring of the institution’s exposure to and preparedness for cyber threats.

Assessment’s Parts and Process

The Assessment consists of two parts: Inherent Risk Profile and Cybersecurity Maturity. Upon completion of both parts, management can evaluate whether the institution’s inherent risk and preparedness are aligned.

Inherent Risk Profile

Cybersecurity inherent risk is the level of risk posed to the institution by the following:

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

Inherent risk incorporates the type, volume, and complexity of the institution’s operations and threats directed at the institution. Inherent risk does not include mitigating controls. The Inherent Risk Profile includes descriptions of activities across risk categories with definitions for the least to most levels of inherent risk. The profile helps management determine exposure to risk that the institution’s activities, services, and products individually and collectively pose to the institution.

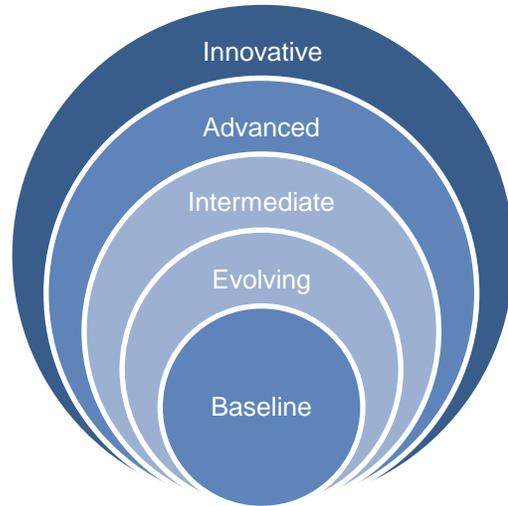


When each of the activities, services, and products are assessed, management can review the results and determine the institution’s overall inherent risk profile.

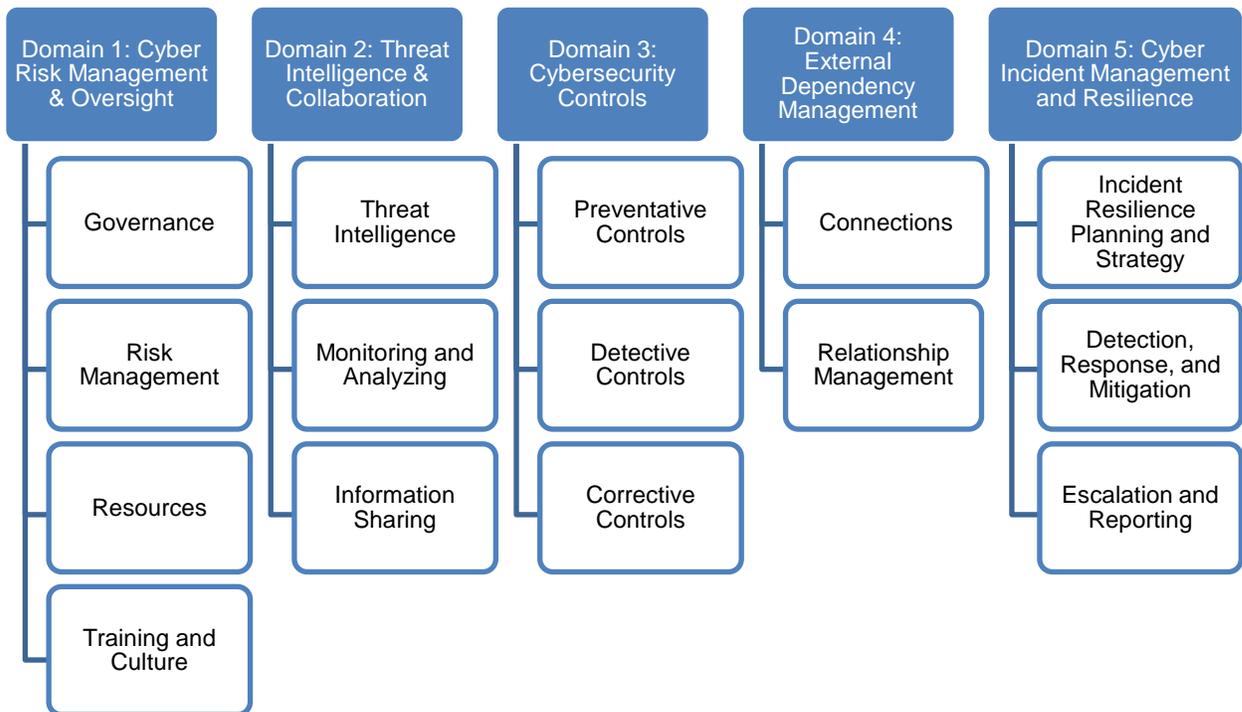
Cybersecurity Maturity

The Assessment’s second part is Cybersecurity Maturity, designed to help management measure the institution’s level of risk and corresponding controls. The levels range from baseline to innovative. Cybersecurity Maturity includes statements to determine whether an institution’s behaviors, practices, and processes can support cybersecurity preparedness within the following five domains:

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience



The domains include assessment factors and contributing components. Within each component, declarative statements describe activities supporting the assessment factor at each maturity level. Management determines which declarative statements best fit the current practices of the institution. **All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain’s maturity level.** While management can determine the institution’s maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level. The figure below provides the five domains and assessment factors.



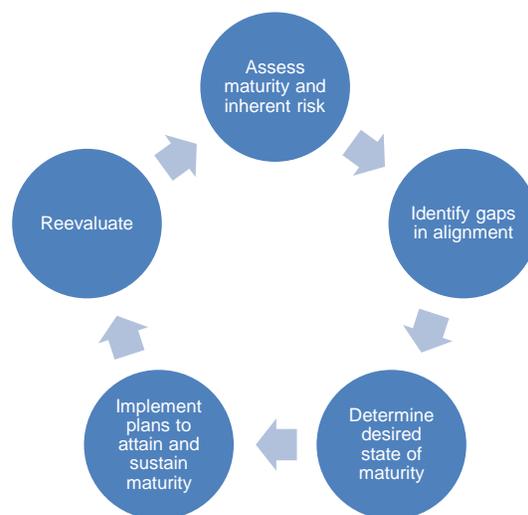
Management can review the institution’s Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain to understand whether they are aligned. The following table depicts the relationship between an institution’s Inherent Risk Profile and its domain Maturity Levels, as there is no single expected level for an institution. In general, as inherent risk rises, an institution’s maturity levels should increase. An institution’s inherent risk profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change. Thus, management should consider reevaluating the institution’s inherent risk profile and cybersecurity maturity periodically and when planned changes can affect its inherent risk profile (e.g., launching new products or services, new connections).

Risk/Maturity Relationship		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative					
	Advanced					
	Intermediate					
	Evolving					
	Baseline					

Management can then decide what actions are needed either to affect the inherent risk profile or to achieve a desired state of maturity. On an ongoing basis, management may use the Assessment to identify changes to the institution’s inherent risk profile when new threats arise or when considering changes to the business strategy, such as expanding operations, offering new products and services, or entering into new third-party relationships that support critical activities. Consequently, management can determine whether additional risk management practices or controls are needed to maintain or augment the institution’s cybersecurity maturity.

Supporting Implementation

An essential part of implementing the Assessment is to validate the institution’s process and findings and the effectiveness and sufficiency of the plans to address any identified weaknesses. The next section provides some questions to assist management and the board when using the Assessment.



Cybersecurity Management & Oversight

- What are the potential cyber threats to the institution?
- Is the institution a direct target of attacks?
- Is the institution’s cybersecurity preparedness receiving the appropriate level of time and attention from management and the board or an appropriate board committee?

- Do the institution's policies and procedures demonstrate management's commitment to sustaining appropriate cybersecurity maturity levels?
- What is the ongoing process for gathering, monitoring, analyzing, and reporting risks?
- Who is accountable for assessing and managing the risks posed by changes to the business strategy or technology?
- Are the accountable individuals empowered with the authority to carry out these responsibilities?
- Do the inherent risk profile and cybersecurity maturity levels meet management's business and risk management expectations? If there is misalignment, what are the proposed plans to bring them into alignment?
- How can management and the board, or an appropriate board committee, make this process part of the institution's enterprise-wide governance framework?

Inherent Risk Profile

- What is the process for gathering and validating the information for the inherent risk profile and cybersecurity maturity?
- How can management and the board, or an appropriate board committee, support improvements to the institution's process for conducting the Assessment?
- What do the results of the Assessment mean to the institution as it looks at its overall risk profile?
- What are the institution's areas of highest inherent risk?
- Is management updating the institution's inherent risk profile to reflect changes in activities, services, and products?

Cybersecurity Maturity

- How effective are the institution's risk management activities and controls identified in the Assessment?
- Are there more efficient or effective means for attaining or improving the institution's risk management and controls?
- What third parties does the institution rely on to support critical activities?
- What is the process to oversee third parties and understand their inherent risks and cybersecurity maturity?
- How does management validate the type and volume of attacks?
- Is the institution sharing threat information with peers, law enforcement, and critical third parties through information-sharing procedures?

Summary

FFIEC has developed the Assessment to assist management and the board, or an appropriate board committee, in assessing their institution's cybersecurity preparedness and risk. For more information and additional questions to consider, refer to the [FFIEC Cybersecurity Assessment General Observations](#) on the FFIEC's Web site.



Cybersecurity Assessment Tool

May 2017

Paperwork Reduction Act (PRA) – OMB Control No. 1557-0328; Expiration date: August 31, 2019

The above OMB Control Number and expiration date pertain to a requirement of the Paperwork Reduction Act and its implementing regulation that a federal agency may not conduct or sponsor, and a person (or organization) is not required to respond to, a collection of information unless it displays a currently valid OMB control number and, if appropriate, an expiration date. See 44 USC 3506(c)(1)(B) and 5 CFR 1320.5(b)(2)(i), 1320.8(b)(1).

Contents

Contents	i
User’s Guide	1
Overview	1
Background	2
Completing the Assessment	2
Part One: Inherent Risk Profile	3
Part Two: Cybersecurity Maturity	5
Interpreting and Analyzing Assessment Results	8
Resources	10
Inherent Risk Profile	11
Cybersecurity Maturity	19
Domain 1: Cyber Risk Management and Oversight	19
Domain 2: Threat Intelligence and Collaboration	30
Domain 3: Cybersecurity Controls	34
Domain 4: External Dependency Management	47
Domain 5: Cyber Incident Management and Resilience	51

Additional Resources

[Overview for Chief Executive Officers and Boards of Directors](#)

[Appendix A: Mapping Baseline Statements to FFIEC IT Examination Handbook](#)

[Appendix B: Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework](#)

[Appendix C: Glossary](#)

User's Guide

Overview

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council¹ (FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity maturity.

The content of the Assessment is consistent with the principles of the *FFIEC Information Technology Examination Handbook (IT Handbook)* and the National Institute of Standards and Technology (NIST) Cybersecurity Framework,² as well as industry accepted cybersecurity practices. The Assessment provides institutions with a repeatable and measureable process to inform management of their institution's risks and cybersecurity preparedness.

The Assessment consists of two parts: Inherent Risk Profile and Cybersecurity Maturity. The Inherent Risk Profile identifies the institution's inherent risk before implementing controls. The Cybersecurity Maturity includes domains, assessment factors, components, and individual declarative statements across five maturity levels to identify specific controls and practices that are in place. While management can determine the institution's maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level.

To complete the Assessment, management first assesses the institution's inherent risk profile based on five categories:

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

Management then evaluates the institution's Cybersecurity Maturity level for each of five domains:

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience

¹ The FFIEC comprises the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

² A mapping is available in [Appendix B: Mapping Cybersecurity Assessment Tool to the NIST Cybersecurity Framework](#). NIST reviewed and provided input on the mapping to ensure consistency with Framework principles and to highlight the complementary nature of the two resources.

By reviewing both the institution's inherent risk profile and maturity levels across the domains, management can determine whether its maturity levels are appropriate in relation to its risk. If not, the institution may take action either to reduce the level of risk or to increase the levels of maturity. This process is intended to complement, not replace, an institution's risk management process and cybersecurity program.

Background

The Assessment is based on the cybersecurity assessment that the FFIEC members piloted in 2014, which was designed to evaluate community institutions' preparedness to mitigate cyber risks. NIST defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks." As part of cybersecurity, institutions should consider managing internal and external threats and vulnerabilities to protect infrastructure and information assets. The definition builds on information security as defined in FFIEC guidance.

Cyber incidents can have financial, operational, legal, and reputational impact. Recent high-profile cyber attacks demonstrate that cyber incidents can significantly affect capital and earnings. Costs may include forensic investigations, public relations campaigns, legal fees, consumer credit monitoring, and technology changes. As such, cybersecurity needs to be integrated throughout an institution as part of enterprise-wide governance processes, information security, business continuity, and third-party risk management. For example, an institution's cybersecurity policies may be incorporated within the information security program. In addition, cybersecurity roles and processes referred to in the Assessment may be separate roles within the security group (or outsourced) or may be part of broader roles across the institution.

Completing the Assessment

The Assessment is designed to provide a measurable and repeatable process to assess an institution's level of cybersecurity risk and preparedness. Part one of this Assessment is the Inherent Risk Profile, which identifies an institution's inherent risk relevant to cyber risks. Part two is the Cybersecurity Maturity, which determines an institution's current state of cybersecurity preparedness represented by maturity levels across five domains. For this Assessment to be an effective risk management tool, an institution may want to complete it periodically and as significant operational and technological changes occur.

Cyber risk programs build upon and align existing information security, business continuity, and disaster recovery programs. The Assessment is intended to be used primarily on an enterprise-wide basis and when introducing new products and services as follows:

- **Enterprise-wide.** Management may review the Inherent Risk Profile and the declarative statements to understand which policies, procedures, processes, and controls are in place enterprise-wide and where gaps may exist. Following this review, management can determine appropriate maturity levels for the institution in each domain or the target state for Cybersecurity Maturity. Management can then develop action plans for achieving the target state.
- **New products, services, or initiatives.** Using the Assessment before launching a new product, service, or initiative can help management understand how these might affect the institution's inherent risk profile and resulting desired maturity levels.

Part One: Inherent Risk Profile

Part one of the Assessment identifies the institution's inherent risk. The Inherent Risk Profile identifies activities, services, and products organized in the following categories:

- **Technologies and Connection Types.** Certain types of connections and technologies may pose a higher inherent risk depending on the complexity and maturity, connections, and nature of the specific technology products or services. This category includes the number of Internet service provider (ISP) and third-party connections, whether systems are hosted internally or outsourced, the number of unsecured connections, the use of wireless access, volume of network devices, end-of-life systems, extent of cloud services, and use of personal devices.
- **Delivery Channels.** Various delivery channels for products and services may pose a higher inherent risk depending on the nature of the specific product or service offered. Inherent risk increases as the variety and number of delivery channels increases. This category addresses whether products and services are available through online and mobile delivery channels and the extent of automated teller machine (ATM) operations.
- **Online/Mobile Products and Technology Services.** Different products and technology services offered by institutions may pose a higher inherent risk depending on the nature of the specific product or service offered. This category includes various payment services, such as debit and credit cards, person-to-person payments, originating automated clearing house (ACH), retail wire transfers, wholesale payments, merchant remote deposit capture, treasury services and clients and trust services, global remittances, correspondent banking, and merchant acquiring activities. This category also includes consideration of whether the institution provides technology services to other organizations.
- **Organizational Characteristics.** This category considers organizational characteristics, such as mergers and acquisitions, number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged access, changes in information technology (IT) environment, locations of business presence, and locations of operations and data centers.
- **External Threats.** The volume and type of attacks (attempted or successful) affect an institution's inherent risk exposure. This category considers the volume and sophistication of the attacks targeting the institution.

Risk Levels

Risk Levels incorporate the type, volume, and complexity of the institution's operations and threats directed at the institution. Inherent risk does not include mitigating controls.

Select the most appropriate inherent risk level for each activity, service, or product within each category. The levels range from Least Inherent Risk to Most Inherent Risk (Figure 1) and incorporate a wide range of descriptions. The risk levels provide parameters for determining the inherent risk for each category. These parameters are not intended to be rigid but rather instructive to assist with assessing a risk level within each activity, service, or product. For situations where the risk level falls between two levels, management should select the higher risk level.

Figure 1: Inherent Risk Profile Layout

Activity, Service, or Product	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

Determine Inherent Risk Profile

Management can determine the institution's overall Inherent Risk Profile based on the number of applicable statements in each risk level for all activities (Figure 2). For example, when a majority of activities, products, or services fall within the Moderate Risk Level, management may determine that the institution has a Moderate Inherent Risk Profile. Each category may, however, pose a different level of inherent risk. Therefore, in addition to evaluating the number of instances that an institution selects for a specific risk level, management may also consider evaluating whether the specific category poses additional risk.

Figure 2: Inherent Risk Summary

	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Number of Statements Selected in Each Risk Level					
Based on Individual Risk Levels Selected, Assign an Inherent Risk Profile	Least	Minimal	Moderate	Significant	Most

The following includes definitions of risk levels.

- Least Inherent Risk.** An institution with a Least Inherent Risk Profile generally has very limited use of technology. It has few computers, applications, systems, and no connections. The variety of products and services are limited. The institution has a small geographic footprint and few employees.
- Minimal Inherent Risk.** An institution with a Minimal Inherent Risk Profile generally has limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services. The institution's mission-critical systems are outsourced. The institution primarily uses established technologies. It maintains a few types of connections to customers and third parties with limited complexity.
- Moderate Inherent Risk.** An institution with a Moderate Inherent Risk Profile generally uses technology that may be somewhat complex in terms of volume and sophistication. The

institution may outsource mission-critical systems and applications and may support elements internally. There is a greater variety of products and services offered through diverse channels.

- **Significant Inherent Risk.** An institution with a Significant Inherent Risk Profile generally uses complex technology in terms of scope and sophistication. The institution offers high-risk products and services that may include emerging technologies. The institution may host a significant number of applications internally. The institution allows either a large number of personal devices or a large variety of device types. The institution maintains a substantial number of connections to customers and third parties. A variety of payment services are offered directly rather than through a third party and may reflect a significant level of transaction volume.
- **Most Inherent Risk.** An institution with a Most Inherent Risk Profile uses extremely complex technologies to deliver myriad products and services. Many of the products and services are at the highest level of risk, including those offered to other organizations. New and emerging technologies are utilized across multiple delivery channels. The institution may outsource some mission-critical systems or applications, but many are hosted internally. The institution maintains a large number of connection types to transfer data with customers and third parties.

Part Two: Cybersecurity Maturity

After determining the Inherent Risk Profile, the institution transitions to the Cybersecurity Maturity part of the Assessment to determine the institution's maturity level within each of the following five domains:

- **Domain 1:** Cyber Risk Management and Oversight
- **Domain 2:** Threat Intelligence and Collaboration
- **Domain 3:** Cybersecurity Controls
- **Domain 4:** External Dependency Management
- **Domain 5:** Cyber Incident Management and Resilience

Domains, Assessment Factors, Components, and Declarative Statements

Within each domain are assessment factors and contributing components. Under each component, there are declarative statements describing an activity that supports the assessment factor at that level of maturity. Table 1 provides definitions for each domain and the underlying assessment factors.

Table 1: Domains and Assessment Factors Defined

Domains and Assessment Factors Defined	
Domain 1	
Cyber Risk Management and Oversight	
<p>Cyber risk management and oversight addresses the board of directors' (board's) oversight and management's development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.</p>	
Assessment Factors	<p>Governance includes oversight, strategies, policies, and IT asset management to implement an effective governance of the cybersecurity program.</p> <p>Risk Management includes a risk management program, risk assessment process, and audit function to effectively manage risk and assess the effectiveness of key controls.</p> <p>Resources include staffing, tools, and budgeting processes to ensure the institution's staff or external resources have knowledge and experience commensurate with the institution's risk profile.</p> <p>Training and Culture includes the employee training and customer awareness programs contributing to an organizational culture that emphasizes the mitigation of cybersecurity threats.</p>
Domain 2	
Threat Intelligence and Collaboration	
<p>Threat intelligence and collaboration includes processes to effectively discover, analyze, and understand cyber threats, with the capability to share information internally and with appropriate third parties.</p>	
Assessment Factors	<p>Threat Intelligence refers to the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making.</p> <p>Monitoring and Analyzing refers to how an institution monitors threat sources and what analysis may be performed to identify threats that are specific to the institution or to resolve conflicts in the different threat intelligence streams.</p> <p>Information Sharing encompasses establishing relationships with peers and information-sharing forums and how threat information is communicated to those groups as well as internal stakeholders.</p>
Domain 3	
Cybersecurity Controls	
<p>Cybersecurity controls are the practices and processes used to protect assets, infrastructure, and information by strengthening the institution's defensive posture through continuous, automated protection and monitoring.</p>	
Assessment Factors	<p>Preventative Controls deter and prevent cyber attacks and include infrastructure management, access management, device and end-point security, and secure coding.</p> <p>Detective Controls include threat and vulnerability detection, anomalous activity detection, and event detection, may alert the institution to network and system irregularities that indicate an incident has or may occur.</p> <p>Corrective Controls are utilized to resolve system and software vulnerabilities through patch management and remediation of issues identified during vulnerability scans and penetration testing.</p>
Domain 4	
External Dependency Management	
<p>External dependency management involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the institution's technology assets and information.</p>	
Assessment Factors	<p>Connections incorporate the identification, monitoring, and management of external connections and data flows to third parties.</p> <p>Relationship Management includes due diligence, contracts, and ongoing monitoring to help ensure controls complement the institution's cybersecurity program.</p>

Domain 5

Cyber Incident Management and Resilience

Cyber incident management includes establishing, identifying, and analyzing cyber events; prioritizing the institution's containment or mitigation; and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber incident.

Assessment Factors	<p>Incident Resilience Planning & Strategy incorporates resilience planning and testing into existing business continuity and disaster recovery plans to minimize service disruptions and the destruction or corruption of data.</p> <p>Detection, Response, & Mitigation refers to the steps management takes to identify, prioritize, respond to, and mitigate the effects of internal and external threats and vulnerabilities.</p> <p>Escalation & Reporting ensures key stakeholders are informed about the impact of cyber incidents, and regulators, law enforcement, and customers are notified as required.</p>
---------------------------	---

Figure 3: Cybersecurity Maturity Levels

Each maturity level includes a set of declarative statements that describe how the behaviors, practices, and processes of an institution can consistently produce the desired outcomes.

The Assessment starts at the Baseline maturity level and progresses to the highest maturity, the Innovative level (Figure 3). Table 2 provides definitions for each of the maturity levels, which are cumulative.

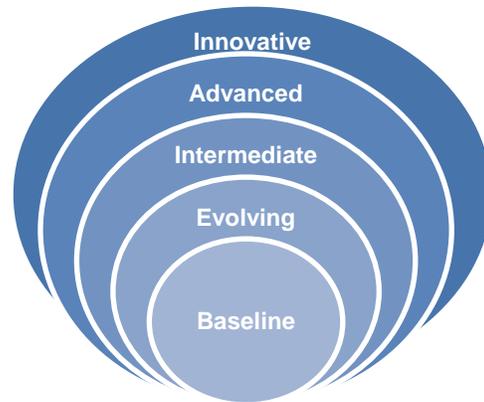


Table 2: Maturity Levels Defined

Maturity Levels Defined	
Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.
Intermediate	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
Advanced	Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

Completing the Cybersecurity Maturity

Each domain and maturity level has a set of declarative statements organized by assessment factor. To assist the institution's ability to follow common themes across maturity levels, statements are categorized by components. The components are groups of similar declarative statements to make the Assessment easier to use (Figure 4).

Figure 4: Cybersecurity Maturity

		Domain 1: Cyber Risk Management and Oversight		← Domain
		Assessment Factor: Governance		← Assessment Factor
Maturity Level	Y, Y(C), N	Component		
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. <i>(FFIEC Information Security Booklet, page 3)</i> Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. <i>(FFIEC Information Security Booklet, page 6)</i> <div style="border: 1px solid black; padding: 2px;"> 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. <i>(FFIEC Information Security Booklet, page 5)</i> </div> The budgeting process includes information security related expenses and tools. <i>(FFIEC E-Banking Booklet, page 20)</i> Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. <i>(FFIEC Business Continuity Planning Booklet, page J-12)</i>	↑ Declarative Statement
	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.	

Management determines which declarative statements best fit the current practices of the institution. ***All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain's maturity level.*** Attained and sustained requires affirmative answers to either “Yes” or “Yes with Compensating Controls”³ for each of the declarative questions within a maturity level. While management can determine the institution's maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level.

Management may determine that a declarative statement has been sufficiently sustained based on proven results. Certain declarative statements may not apply to all institutions if the product, service, or technology is not offered or used. Declarative statements that may not be applicable to all institutions are clearly designated and would not affect the determination of the specific maturity level.

Interpreting and Analyzing Assessment Results

Management can review the institution's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain to understand whether they are aligned.

Table 3 depicts the relationship between an institution's Inherent Risk Profile and its domain Maturity Levels, as there is no single expected level for an institution. In general, as inherent risk

³Compensating control - A management, operational, and/or technical control (e.g., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

risks, an institution's maturity levels should increase. An institution's inherent risk profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change. Thus, management should consider reevaluating its inherent risk profile and cybersecurity maturity periodically and when planned changes can affect its inherent risk profile (e.g., launching new products or services, new connections).

Table 3: Risk/Maturity Relationship

		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative					
	Advanced					
	Intermediate					
	Evolving					
	Baseline					

If management determines that the institution's maturity levels are not appropriate in relation to the inherent risk profile, management should consider reducing inherent risk or developing a strategy to improve the maturity levels. This process includes

- determining target maturity levels.
- conducting a gap analysis.
- prioritizing and planning actions.
- implementing changes.
- reevaluating over time.
- communicating the results.

Management can set target maturity levels for each domain or across domains based on the institution's business objectives and risk appetite. Management can conduct a gap analysis between the current and target maturity levels and initiate improvements based on the gaps. Each declarative statement can represent a range of strategies and processes that have enterprise-wide impact. For example, declarative statements not yet attained provide insights for policies, processes, procedures, and controls that may improve risk management in relation to a specific risk or the institution's overall cybersecurity preparedness.

Using the maturity levels in each domain, management can identify potential actions that would increase the institution's overall cybersecurity preparedness. Management can review declarative statements at maturity levels beyond what the institution has achieved to determine the actions needed to reach the next level and implement changes to address gaps. Management's periodic

reevaluations of the inherent risk profile and maturity levels may further assist the institution in maintaining an appropriate level of cybersecurity preparedness. In addition, management may also seek an independent validation, such as by the internal audit function, of the institution's Assessment process and findings.

The Assessment results should be communicated to the chief executive officer (CEO) and board. More information and questions to consider are contained in the "[Overview for Chief Executive Officers and Boards of Directors](#)."

Resources

In addition to the "Overview for Chief Executive Officers and Boards of Directors," the FFIEC has released the following documents to assist institutions with the Cybersecurity Assessment Tool.

- [Appendix A: Mapping Baseline Statements to FFIEC IT Examination Handbook](#)
- [Appendix B: Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework](#)
- [Appendix C: Glossary](#)

Inherent Risk Profile

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)
Personal devices allowed to connect to the corporate network	None	Only one device type available; available to <5% of employees (staff, executives, managers); e-mail access only	Multiple device types used; available to <10% of employees (staff, executives, managers) and board; e-mail access only	Multiple device types used; available to <25% of authorized employees (staff, executives, managers) and board; e-mail and some applications accessed	Any device type used; available to >25% of employees (staff, executives, managers) and board; all applications accessed
Third parties, including number of organizations and number of individuals from vendors and subcontractors, with access to internal systems (e.g., virtual private network, modem, intranet, direct connection)	No third parties and no individuals from third parties with access to systems	Limited number of third parties (1–5) and limited number of individuals from third parties (<50) with access; low complexity in how they access systems	Moderate number of third parties (6–10) and moderate number of individuals from third parties (50–500) with access; some complexity in how they access systems	Significant number of third parties (11–25) and significant number of individuals from third parties (501–1,500) with access; high level of complexity in terms of how they access systems	Substantial number of third parties (>25) and substantial number of individuals from third parties (>1,500) with access; high complexity in how they access systems

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Wholesale customers with dedicated connections	None	Few dedicated connections (between 1–5)	Several dedicated connections (between 6–10)	Significant number of dedicated connections (between 11–25)	Substantial number of dedicated connections (>25)
Internally hosted and developed or modified vendor applications supporting critical activities	No applications	Few applications (between 1–5)	Several applications (between 6–10)	Significant number of applications (between 11–25)	Substantial number of applications and complexity (>25)
Internally hosted, vendor-developed applications supporting critical activities	Limited applications (0–5)	Few applications (6–30)	Several applications (31–75)	Significant number of applications (76–200)	Substantial number of applications and complexity (>200)
User-developed technologies and user computing that support critical activities (includes Microsoft Excel spreadsheets and Access databases or other user-developed tools)	No user-developed technologies	1–100 technologies	101–500 technologies	501–2,500 technologies	>2,500 technologies
End-of-life (EOL) systems	No systems (hardware or software) that are past EOL or at risk of nearing EOL within 2 years	Few systems that are at risk of EOL and none that support critical operations	Several systems that will reach EOL within 2 years and some that support critical operations	A large number of systems that support critical operations at EOL or are at risk of reaching EOL in 2 years	Majority of critical operations dependent on systems that have reached EOL or will reach EOL within the next 2 years or an unknown number of systems that have reached EOL
Open Source Software (OSS)	No OSS	Limited OSS and none that support critical operations	Several OSS that support critical operations	Large number of OSS that support critical operations	Majority of operations dependent on OSS
Network devices (e.g., servers, routers, and firewalls; include physical and virtual)	Limited or no network devices (<250)	Few devices (250–1,500)	Several devices (1,501–25,000)	Significant number of devices (25,001–50,000)	Substantial number of devices (>50,000)
Third-party service providers storing and/or processing information that support critical activities (Do not have access to internal systems, but the institution relies on their services)	No third parties that support critical activities	1–25 third parties that support critical activities	26–100 third parties that support critical activities	101–200 third parties that support critical activities; 1 or more are foreign-based	>200 third parties that support critical activities; 1 or more are foreign-based

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Cloud computing services hosted externally to support critical activities	No cloud providers	Few cloud providers; private cloud only (1–3)	Several cloud providers (4–7)	Significant number of cloud providers (8–10); cloud-provider locations used include international; use of public cloud	Substantial number of cloud providers (>10); cloud-provider locations used include international; use of public cloud

Category: Delivery Channels	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Online presence (customer)	No Web-facing applications or social media presence	Serves as an informational Web site or social media page (e.g., provides branch and ATM locations and marketing materials)	Serves as a delivery channel for retail online banking; may communicate to customers through social media	Serves as a delivery channel for wholesale customers; may include retail account origination	Internet applications serve as a channel to wholesale customers to manage large value assets
Mobile presence	None	SMS text alerts or notices only; browser-based access	Mobile banking application for retail customers (e.g., bill payment, mobile check capture, internal transfers only)	Mobile banking application includes external transfers (e.g., for corporate clients, recurring external transactions)	Full functionality, including originating new transactions (e.g., ACH, wire)
Automated Teller Machines (ATM) (Operation)	No ATM services	ATM services offered but no owned machines	ATM services managed by a third party; ATMs at local and regional branches; cash reload services outsourced	ATM services managed internally; ATMs at U.S. branches and retail locations; cash reload services outsourced	ATM services managed internally; ATM services provided to other financial institutions; ATMs at domestic and international branches and retail locations; cash reload services managed internally

Category: Online/Mobile Products and Technology Services	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Issue debit or credit cards	Do not issue debit or credit cards	Issue debit and/or credit cards through a third party; <10,000 cards outstanding	Issue debit or credit cards through a third party; between 10,000–50,000 cards outstanding	Issue debit or credit cards directly; between 50,000–100,000 cards outstanding	Issue debit or credit cards directly; >100,000 cards outstanding; issue cards on behalf of other financial institutions
Prepaid cards	Do not issue prepaid cards	Issue prepaid cards through a third party; <5,000 cards outstanding	Issue prepaid cards through a third party; 5,000–10,000 cards outstanding	Issue prepaid cards through a third party; 10,001–20,000 cards outstanding	Issue prepaid cards internally, through a third party, or on behalf of other financial institutions; >20,000 cards outstanding
Emerging payments technologies (e.g., digital wallets, mobile wallets)	Do not accept or use emerging payments technologies	Indirect acceptance or use of emerging payments technologies (customer use may affect deposit or credit account)	Direct acceptance or use of emerging payments technologies; partner or co-brand with non-bank providers; limited transaction volume	Direct acceptance or use of emerging payments technologies; small transaction volume; no foreign payments	Direct acceptance of emerging payments technologies; moderate transaction volume and/or foreign payments
Person-to-person payments (P2P)	Not offered	Customers allowed to originate payments; used by <1,000 customers or monthly transaction volume is <50,000	Customers allowed to originate payments; used by 1,000–5,000 customers or monthly transaction volume is between 50,000–100,000	Customers allowed to originate payments; used by 5,001–10,000 customers or monthly transaction volume is between 100,001–1 million	Customers allowed to request payment or to originate payment; used by >10,000 customers or monthly transaction volume >1 million
Originating ACH payments	No ACH origination	Originate ACH credits; daily volume <3% of total assets	Originate ACH debits and credits; daily volume is 3%–5% of total assets	Sponsor third-party payment processor; originate ACH debits and credits with daily volume 6%–25% of total assets	Sponsor nested third-party payment processors; originate debits and credits with daily volume that is >25% of total assets
Originating wholesale payments (e.g., CHIPS)	Do not originate wholesale payments	Daily originated wholesale payment volume <3% of total assets	Daily originated wholesale payment volume 3%–5% of total assets	Daily originated wholesale payment volume 6%–25% of total assets	Daily originated wholesale payment volume >25% of total assets

Category: Online/Mobile Products and Technology Services	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Wire transfers	Not offered	In person wire requests only; domestic wires only; daily wire volume <3% of total assets	In person, phone, and fax wire requests; domestic daily wire volume 3%–5% of total assets; international daily wire volume <3% of total assets	Multiple request channels (e.g., online, text, e-mail, fax, and phone); daily domestic wire volume 6%–25% of total assets; daily international wire volume 3%–10% of total assets	Multiple request channels (e.g., online, text, e-mail, fax, and phone); daily domestic wire volume >25% of total assets; daily international wire volume >10% of total assets
Merchant remote deposit capture (RDC)	Do not offer Merchant RDC	<100 merchant clients; daily volume of transactions is <3% of total assets	100–500 merchant clients; daily volume of transactions is 3%–5% of total assets	501–1,000 merchant clients; daily volume of transactions is 6%–25% of total assets	>1,000 merchant clients; daily volume of transactions is >25% of total assets
Global remittances	Do not offer global remittances	Gross daily transaction volume is <3% of total assets	Gross daily transaction volume is 3%–5% of total assets	Gross daily transaction volume is 6%–25% of total assets	Gross daily transaction volume is >25% of total assets
Treasury services and clients	No treasury management services are offered	Limited services offered; number of clients is <1,000	Services offered include lockbox, ACH origination, and remote deposit capture; number of clients is between 1,000–10,000	Services offered include accounts receivable solutions and liquidity management; number of clients is between 10,001–20,000	Multiple services offered including currency services, online investing, and investment sweep accounts; number of clients is >20,000
Trust services	Trust services are not offered	Trust services are offered through a third-party provider; assets under management total <\$500 million	Trust services provided directly; portfolio of assets under management total \$500 million–\$999 million	Trust services provided directly; assets under management total \$1 billion–\$10 billion	Trust services provided directly; assets under management total >\$10 billion
Act as a correspondent bank (Interbank transfers)	Do not act as a correspondent bank	Act as a correspondent bank for <100 institutions	Act as a correspondent bank for 100–250 institutions	Act as a correspondent bank for 251–500 institutions	Act as a correspondent bank for >500 institutions

Category: Online/Mobile Products and Technology Services	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Merchant acquirer (sponsor merchants or card processor activity into the payment system)	Do not act as a merchant acquirer	Act as a merchant acquirer; <1,000 merchants	Act as a merchant acquirer; outsource card payment processing; 1,000–10,000 merchants	Act as a merchant acquirer and card payment processor; 10,001–100,000 merchants	Act as a merchant acquirer and card payment processor; >100,000 merchants
Host IT services for other organizations (either through joint systems or administrative support)	Do not provide IT services for other organizations	Host or provide IT services for affiliated organizations	Host or provide IT services for up to 25 unaffiliated organizations	Host or provide IT services for 26–50 unaffiliated organizations	Host or provide IT services for >50 unaffiliated organizations

Category: Organizational Characteristics	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Mergers and acquisitions (including divestitures and joint ventures)	None planned	Open to initiating discussions or actively seeking a merger or acquisition	In discussions with at least 1 party	A sale or acquisition has been publicly announced within the past year, in negotiations with 1 or more parties	Multiple ongoing integrations of acquisitions are in process
Direct employees (including information technology and cybersecurity contractors)	Number of employees totals <50	Number of employees totals 50–2,000	Number of employees totals 2,001–10,000	Number of employees totals 10,001–50,000	Number of employees is >50,000
Changes in IT and information security staffing	Key positions filled; low or no turnover of personnel	Staff vacancies exist for non-critical roles	Some turnover in key or senior positions	Frequent turnover in key staff or senior positions	Vacancies in senior or key positions for long periods; high level of employee turnover in IT or information security
Privileged access (Administrators–network, database, applications, systems, etc.)	Limited number of administrators; limited or no external administrators	Level of turnover in administrators does not affect operations or activities; may utilize some external administrators	Level of turnover in administrators affects operations; number of administrators for individual systems or applications exceeds what is necessary	High reliance on external administrators; number of administrators is not sufficient to support level or pace of change	High employee turnover in network administrators; many or most administrators are external (contractors or vendors); experience in network administration is limited

Category: Organizational Characteristics	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Changes in IT environment (e.g., network, infrastructure, critical applications, technologies supporting new products or services)	Stable IT environment	Infrequent or minimal changes in the IT environment	Frequent adoption of new technologies	Volume of significant changes is high	Substantial change in outsourced provider(s) of critical IT services; large and complex changes to the environment occur frequently
Locations of branches/business presence	1 state	1 region	1 country	1–20 countries	>20 countries
Locations of operations/data centers	1 state	1 region	1 country	1–10 countries	>10 countries

Category: External Threats	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Attempted cyber attacks	No attempted attacks or reconnaissance	Few attempts monthly (<100); may have had generic phishing campaigns received by employees and customers	Several attempts monthly (100– 500); phishing campaigns targeting employees or customers at the institution or third parties supporting critical activities; may have experienced an attempted Distributed Denial of Service (DDoS) attack within the last year	Significant number of attempts monthly (501–100,000); spear phishing campaigns targeting high net worth customers and employees at the institution or third parties supporting critical activities; Institution specifically is named in threat reports; may have experienced multiple attempted DDoS attacks within the last year	Substantial number of attempts monthly (>100,000); persistent attempts to attack senior management and/or network administrators; frequently targeted for DDoS attacks

Total	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Number of Statements Selected in Each Risk Level					
Based on Individual Risk Levels Selected, Assign an Inherent Risk Profile	Least	Minimal	Moderate	Significant	Most

Cybersecurity Maturity

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

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

STRATEGY/ POLICIES

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

	Advanced	<p>The cybersecurity strategy outlines the institution’s future state of cybersecurity with short-term and long-term perspectives.</p> <p>Industry-recognized cybersecurity standards are used as sources during the analysis of cybersecurity program gaps.</p> <p>The cybersecurity strategy identifies and communicates the institution’s role as a component of critical infrastructure in the financial services industry.</p> <p>The risk appetite is informed by the institution’s role in critical infrastructure.</p> <p>Management is continuously improving the existing cybersecurity program to adapt as the desired cybersecurity target state changes.</p>
	Innovative	<p>The cybersecurity strategy identifies and communicates the institution’s role as it relates to other critical infrastructures.</p>
IT ASSET MANAGEMENT	Baseline	<p>An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. (FFIEC Information Security Booklet, page 9)</p> <p>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)</p> <p>Management assigns accountability for maintaining an inventory of organizational assets. (FFIEC Information Security Booklet, page 9)</p> <p>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)</p>
	Evolving	<p>The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets.</p> <p>The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards.</p> <p>The institution proactively manages system EOL (e.g., replacement) to limit security risks.</p> <p>Changes are formally approved by an individual or committee with appropriate authority and with separation of duties.</p>
	Intermediate	<p>Baseline configurations cannot be altered without a formal change request, documented approval, and an assessment of security implications.</p> <p>A formal IT change management process requires cybersecurity risk to be evaluated during the analysis, approval, testing, and reporting of changes.</p>

	Advanced	<p>Supply chain risk is reviewed before the acquisition of mission-critical information systems including system components.</p> <p>Automated tools enable tracking, updating, asset prioritizing, and custom reporting of the asset inventory.</p> <p>Automated processes are in place to detect and block unauthorized changes to software and hardware.</p> <p>The change management system uses thresholds to determine when a risk assessment of the impact of the change is required.</p>
	Innovative	<p>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.</p> <p>Comprehensive automated enterprise tools are implemented to detect and block unauthorized changes to software and hardware.</p>
Assessment Factor: Risk Management		
RISK MANAGEMENT PROGRAM	Baseline	<p>An information security and business continuity risk management function(s) exists within the institution. (FFIEC Information Security Booklet, page 68)</p>
	Evolving	<p>The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring, and reporting.</p> <p>Management reviews and uses the results of audits to improve existing cybersecurity policies, procedures, and controls.</p> <p>Management monitors moderate and high residual risk issues from the cybersecurity risk assessment until items are addressed.</p>
	Intermediate	<p>The cybersecurity function has a clear reporting line that does not present a conflict of interest.</p> <p>The risk management program specifically addresses cyber risks beyond the boundaries of the technological impacts (e.g., financial, strategic, regulatory, compliance).</p> <p>Benchmarks or target performance metrics have been established for showing improvements or regressions of the security posture over time.</p> <p>Management uses the results of independent audits and reviews to improve cybersecurity.</p> <p>There is a process to analyze and assign potential losses and related expenses, by cost center, associated with cybersecurity incidents.</p>

	Advanced	<p>Cybersecurity metrics are used to facilitate strategic decision-making and funding in areas of need.</p> <p>Independent risk management sets and monitors cyber-related risk limits for business units.</p> <p>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.</p> <p>A process is in place to analyze the financial impact cyber incidents have on the institution’s capital.</p> <p>The cyber risk data aggregation and real-time reporting capabilities support the institution’s ongoing reporting needs, particularly during cyber incidents.</p>
	Innovative	<p>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.</p> <p>A process is in place to analyze the financial impact that a cyber incident at the institution may have across the financial sector.</p>
RISK ASSESSMENT	Baseline	<p>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)</p> <p>The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls. (FFIEC Information Security Booklet, page 12)</p> <p>The risk assessment is updated to address new technologies, products, services, and connections before deployment. (FFIEC Information Security Booklet, page 13)</p>
	Evolving	<p>Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships.</p> <p>The focus of the risk assessment has expanded beyond customer information to address all information assets.</p> <p>The risk assessment considers the risk of using EOL software and hardware components.</p>
	Intermediate	<p>The risk assessment is adjusted to consider widely known risks or risk management practices.</p>

	Advanced	An enterprise-wide risk management function incorporates cyber threat analysis and specific risk exposure as part of the enterprise risk assessment.
	Innovative	<p>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.</p> <p>The institution uses information from risk assessments to predict threats and drive real-time responses.</p> <p>Advanced or automated analytics offer predictive information and real-time risk metrics.</p>
AUDIT	Baseline	<p>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)</p> <p>The independent audit function validates controls related to the storage or transmission of confidential data. (FFIEC Audit Booklet, page 1)</p> <p>Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance). (FFIEC Operations Booklet, page 29)</p> <p>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)</p>
	Evolving	<p>The independent audit function validates that the risk management function is commensurate with the institution's risk and complexity.</p> <p>The independent audit function validates that the institution's threat information sharing is commensurate with the institution's risk and complexity.</p> <p>The independent audit function validates that the institution's cybersecurity controls function is commensurate with the institution's risk and complexity.</p> <p>The independent audit function validates that the institution's third-party relationship management is commensurate with the institution's risk and complexity.</p> <p>The independent audit function validates that the institution's incident response program and resilience are commensurate with the institution's risk and complexity.</p>

	Intermediate	<p>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.</p> <p>The independent audit function validates that the institution’s threat intelligence and collaboration are commensurate with the institution’s risk and complexity.</p> <p>The independent audit function regularly reviews management’s cyber risk appetite statement.</p> <p>Independent audits or reviews are used to identify gaps in existing security capabilities and expertise.</p>
	Advanced	<p>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.</p> <p>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.</p> <p>Independent audits or reviews are used to identify cybersecurity weaknesses, root causes, and the potential impact to business units.</p>
	Innovative	<p>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.</p> <p>The independent audit function uses sophisticated data mining tools to perform continuous monitoring of cybersecurity processes or controls.</p>
Assessment Factor: Resources		
STAFFING	Baseline	<p>Information security roles and responsibilities have been identified. (FFIEC Information Security Booklet, page 7)</p> <p>Processes are in place to identify additional expertise needed to improve information security defenses. (FFIEC Information Security Work Program, Objective 1: 2-8)</p>

TRAINING	Evolving	<p>A formal process is used to identify cybersecurity tools and expertise that may be needed.</p> <p>Management with appropriate knowledge and experience leads the institution's cybersecurity efforts.</p> <p>Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position.</p> <p>Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk.</p>
	Intermediate	<p>The institution has a program for talent recruitment, retention, and succession planning for the cybersecurity and resilience staffs.</p>
	Advanced	<p>The institution benchmarks its cybersecurity staffing against peers to identify whether its recruitment, retention, and succession planning are commensurate.</p> <p>Dedicated cybersecurity staff develops, or contributes to developing, integrated enterprise-level security and cyber defense strategies.</p>
	Innovative	<p>The institution actively partners with industry associations and academia to inform curricula based on future cybersecurity staffing needs of the industry.</p>

Assessment Factor: Training and Culture

TRAINING	Baseline	<p>Annual information security training is provided. (FFIEC Information Security Booklet, page 66)</p> <p>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)</p> <p>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)</p> <p>Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials). (FFIEC E-Banking Work Program, Objective 6-3)</p>
-----------------	-----------------	--

	Evolving	<p>The institution has a program for continuing cybersecurity training and skill development for cybersecurity staff.</p> <p>Management is provided cybersecurity training relevant to their job responsibilities.</p> <p>Employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility.</p> <p>Business units are provided cybersecurity training relevant to their particular business risks.</p> <p>The institution validates the effectiveness of training (e.g., social engineering or phishing tests).</p>
	Intermediate	<p>Management incorporates lessons learned from social engineering and phishing exercises to improve the employee awareness programs.</p> <p>Cybersecurity awareness information is provided to retail customers and commercial clients at least annually.</p> <p>Business units are provided cybersecurity training relevant to their particular business risks, over and above what is required of the institution as a whole.</p> <p>The institution routinely updates its training to security staff to adapt to new threats.</p>
	Advanced	<p>Independent directors are provided with cybersecurity training that addresses how complex products, services, and lines of business affect the institution's cyber risk.</p>
	Innovative	<p>Key performance indicators are used to determine whether training and awareness programs positively influence behavior.</p>
CULTURE	Baseline	<p>Management holds employees accountable for complying with the information security program. (FFIEC Information Security Booklet, page 7)</p>
	Evolving	<p>The institution has formal standards of conduct that hold all employees accountable for complying with cybersecurity policies and procedures.</p> <p>Cyber risks are actively discussed at business unit meetings.</p> <p>Employees have a clear understanding of how to identify and escalate potential cybersecurity issues.</p>

Intermediate		<p>Management ensures performance plans are tied to compliance with cybersecurity policies and standards in order to hold employees accountable.</p> <p>The risk culture requires formal consideration of cyber risks in all business decisions.</p> <p>Cyber risk reporting is presented and discussed at the independent risk management meetings.</p>
Advanced		<p>Management ensures continuous improvement of cyber risk cultural awareness.</p>
Innovative		<p>The institution leads efforts to promote cybersecurity culture across the sector and to other sectors that they depend upon.</p>

Domain 2: Threat Intelligence and Collaboration			
Assessment Factor: Threat Intelligence			
		Y, Y(C), N	
THREAT INTELLIGENCE AND INFORMATION	Baseline		<p>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)</p> <p>Threat information is used to monitor threats and vulnerabilities. (FFIEC Information Security Booklet, page 83)</p> <p>Threat information is used to enhance internal risk management and controls. (FFIEC Information Security Booklet, page 4)</p>
	Evolving		Threat information received by the institution includes analysis of tactics, patterns, and risk mitigation recommendations.
	Intermediate		<p>A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources.</p> <p>Protocols are implemented for collecting information from industry peers and government.</p> <p>A read-only, central repository of cyber threat intelligence is maintained.</p>
	Advanced		<p>A cyber intelligence model is used for gathering threat information.</p> <p>Threat intelligence is automatically received from multiple sources in real time.</p> <p>The institution's threat intelligence includes information related to geopolitical events that could increase cybersecurity threat levels.</p>
	Innovative		<p>A threat analysis system automatically correlates threat data to specific risks and then takes risk-based automated actions while alerting management.</p> <p>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.</p>

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

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

<p>Innovative</p>	<p>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.</p> <p>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.</p> <p>The institution is leading efforts to create new sector-wide information-sharing channels to address gaps in external-facing information-sharing mechanisms.</p>
--------------------------	---

Domain 3: Cybersecurity Controls		
Assessment Factor: Preventative Controls		
	Y, Y(C), N	
INFRASTRUCTURE MANAGEMENT	Baseline	<p>Network perimeter defense tools (e.g., border router and firewall) are used. (FFIEC Information Security Booklet, page 33)</p> <p>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)</p> <p>All ports are monitored. (FFIEC Information Security Booklet, page 50)</p> <p>Up to date antivirus and anti-malware tools are used. (FFIEC Information Security Booklet, page 78)</p> <p>Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced. (FFIEC Information Security Booklet, page 56)</p> <p>Ports, functions, protocols and services are prohibited if no longer needed for business purposes. (FFIEC Information Security Booklet, page 50)</p> <p>Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. (FFIEC Information Security Booklet, page 56)</p> <p>Programs that can override system, object, network, virtual machine, and application controls are restricted. (FFIEC Information Security Booklet, page 41)</p> <p>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)</p> <p>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)</p>
	Evolving	<p>There is a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and internal network(s).</p> <p>Antivirus and intrusion detection/prevention systems (IDS/IPS) detect and block actual and attempted attacks or intrusions.</p> <p>Technical controls prevent unauthorized devices, including rogue wireless access devices and removable media, from connecting to the internal network(s).</p> <p>A risk-based solution is in place at the institution or Internet hosting</p>

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

ACCESS AND DATA MANAGEMENT		<p>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.</p>
	<p>Baseline</p>	<p>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)</p> <p>Employee access to systems and confidential data provides for separation of duties. (FFIEC Information Security Booklet, page 19)</p> <p>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)</p> <p>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)</p> <p>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)</p> <p>Identification and authentication are required and managed for access to systems, applications, and hardware. (FFIEC Information Security Booklet, page 21)</p> <p>Access controls include password complexity and limits to password attempts and reuse. (FFIEC Information Security Booklet, page 66)</p> <p>All default passwords and unnecessary default accounts are changed before system implementation. (FFIEC Information Security Booklet, page 61)</p> <p>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)</p> <p>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)</p> <p>Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems. (FFIEC Information Security Booklet, page 47)</p> <p>All passwords are encrypted in storage and in transit. (FFIEC Information Security Booklet, page 21)</p>

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

<p>Intermediate</p>		<p>The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.</p> <p>Controls are in place to prevent unauthorized escalation of user privileges.</p> <p>Access controls are in place for database administrators to prevent unauthorized downloading or transmission of confidential data.</p> <p>All physical and logical access is removed immediately upon notification of involuntary termination and within 24 hours of an employee's voluntary departure.</p> <p>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.</p> <p>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.)</p> <p>Confidential data are encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.</p> <p>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.)</p>
<p>Advanced</p>		<p>Encryption of select data at rest is determined by the institution's data classification and risk assessment.</p> <p>Customer authentication for high-risk transactions includes methods to prevent malware and man-in-the-middle attacks (e.g., using visual transaction signing).</p>

DEVICE/END-POINT SECURITY	Innovative	<p>Adaptive access controls de-provision or isolate an employee, third-party, or customer credentials to minimize potential damage if malicious behavior is suspected.</p> <p>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.</p> <p>Tokenization is used to substitute unique values for confidential information (e.g., virtual credit card).</p> <p>The institution is leading efforts to create new technologies and processes for managing customer, employee, and third-party authentication and access.</p> <p>Real-time risk mitigation is taken based on automated risk scoring of user credentials.</p>
	Baseline	<p>Controls are in place to restrict the use of removable media to authorized personnel. (FFIEC Information Security Work Program, Objective I: 4-1)</p>
	Evolving	<p>Tools automatically block attempted access from unpatched employee and third-party devices.</p> <p>Tools automatically block attempted access by unregistered devices to internal networks.</p> <p>The institution has controls to prevent the unauthorized addition of new connections.</p> <p>Controls are in place to prevent unauthorized individuals from copying confidential data to removable media.</p> <p>Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices).</p> <p>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.)</p> <p>The institution wipes data remotely on mobile devices when a device is missing or stolen. (*N/A if mobile devices are not used.)</p>
	Intermediate	<p>Data loss prevention controls or devices are implemented for inbound and outbound communications (e.g., e-mail, FTP, Telnet, prevention of large file transfers).</p> <p>Mobile device management includes integrity scanning (e.g., jailbreak/rooted detection). (*N/A if mobile devices are not used.)</p> <p>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.)</p>

	Advanced	<p>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.</p> <p>Confidential data and applications on mobile devices are only accessible via a secure, isolated sandbox or a secure container.</p>
	Innovative	<p>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.</p>
SECURE CODING	Baseline	<p>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)</p> <p>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)</p> <p>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)</p> <p>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)</p>
	Evolving	<p>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.)</p>
	Intermediate	<p>Processes are in place to mitigate vulnerabilities identified as part of the secure development of systems and applications.</p> <p>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.</p> <p>Software code executables and scripts are digitally signed to confirm the software author and guarantee that the code has not been altered or corrupted.</p> <p>A risk-based, independent information assurance function evaluates the security of internal applications.</p>
	Advanced	<p>Vulnerabilities identified through a static code analysis are remediated before implementing newly developed or changed applications into production.</p> <p>All interdependencies between applications and services have been</p>

		<p>identified.</p> <p>Independent code reviews are completed on internally developed or vendor-provided custom applications to ensure there are no security gaps.</p>
	Innovative	<p>Software code is actively scanned by automated tools in the development environment so that security weaknesses can be resolved immediately during the design phase.</p>
Assessment Factor: Detective Controls		
THREAT AND VULNERABILITY DETECTION	Baseline	<p>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)</p> <p>Antivirus and anti-malware tools are used to detect attacks. (FFIEC Information Security Booklet, page 55)</p> <p>Firewall rules are audited or verified at least quarterly. (FFIEC Information Security Booklet, page 82)</p> <p>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)</p>
	Evolving	<p>Independent penetration testing of network boundary and critical Web-facing applications is performed routinely to identify security control gaps.</p> <p>Independent penetration testing is performed on Internet-facing applications or systems before they are launched or undergo significant change.</p> <p>Antivirus and anti-malware tools are updated automatically.</p> <p>Firewall rules are updated routinely.</p> <p>Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices.</p> <p>Processes are in place to monitor potential insider activity that could lead to data theft or destruction.</p>
	Intermediate	<p>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.</p> <p>E-mails and attachments are automatically scanned to detect malware and are blocked when malware is present.</p>

	Advanced	<p>Weekly vulnerability scanning is rotated among environments to scan all environments throughout the year.</p> <p>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.</p> <p>Automated tool(s) proactively identifies high-risk behavior signaling an employee who may pose an insider threat.</p>
	Innovative	<p>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.</p> <p>Vulnerability scanning is performed on a weekly basis across all environments.</p>
ANOMALOUS ACTIVITY DETECTION	Baseline	<p>The institution is able to detect anomalous activities through monitoring across the environment. (FFIEC Information Security Booklet, page 32)</p> <p>Customer transactions generating anomalous activity alerts are monitored and reviewed. (FFIEC Wholesale Payments Booklet, page 12)</p> <p>Logs of physical and/or logical access are reviewed following events. (FFIEC Information Security Booklet, page 73)</p> <p>Access to critical systems by third parties is monitored for unauthorized or unusual activity. (FFIEC Outsourcing Booklet, page 26)</p> <p>Elevated privileges are monitored. (FFIEC Information Security Booklet, page 19)</p>
	Evolving	<p>Systems are in place to detect anomalous behavior automatically during customer, employee, and third-party authentication.</p> <p>Security logs are reviewed regularly.</p> <p>Logs provide traceability for all system access by individual users.</p> <p>Thresholds have been established to determine activity within logs that would warrant management response.</p>

<p>Intermediate</p>		<p>Online customer transactions are actively monitored for anomalous behavior.</p> <p>Tools to detect unauthorized data mining are used.</p> <p>Tools actively monitor security logs for anomalous behavior and alert within established parameters.</p> <p>Audit logs are backed up to a centralized log server or media that is difficult to alter.</p> <p>Thresholds for security logging are evaluated periodically.</p> <p>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).</p>
<p>Advanced</p>		<p>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.</p> <p>External transfers from customer accounts generate alerts and require review and authorization if anomalous behavior is detected.</p> <p>A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.</p> <p>An automated tool(s) is in place to detect and prevent data mining by insider threats.</p> <p>Tags on fictitious confidential data or files are used to provide advanced alerts of potential malicious activity when the data is accessed.</p>
<p>Innovative</p>		<p>The institution has a mechanism for real-time automated risk scoring of threats.</p> <p>The institution is developing new technologies that will detect potential insider threats and block activity in real time.</p>

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

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

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	<p>Data is destroyed or wiped on hardware and portable/mobile media when a device is missing, stolen, or no longer needed.</p> <p>Formal processes are in place to resolve weaknesses identified during penetration testing.</p>
	Intermediate	<p>Remediation efforts are confirmed by conducting a follow-up vulnerability scan.</p> <p>Penetration testing is repeated to confirm that medium- and high-risk, exploitable vulnerabilities have been resolved.</p> <p>Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties.</p> <p>Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action.</p> <p>The maintenance and repair of organizational assets are performed by authorized individuals with approved and controlled tools.</p> <p>The maintenance and repair of organizational assets are logged in a timely manner.</p>
	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, Y(C), N	
CONNECTIONS	Baseline		<p>The critical business processes that are dependent on external connectivity have been identified. (FFIEC Information Security Booklet, page 9)</p> <p>The institution ensures that third-party connections are authorized. (FFIEC Information Security Booklet, page 17)</p> <p>A network diagram is in place and identifies all external connections. (FFIEC Information Security Booklet, page 9)</p> <p>Data flow diagrams are in place and document information flow to external parties. (FFIEC Information Security Booklet, page 10)</p>
	Evolving		<p>Critical business processes have been mapped to the supporting external connections.</p> <p>The network diagram is updated when connections with third parties change or at least annually.</p> <p>Network and systems diagrams are stored in a secure manner with proper restrictions on access.</p> <p>Controls for primary and backup third-party connections are monitored and tested on a regular basis.</p>
	Intermediate		<p>A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.</p> <p>Security controls are designed and verified to detect and prevent intrusions from third-party connections.</p> <p>Monitoring controls cover all external connections (e.g., third-party service providers, business partners, customers).</p> <p>Monitoring controls cover all internal network-to-network connections.</p>
	Advanced		<p>The security architecture is validated and documented before network connection infrastructure changes.</p> <p>The institution works closely with third-party service providers to maintain and improve the security of external connections.</p>

	Innovative	<p>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.</p> <p>The institution's connections can be segmented or severed instantaneously to prevent contagion from cyber attacks.</p>
Assessment Factor: Relationship Management		
DUE DILIGENCE	Baseline	<p>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)</p> <p>A list of third-party service providers is maintained. (FFIEC Outsourcing Booklet, page 19)</p> <p>A risk assessment is conducted to identify criticality of service providers. (FFIEC Outsourcing Booklet, page 6)</p>
	Evolving	<p>A formal process exists to analyze assessments of third-party cybersecurity controls.</p> <p>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.</p>
	Intermediate	<p>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).</p> <p>Pre-contract, physical site visits of high-risk vendors are conducted by the institution or by a qualified third party.</p>
	Advanced	<p>A continuous process improvement program is in place for third-party due diligence activity.</p> <p>Audits of high-risk vendors are conducted on an annual basis.</p>
	Innovative	<p>The institution promotes sector-wide efforts to build due diligence mechanisms that lead to in-depth and efficient security and resilience reviews.</p> <p>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.</p>

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

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

Domain 5: Cyber Incident Management and Resilience			
Assessment Factor: Incident Resilience Planning and Strategy			
		Y, Y(C), N	
PLANNING	Baseline		<p>The institution has documented how it will react and respond to cyber incidents. (FFIEC Business Continuity Planning Booklet, page 4)</p> <p>Communication channels exist to provide employees a means for reporting information security events in a timely manner. (FFIEC Information Security Booklet, page 83)</p> <p>Roles and responsibilities for incident response team members are defined. (FFIEC Information Security Booklet, page 84)</p> <p>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)</p> <p>A formal backup and recovery plan exists for all critical business lines. (FFIEC Business Continuity Planning Booklet, page 4)</p> <p>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)</p>
	Evolving		<p>The remediation plan and process outlines the mitigating actions, resources, and time parameters.</p> <p>The corporate disaster recovery, business continuity, and crisis management plans have integrated consideration of cyber incidents.</p> <p>Alternative processes have been established to continue critical activity within a reasonable time period.</p> <p>Business impact analyses have been updated to include cybersecurity.</p> <p>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.</p>

	Intermediate	<p>A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.</p> <p>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.</p> <p>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.</p> <p>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.</p>
	Advanced	<p>Methods for responding to and recovering from cyber incidents are tightly woven throughout the business units' disaster recovery, business continuity, and crisis management plans.</p> <p>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.</p> <p>A process is in place to continuously improve the resilience plan.</p>
	Innovative	<p>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.</p> <p>The incident response process includes detailed actions and rule-based triggers for automated response.</p>
TESTING	Baseline	<p>Scenarios are used to improve incident detection and response. (FFIEC Information Security Booklet, page 71)</p> <p>Business continuity testing involves collaboration with critical third parties. (FFIEC Business Continuity Planning Booklet, page J-6)</p> <p>Systems, applications, and data recovery is tested at least annually. (FFIEC Business Continuity Planning Booklet, page J-7)</p>
	Evolving	<p>Recovery scenarios include plans to recover from data destruction and impacts to data integrity, data loss, and system and data availability.</p> <p>Widely reported events are used to evaluate and improve the institution's response.</p> <p>Information backups are tested periodically to verify they are accessible and readable.</p>

<p>Intermediate</p>	<p>Cyber-attack scenarios are analyzed to determine potential impact to critical business processes.</p> <p>The institution participates in sector-specific cyber exercises or scenarios (e.g., FS-ISAC Cyber Attack (against) Payment Processors (CAPP)).</p> <p>Resilience testing is based on analysis and identification of realistic and highly likely threats as well as new and emerging threats facing the institution.</p> <p>The critical online systems and processes are tested to withstand stresses for extended periods (e.g., DDoS).</p> <p>The results of cyber event exercises are used to improve the incident response plan and automated triggers.</p>
<p>Advanced</p>	<p>Resilience testing is comprehensive and coordinated across all critical business functions.</p> <p>The institution validates that it is able to recover from cyber events similar to by known sophisticated attacks at other organizations.</p> <p>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.</p> <p>The institution corrects root causes for problems discovered during cybersecurity resilience testing.</p> <p>Cybersecurity incident scenarios involving significant financial loss are used to stress test the institution's risk management.</p>
<p>Innovative</p>	<p>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.</p> <p>The institution has validated that it is able to remediate systems damaged by zero-day attacks to maintain current recovery time objectives.</p> <p>The institution is leading the development of more realistic test environments.</p> <p>Cyber incident scenarios are used to stress test potential financial losses across the sector.</p>

Assessment Factor: Detection, Response, and Mitigation		
DETECTION	Baseline	<p>Alert parameters are set for detecting information security incidents that prompt mitigating actions. (FFIEC Information Security Booklet, page 43)</p> <p>System performance reports contain information that can be used as a risk indicator to detect information security incidents. (FFIEC Information Security Booklet, page 86)</p> <p>Tools and processes are in place to detect, alert, and trigger the incident response program. (FFIEC Information Security Booklet, page 84)</p>
	Evolving	<p>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.</p>
	Intermediate	<p>The incident response program is triggered when anomalous behaviors and attack patterns or signatures are detected.</p> <p>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.</p> <p>Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.</p> <p>Network and system alerts are correlated across business units to better detect and prevent multifaceted attacks (e.g., simultaneous DDoS attack and account takeover).</p> <p>Incident detection processes are capable of correlating events across the enterprise.</p>
	Advanced	<p>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.</p> <p>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.</p>
	Innovative	<p>The institution is able to detect and block zero-day attempts and inform management and the incident response team in real time.</p>

RESPONSE AND MITIGATION	Baseline	<p>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)</p>
	Evolving	<p>The incident response plan is designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities.</p> <p>A process is in place to help contain incidents and restore operations with minimal service disruption.</p> <p>Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware).</p> <p>Procedures include containment strategies and notifying potentially impacted third parties.</p> <p>Processes are in place to trigger the incident response program when an incident occurs at a third party.</p> <p>Records are generated to support incident investigation and mitigation.</p> <p>The institution calls upon third parties, as needed, to provide mitigation services.</p> <p>Analysis of events is used to improve the institution's security measures and policies.</p>
	Intermediate	<p>Analysis of security incidents is performed in the early stages of an intrusion to minimize the impact of the incident.</p> <p>Any changes to systems/applications or to access entitlements necessary for incident management are reviewed by management for formal approval before implementation.</p> <p>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.</p> <p>Processes are in place to ensure that restored assets are appropriately reconfigured and thoroughly tested before being placed back into operation.</p>
	Advanced	<p>The incident management function collaborates effectively with the cyber threat intelligence function during an incident.</p> <p>Links between threat intelligence, network operations, and incident response allow for proactive response to potential incidents.</p> <p>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.</p>

	Innovative	<p>The institution's risk management of significant cyber incidents results in limited to no disruptions to critical services.</p> <p>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).</p>
Assessment Factor: Escalation and Reporting		
ESCALATION AND REPORTING	Baseline	<p>A process exists to contact personnel who are responsible for analyzing and responding to an incident. (FFIEC Information Security Booklet, page 83)</p> <p>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)</p> <p>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)</p> <p>Incidents are classified, logged, and tracked. (FFIEC Operations Booklet, page 28)</p>
	Evolving	<p>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.</p> <p>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.</p> <p>Tracked cyber incidents are correlated for trend analysis and reporting.</p>
	Intermediate	<p>Employees that are essential to mitigate the risk (e.g., fraud, business resilience) know their role in incident escalation.</p> <p>A communication plan is used to notify other organizations, including third parties, of incidents that may affect them or their customers.</p> <p>An external communication plan is used for notifying media regarding incidents when applicable.</p>
	Advanced	<p>The institution has established quantitative and qualitative metrics for the cybersecurity incident response process.</p> <p>Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the board meeting package.</p>

	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.
--	-------------------	---

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	
	<p>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.</p> <p><i>Source:</i> IS.I:pg3 The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions.</p> <p>IS.I:pg4: The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program.</p> <p>IS.WP.2.3: Determine whether the board holds management accountable for the following: Central oversight and coordination, Assignment of responsibility, Support of the information security program, and Effectiveness of the information security program.</p> <p>MGT.III.C.3:pg28: The board of directors is responsible for overseeing the development, implementation, management, and maintenance of the institution's information security program. This oversight includes assigning specific responsibility and accountability for the program's implementation and reviewing reports from management.</p> <p>MGT.WP.2: Determine whether the board of directors oversees and senior management appropriately establishes an effective governance structure that includes oversight of IT activities.</p> <p>MGT.WP.2.2.g: Review whether the board or a committee of the board appropriately holds management accountable for the identification, measurement, and mitigation of IT risks.</p>
	<p>Governance/Oversight: Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.</p> <p><i>Source:</i> IS.I.B:pg4: Management also should do the following: Participate in assessing the effect of security threats or incidents on the institution and its lines of business and processes.</p> <p>IS.III.A:pg47: Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information.</p>

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

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Governance/Oversight: Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution.</p> <p><i>Source: BCP.B.J-12:</i> 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.</p> <p><i>BCP.WP.10:</i> 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.</p>
	<p>Governance/Strategy-Policies: The institution has an information security strategy that integrates technology, policies, procedures, and training to mitigate risk.</p> <p><i>Source: IS.Introduction:pg2:</i> Information security is far more effective when management does the following: Integrates processes, people, and technology to maintain a risk profile that is in accordance with the board's risk appetite. Aligns the information security program with the enterprise risk management program and identifies, measures, mitigates, and monitors risk.</p> <p><i>IS.WP.6.3:</i> Determine whether the institution continually assesses the capability of technology needed to sustain an appropriate level of information security based on the size, complexity, and risk appetite of the institution.</p> <p><i>MGT.III.C.1:pg27:</i> Senior management should ensure that policies, standards, and procedures are current, well documented, and integrated with the institution's information security strategy.</p> <p><i>MGT.WP.4.3:</i> Determine whether the institution has adequate tactical and operational IT plans to support the larger IT strategic plans.</p>
	<p>Governance/Strategy-Policies: The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management.</p> <p><i>Source: IS.II:pg6:</i> Management should develop and implement an information security program that does the following: Supports the institution's IT risk management (ITRM) process by identifying threats, measuring risk, defining information security requirements, and implementing controls.</p> <p><i>IS.WP.3.1:</i> Determine whether the institution has an effective information security program that supports the ITRM process.</p> <p><i>MGT.III.C.1:pg27:</i> Institution management should create, document, maintain, and adhere to policies, standards, and procedures to manage and control the institution's IT risk. The level of detail depends on the complexity of the IT environment but should enable management to monitor the identified risk posture.</p> <p><i>MGT.WP.12.4:</i> Determine whether IT management has developed adequate policies, standards, and procedures to manage the risk from technology and that they are current, documented, and appropriately communicated.</p>

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

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

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

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Risk Management/Risk Management Program: An information security and business continuity risk management function(s) exists within the institution.</p> <p><i>Source:</i> IS.II.C.21:pg43: Management should do the following: Identify personnel who will have critical information security roles during a disaster, and train personnel in those roles. Define information security needs for backup sites and alternate communication networks. Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios.</p> <p><i>IS.WP.6.34:</i> Determine whether management effectively manages the following information security considerations related to business continuity planning.</p> <p>MGT.I.B.4:pg12: The business continuity function often resides in the risk management organizational structure. A specific member of management should be assigned responsibility for the oversight of the business continuity function, and both business and technology departments should assign personnel to develop and maintain the individual business unit plans.</p> <p>MGT.WP.3.: As part of the ITRM structure, determine whether financial institution management has defined IT responsibilities and functions. Verify the existence of well-defined responsibilities and expectations between risk management and IT functional areas, such as information security, project management, business continuity, and information systems reporting.</p>
	<p>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.</p> <p><i>Source:</i> IS.I.B:pg4: Management should provide a report to the board at least annually that describes the overall status of the program and material matters related to the program, including the following: Risk assessment process, including threat identification and assessment.</p> <p>IS.WP.2.4: Determine whether the board approves a written information security program and receives a report on the effectiveness of the information security program at least annually. Determine whether the report to the board describes the overall status of the information security program and discusses material matters related to the program such as the following:</p> <ol style="list-style-type: none"> a. Risk assessment process, including threat identification and assessment. <p>MGT.III.A:pg22: Comprehensive IT risk identification should include identification of cybersecurity risks as well as details gathered during information security risk assessments required under guidelines implementing the GLBA.</p> <p>MGT.WP.7.4: Determine whether the institution maintains a risk assessment process to perform the following:</p> <ol style="list-style-type: none"> a. Identify risks and threats from both internal and external sources. b. Develop or update policies within the risk management function to guide risk measurement activities. c. Ensure the existence of a process to promote sound understanding and analysis of threats, events, assets, and controls. d. Maintain processes within the risk management function to help make risk mitigation decisions. e. Determine the entities that should have involvement in that decision-making process. f. Ensure that the board and management understand the risk categories.

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

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>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.</p> <p><i>Source: AUD.B.4:</i> The internal audit manager should be responsible for internal control risk assessments, audit plans, audit programs, and audit reports associated with IT.</p> <p>IS.IV.A.2(d):pg56: Independent internal departments or third parties typically perform audits. Audits should review every aspect of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the reasonableness and appropriateness of, and compliance with, policies, standards, and procedures; report on information security activity and control deficiencies to decision makers; identify root causes and recommendations to address deficiencies; and test the effectiveness of controls within the program.</p> <p>MGT.I.B.7(b)pg19: IT auditors should validate that IT controls are designed appropriately to mitigate risk and are operating as management intended. IT audit should be completely independent, should have no role in designing or implementing controls, and should not have primary responsibility for enforcing policy.</p> <p>MGT.WP.6.3: Determine whether the board, or its committee, has appropriate oversight of audit through the following:</p> <ol style="list-style-type: none"> a. Audit risk assessment and audit plan. b. Audit review activities. c. Audit reports with identified weaknesses. d. Management's responses and corrective actions to audit issues. e. Updates on any audit concerns and the status of issues.
	<p>Risk Management/Audit: The independent audit function validates controls related to the storage or transmission of confidential data.</p> <p><i>Source: AUD.B.1:</i> An effective IT audit program should... promote the confidentiality, integrity, and availability of information systems.</p>
	<p>Risk Management/Audit: Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance).</p> <p><i>Source: OPS.B.29:</i> Operations management should periodically review all logs for completeness and ensure they have not been deleted, modified, overwritten, or compromised.</p> <p>IS.II.C.22:pg43: Logging practices should be reviewed periodically by an independent party to ensure appropriate log management.</p> <p>IS.WP.6.35(c): Review whether management has the following: Independent review of logging practices.</p>

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>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.</p> <p><i>Source:</i> IS.IV.A.2(d):pg56: Internal audit should track the results and the remediation of control deficiencies reported in audits and additional technical reviews, such as penetration tests and vulnerability assessments.</p> <p>IS.WP.2.8: Determine the adequacy of audit coverage and reporting of the information security program by reviewing appropriate audit reports and board or audit committee minutes.</p> <p>AUD.B.8: A risk assessment process to describe and analyze the risks inherent in a given line of business.</p> <p>AUD.WP.I.7.1: Determine the adequacy of the overall audit plan in providing appropriate coverage of IT risks.</p> <p>MGT.I.B.7(b):pg19: Management should also ensure timely and accurate response to audit concerns and exceptions and ensure appropriate and timely corrective action.</p> <p>MGT.WP.1.2: Review management's response to issues raised during, or since, the last examination. Consider the following: a. Adequacy and timing of corrective action. b. Resolution of root causes rather than just specific issues. c. Existence of any outstanding issues. d. Whether management has taken positive action toward correcting exceptions reported in audit and examining reports. e. Independent review of resolution and reporting of resolution to the audit committee.</p> <p>MGT.WP.6.1: Consult with the examiner reviewing audit or IT audit to determine the adequacy of IT audit coverage and management's responsiveness to identified weaknesses.</p>
	<p>Resources/Staffing: Information security roles and responsibilities have been identified.</p> <p><i>Source:</i> IS.II.C.1:pg11: Policies, standards, and procedures guide decisions and activities of users, developers, administrators, and managers and inform those individuals of their information security responsibilities. Policies, standards, and procedures should also specify the mechanisms through which responsibilities can be met. ... Policies, standards, and procedures that address the information security program should describe the roles of the information security department, lines of business, and IT organization in administering the information security program.</p> <p>MGT.I:pg4: The governance structure specifies the responsibilities for the board of directors, managers, auditors, and other stakeholders and specifies the level of authority and accountability for decision making.</p> <p>MGT.WP.2.11: Review the institution's structure to determine whether the board established the following:</p> <ul style="list-style-type: none"> a. The organizational structure provides for effective IT support throughout the institution, from IT management up through senior management and the board. b. Defined roles and responsibilities for key IT positions, including executive management (CEO and COO, and often CIO or CTO), and CISO. e. A CISO or information security officer position responsible for the management and mitigation of information security risks.

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

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Training and Culture/Training: Situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts.</p> <p><i>Source:</i> IS.II.C.7(e):pg17:: Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training.</p> <p>IS.WP.6.8.f: Determine whether management effectively mitigates risks posed by users. Review whether management does the following: Provides training to support awareness and policy compliance.</p>
	<p>Training and Culture/Training: Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials).</p> <p><i>Source:</i> IS.II.C.16:pg36: Beyond authentication, remote access controls should include additional layered security controls and may include some combination of the following: Customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.</p> <p>IS.II.C.16(a): pg37: The institution's customer awareness and education efforts should consider both retail and commercial account holders.</p> <p>IS.WP.6.26: Determine whether management develops customer awareness and education efforts that address both retail (consumer) and commercial account holders.</p>
	<p>Training and Culture/Culture: Management holds employees accountable for complying with the information security program.</p> <p><i>Source:</i> IS.II.C.7(e):pg17: Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected.</p> <p>MGT.III.C.2:pg28: Management should require periodic acknowledgement of acceptable use policies for the network, software applications, Internet, e-mail, confidential data, and social media. Information security awareness and training programs help support information security and other management policies.</p> <p>MGT.WP.12.5: Determine whether management has effective hiring and training practices that include the following:</p> <ul style="list-style-type: none"> d. Requiring periodic acknowledgement of acceptable use policies. e. Obtaining signed confidentiality and nondisclosure agreements. f. Providing information security awareness and training programs.

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

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

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Information Sharing/Information Sharing: Information security threats are gathered and shared with applicable internal employees.</p> <p><i>Source:</i> IS.II.D:pg45: Risk reporting is a process that produces information systems reports that address threats, capabilities, vulnerabilities, and inherent risk changes. Risk reporting should describe any information security events that the institution faces and the effectiveness of management's response and resilience to those events. The reporting process should provide a method of disseminating those reports to appropriate members of management. The contents of the reports should prompt action, if necessary, in a timely manner to maintain appropriate levels of risk.</p> <p>IS.WP.7.1: Determine whether the institution has risk monitoring and reporting processes that address changing threat conditions in both the institution and the greater financial industry. Determine whether these processes address information security events faced by the institution, the effectiveness of management's response, and the institution's resilience to those events. Review whether the reporting process includes a method of disseminating those reports to appropriate members of management.</p>
	<p>Information Sharing/Information Sharing: Contact information for law enforcement and the regulator(s) is maintained and updated regularly.</p> <p><i>Source:</i> BCP.WP.1.5.1: 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.</p> <p>IS.III.D:pg.51: Primary considerations for incident response include the following: Protocols to define when and under what circumstances to notify and involve regulators, customers, and law enforcement, including names and contact information for each group.</p> <p>MGT.III.C.3:pg29: Develop a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulator based on thresholds defined by the financial institution and applicable legal requirements. Relevant thresholds could include significant financial impact, significant operational downtime, operational or system breach, or loss of critical infrastructure.</p> <p>MGT.WP.12.8.i: Developing a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulators based on thresholds defined by the financial institution.</p>
	<p>Information Sharing/Information Sharing: Information about threats is shared with law enforcement and regulators when required or prompted.</p> <p><i>Source:</i> IS.III.D:pg.51: Primary considerations for incident response include the following: How, when, and what to communicate outside of the institution, whether to law enforcement, regulatory agencies, information-sharing organizations, customers, third-party service providers, potential victims, or others.</p> <p>MGT.III.C.3:pg29: Develop a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulator based on thresholds defined by the financial institution and applicable legal requirements. Relevant thresholds could include significant financial impact, significant operational downtime, operational or system breach, or loss of critical infrastructure.</p> <p>MGT.WP.12.8.i: Developing a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's primary federal and state regulators based on thresholds defined by the financial institution.</p>

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

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

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

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

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

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

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

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>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.</p> <p><i>Source:</i> IS.II.C.17:pg38: A secure software development life cycle ensures that Internet- and client-facing applications have the necessary security controls. The institution should ensure that all applications are securely developed.... At institutions that employ third parties to develop applications, management should ensure that the third parties meet the same controls.</p> <p>IS.WP.6.27: Determine whether management uses applications that were developed by following secure development practices and that meet a prudent level of security.</p> <p>MGT.III.C.5:pg31: Management should guide the development or acquisition of software by using a system development life cycle (SDLC) or similar methodology appropriate for the specific IT environment. The extent or use of the SDLC depends on the size and complexity of the institution and the type of development activities performed. If the institution primarily acquires software, management should verify the effective use of an SDLC by the third-party provider.</p> <p>MGT.WP.12.10. Determine whether management assesses and mitigates the operational risks associated with the development or acquisition of software. Appropriate management of the risks should include the following:</p> <ul style="list-style-type: none"> a. Policies documenting risk management controls for the development and acquisition of systems. b. System development life cycle or similar methodology based on the complexity and type of development performed.
	<p>Preventive Controls/Secure Coding: The security controls of internally developed software are periodically reviewed and tested. (*N/A if there is no software development.)</p> <p><i>Source:</i> IS.II.C.10:pg21: The process for introducing software should encompass securely developing, implementing, and testing changes to both internally developed and acquired software.</p> <p>IS.WP.6.15: Determine whether management has a process to update and patch operating systems, network devices, and software applications, including internally developed software provided to customers, for newly discovered vulnerabilities.</p> <p>MGT.III.C.5:pg31: Testing, which should include tests of security, validates that equipment and systems function properly and produce the desired results. As part of the testing process, management should verify whether new technology systems operate effectively with other technology components, including vendor-supplied technology. Management should conduct retesting periodically to help manage risk exposure on an ongoing basis.</p> <p>MGT.WP.12.10. Determine whether management assesses and mitigates the operational risks associated with the development or acquisition of software. Appropriate management of the risks should include the following:</p> <ul style="list-style-type: none"> a. Policies documenting risk management controls for the development and acquisition of systems. b. System development life cycle or similar methodology based on the complexity and type of development performed. c. Tests of new technology, systems, and products before deployment to validate functionality, controls, and interoperability.

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>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.)</p> <p><i>Source:</i> 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.</p> <p>D&A.B.9: Independence – Audit and quality assurance personnel should be independent of the project they are reviewing.</p> <p>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.</p> <p>MGT.III.C.5:pg31: Audit should review the SDLC to ensure that appropriate controls are incorporated during development. Management should test new technology, systems, and products thoroughly before deployment.</p> <p>MGT.WP.12.10.c: Appropriate management of the risks should include tests of new technology, systems, and products before deployment to validate functionality, controls, and interoperability.</p>
	<p>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.)</p> <p><i>Source:</i> 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.</p> <p>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.</p>
	<p>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.</p> <p><i>Source:</i> ISIS.II.C.17:pg38: To verify the controls have been developed and implemented appropriately, management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications.</p> <p>IS.WP.4.2.d: Review whether management has the following: A validation of the risk identification process through audits, self-assessments, penetration tests, and vulnerability assessments.</p> <p>MGT.III.C.3:pg29: Perform penetration tests before launching or making significant changes to critical systems, including Internet- and client-facing applications. Management should review all findings and develop processes to ensure the timely remediation of issues identified by the tests.</p> <p>MGT.WP.12.8.f: Determine whether, as part of the institution’s information security program, the board of directors oversees and management establishes a control structure that is intended to specifically address cybersecurity risks and includes the following: Performing penetration tests before launching new or making significant changes to existing Internet- and client-facing applications and remediating findings from the tests.</p>

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

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Detective Controls/Anomalous Activity Detection: Logs of physical and/or logical access are reviewed following events.</p> <p><i>Source:</i> IS.III.C.22:pg44: Institutions maintain event logs to understand an incident or cyber event after it occurs. Monitoring event logs for anomalies and relating that information with other sources of information broadens the institution's ability to understand trends, react to threats, and improve reports to management and the board.</p> <p>IS.WP.6.21(f): As part of management's process to secure the operating system and all system components, determine whether management does the following: Filters and reviews logs for potential security events and provides adequate reports and alerts.</p>
	<p>Detective Controls/Anomalous Activity Detection: Access to critical systems by third parties is monitored for unauthorized or unusual activity.</p> <p><i>Source:</i> OT.B.26: Appropriate access controls and monitoring should be in place between service provider's systems and the institution.</p>
	<p>Detective Controls/Anomalous Activity Detection: Elevated privileges are monitored.</p> <p><i>Source:</i> IS.II.C.15:pg31: Authorization for privileged access should be tightly controlled.</p> <p>IS.WP.8.4.f: Determine whether management has effective threat monitoring processes, including the following: Establishing and documenting a process to independently monitor administrators and other users with higher privileges.</p>
	<p>Detective Controls/Event Detection: A normal network activity baseline is established.</p> <p><i>Source:</i> IS.III.C:pg49: Incident identification involves indicators and analysis. ...Examples of technology-based intrusion identification systems and tools include the following:...Network behavior analysis systems.</p> <p>IS.WP.8.4.e: Determine whether management has effective threat monitoring processes, including the following: Monitoring both incoming and outgoing network traffic to identify malicious activity and data exfiltration.</p>
	<p>Detective Controls/Event Detection: Mechanisms (e.g., anti-virus alerts, log event alerts) are in place to alert management to potential attacks.</p> <p><i>Source:</i> IS.III.B:pg48: Threat monitoring policies should provide for continual and ad hoc monitoring of threat intelligence communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal procedures.... Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies.</p> <p>IS.WP.8.5: Determine whether management has effective incident identification and assessment processes to do the following:</p> <ul style="list-style-type: none"> e. Escalate the event consistent with the classification. f. Report internally and externally as appropriate.
	<p>Detective Controls/Event Detection: Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.</p> <p><i>Source:</i> IS.Introduction:pg2: Aligns the information security program with the enterprise risk management program and identifies, measures, mitigates, and monitors risk...Management should be able to identify and characterize the threats, assess the risks, make decisions regarding the implementation of appropriate controls, and provide appropriate monitoring and reporting.</p>

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Detective Controls/Event Detection: Responsibilities for monitoring and reporting suspicious systems activity have been assigned.</p> <p><i>Source:</i> IS.III.B:pg48: Management should establish the responsibility and authority of security personnel and system administrators for monitoring. Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies.</p> <p>IS.WP.8.4.b: Determine whether management has effective threat monitoring processes, including the following: Establishing responsibility and accountability for security personnel and system administrators for monitoring.</p>
	<p>Detective Controls/Event Detection: The physical environment is monitored to detect potential unauthorized access.</p> <p><i>Source:</i> IS.II.C.8:pg18: Management should implement appropriate preventive, detective, and corrective controls for physical security.</p> <p>IS.WP.6.9: Determine whether management applies appropriate physical security controls to protect its premises and more sensitive areas, such as its data center(s).</p>
	<p>Corrective Controls/Patch Management: A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner.</p> <p><i>Source:</i> IS.II.C.10(d):pg24: Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated.</p> <p>IS.WP.6.15: Determine whether management has a process to update and patch operating systems, network devices, and software applications, including internally developed software provided to customers, for newly discovered vulnerabilities.</p> <p>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.</p> <p>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.</p>
	<p>Corrective Controls/Patch Management: Patches are tested before being applied to systems and/or software.</p> <p><i>Source:</i> 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.</p> <p>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.</p>
	<p>Corrective Controls/Patch Management: Patch management reports are reviewed and reflect missing security patches.</p> <p><i>Source:</i> 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.</p>

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

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Connections/Connections: Data flow diagrams are in place and document information flow to external parties.</p> <p><i>Source:</i> IS.II.C.9:pg20: To ensure appropriate network security, management should maintain accurate network and data flow diagrams, and store them securely, providing access only to essential personnel. These diagrams should identify hardware, software, and network components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture.</p> <p>IS.WP.6.10.b: Determine whether management secures access to its computer networks through multiple layers of access controls. Review whether management does the following: Maintains accurate network diagrams and data flow charts.</p>
	<p>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.</p> <p><i>Source:</i> IS.II.C.20:pg42: Management should oversee outsourced operations through the following: Appropriate due diligence in third-party research, selection, and relationship management.</p> <p>IS.WP.6.31: Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. Review the due diligence involved, security controls to mitigate risk, and monitoring capabilities over the institution's third parties.</p> <p>MGT.III.C.8:pg34: An effective third-party management program should provide the framework for management to identify, measure, mitigate, monitor, and report risks associated with the use of third-party providers. Management should develop and implement enterprise-wide policies and procedures to govern the third-party management program, including establishing objectives and strategies, selecting a provider, negotiating the contract, and monitoring the outsourced relationship.</p> <p>MGT.WP.12.14.d: An effective third-party management program should incorporate: Evaluation of prospective third-party providers based on the scope and criticality of services provided.</p>
	<p>Relationship Management/Due Diligence: A list of third-party service providers is maintained.</p> <p><i>Source:</i> 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.</p> <p>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.</p>

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Relationship Management/Due Diligence: A risk assessment is conducted to identify criticality of service providers.</p> <p><i>Source:</i> 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.</p> <p>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.</p> <p>MGT.III.C.8:pg34: Management should evaluate the quality of service, control environment, and financial condition of the third parties providing the institution with critical IT services.</p> <p>MGT.III.C.8:pg35: Some factors that management should consider or address regarding an effective third-party management program include the following: Tailoring the institution's third-party management program based on an initial and ongoing risk assessment of the institution's third parties and the services they provide.</p> <p>MGT.WP.12.14: An effective third-party management program should incorporate the following:</p> <ul style="list-style-type: none"> d. Evaluation of prospective third-party providers based on the scope and criticality of services provided. e. Tailoring of the monitoring program based on the initial and ongoing risk assessment of the third party and the services provided..
	<p>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.</p> <p><i>Source:</i> IS.II.C.20:pg42: If the third-party service provider stores, transmits, processes, or disposes of customer information, management should require third- party service providers by contract to implement appropriate measures designed to meet the Information Security Standards.</p> <p>IS.WP.6.31(c): Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. Review the due diligence involved, security controls to mitigate risk, and monitoring capabilities over the institution's third parties. Review the institution's policies, standards, and procedures related to the use of the following: ...Contractual assurances from third-party service providers for security responsibilities, controls, and reporting.</p> <p>MGT.III.C.8:pg35: Third parties should support the responsibilities of their financial institution clients to adhere to all applicable laws, regulations, and supervisory guidance .</p> <p>MGT.III.C.8:pg35: When financial institution management contracts with third-party providers for some or all IT services, it should ensure that controls over outsourced activities provide the institution with the same level of assurance as controls over those activities performed in-house.</p>
	<p>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.</p> <p><i>Source:</i> IS.II.C.20:pg42: Management should oversee outsourced operations through the following: Contractual assurances for security responsibilities, controls, and reporting.</p> <p>IS.WP.6.31(c): Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. ... Review the institution's policies, standards, and procedures related to the use of the following: Contractual assurances from third-party service providers for security responsibilities, controls, and reporting.</p>

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Relationship Management/Contracts: Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party.</p> <p><i>Source:</i> IS.II.C.20:pg42: Management should verify that third-party service providers implement and maintain controls sufficient to appropriately mitigate risks. The institution's contracts should do the following: ...Specify that the institution or an independent auditor has access to the service provider to perform evaluations of the service provider's performance against the Information Security Standards.</p> <p>IS.WP.6.31.e: Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers. ...Review the institution's policies, standards, and procedures related to the use of the following: Independent review of the third-party service provider's security through appropriate reports from audits and tests.</p>
	<p>Relationship Management/Contracts: Contracts identify the recourse available to the institution should the third party fail to meet defined security requirements.</p> <p><i>Source:</i> OT.B.12: Institutions should include performance standards that define minimum service level requirements and remedies for failure to meet standards in the contract.</p> <p>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.</p>
	<p>Relationship Management/Contracts: Contracts establish responsibilities for responding to security incidents.</p> <p><i>Source:</i> IS.II.C.20:pg42: Management should oversee outsourced operations through the following:</p> <ul style="list-style-type: none"> • Contractual assurances for security responsibilities, controls, and reporting. • Coordination of incident response policies and contractual notification requirements. • Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported. <p>IS.WP.6.31(f) & (g): Review the institution's policies, standards, and procedures related to the use of the following:</p> <p>f. Coordination of incident response policies and contractual notification requirements.</p> <p>g. Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported.</p>
	<p>Relationship Management/Contracts: Contracts specify the security requirements for the return or destruction of data upon contract termination.</p> <p><i>Source:</i> 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.</p>
	<p>Relationship Management/Ongoing Monitoring: The third-party risk assessment is updated regularly.</p> <p><i>Source:</i> 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.</p>

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Relationship Management/Ongoing Monitoring: Audits, assessments, and operational performance reports are obtained and reviewed regularly validating security controls for critical third parties.</p> <p><i>Source:</i> IS.II.C.20:pg42: Management should oversee outsourced operations through the following: ...Independent review of the third party's security through appropriate reports from audits and tests.</p> <p>IS.WP.6.31.e: Determine whether management appropriately oversees the effectiveness of information security controls over outsourced operations and is accountable for the mitigation of risks involved with the use of third-party service providers.... Review the institution's policies, standards, and procedures related to the use of the following:...Independent review of the third-party service provider's security through appropriate reports from audits and tests.</p> <p>MGT.III.C.8:pg34 As part of a financial institution's third-party management program, management should ensure that third-party providers effectively provide support by doing the following: Reviewing results of independent audits of IT controls at third-party providers.</p> <p>MGT.WP.12.18: When reviewing information provided by the institution's third party providers, determine the quality of management's follow-up and resolution of customer concerns and problems with its third-party providers.</p>
	<p>Relationship Management/Ongoing Monitoring: Ongoing monitoring practices include reviewing critical third-parties' resilience plans.</p> <p><i>Source:</i> OT.B.19: The program should monitor the service provider environment including its security controls, financial strength, and the impact of any external events.</p> <p>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.</p> <p>MGT.WP.4.7.c: Determine whether management has an effective ongoing monitoring process of its third-party providers.</p>
Domain 5 – Cyber Incident Management and Resilience	
	<p>Incident Resilience Planning and Strategy/Planning: The institution has documented how it will react and respond to cyber incidents.</p> <p><i>Source:</i> 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.</p> <p>BCP.WP.7.5: Determine the existence of an appropriate enterprise-wide BCP.</p> <p>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.</p> <p>MGT.III.C.3:pg29: Institution management should develop, implement, and periodically test incident response procedures, which should address escalation, remediation, and reporting of events and incidents.</p> <p>MGT.III.C.3(b):pg30: To address cybersecurity risk, the information security program should consider the following: Cyber incident management and resilience.</p> <p>MGT.WP.12.8.a: Determine whether a control structure includes: Developing and implementing processes to identify, protect against, detect, respond to, and recover from security events and incidents.</p>

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Incident Resilience Planning and Strategy/Planning: Communication channels exist to provide employees a means for reporting information security events in a timely manner.</p> <p><i>Source:</i> IS.III:pg46: Management should establish defined processes and appropriate governance to facilitate the performance of security operations. Policies should address the timing and extent of the security operations activities, reporting, escalation triggers, and response actions.</p> <p>IS.WP.2.7: Determine whether security officers and employees know, understand, and are accountable for fulfilling their security responsibilities.</p>
	<p>Incident Resilience Planning and Strategy/Planning: Roles and responsibilities for incident response team members are defined.</p> <p><i>Source:</i> IS.III.D:pg51: Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals....</p> <p>IS.WP.8.6.e: Determine whether management has effective incident response processes, including the following:...Policies and procedures to guide the response, assigning responsibilities to individuals;...</p>
	<p>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).</p> <p><i>Source:</i> IS.III.D:pg52: Because of the wide range of technical and nontechnical issues posed by an intrusion, typical SIRT membership includes individuals with a wide range of backgrounds and expertise from different areas within the institution. Those areas include management, legal, and public relations, as well as IT staff.</p> <p>IS.WP.8.6.c: Determine whether management has effective incident response processes, including the following:...Appropriate balance of adequate people and technologies in the response.</p>
	<p>Incident Resilience Planning and Strategy/Planning: A formal backup and recovery plan exists for all critical business lines.</p> <p><i>Source:</i> 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.</p> <p>BCP.WP.3.1: Determine whether the work flow analysis was performed to ensure that all departments and business processes are covered.</p>

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>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.</p> <p><i>Source:</i> IS.II.C.21:pg43: Business continuity plans should be reviewed as an integral part of the security process. Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution if continuity plans must be implemented. Management should train personnel regarding their security roles during a disaster. Additionally, management should update technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of the business continuity plan.</p> <p>IS.WP.6.34: Determine whether management effectively manages the following information security considerations related to business continuity planning.</p> <p>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.</p> <p>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.</p>
	<p>Incident Resilience Planning and Strategy/Testing: Scenarios are used to improve incident detection and response.</p> <p><i>Source:</i> IS.II.C.21:pg43: Management should do the following:... Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios.</p> <p>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.</p> <p>BCP.WP.II.1.1: Determine whether the testing strategy addresses various event scenarios, including potential issues encountered during a wide-scale disruption.</p>
	<p>Incident Resilience Planning and Strategy/Testing: Business continuity testing involves collaboration with critical third parties.</p> <p><i>Source:</i> 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.</p> <p>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.</p>
	<p>Incident Resilience Planning and Strategy/Testing: Systems, applications, and data recovery is tested at least annually.</p> <p><i>Source:</i> 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.</p> <p>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.</p>

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

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

Yes/No	FFIEC Cybersecurity Assessment Tool
	<p>Escalation and Reporting/Escalation and Reporting: Incidents are classified, logged, and tracked.</p> <p><i>Source:</i> 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.</p> <p>OPS.WP.10.1: Describe and assess the event/problem management program’s ability to identify, analyze, and resolve issues and events.</p>

Explanation of FFIEC IT Examination Handbook References

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

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

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

Older references:

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

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

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

Newer references (Information Security and Management Booklets):

If it is from a booklet, then the booklet Chapter, Section and Sub-Section are list, followed by the page number. Chapter, Section and Sub-Section are separated by a period, Page number is separated by colons.

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

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

Appendix B: Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework

In 2014, the National Institute of Standards and Technology (NIST) released a Cybersecurity Framework for all sectors. The following provides a mapping of the FFIEC Cybersecurity Assessment Tool (Assessment) to the statements included in the NIST Cybersecurity Framework. NIST reviewed and provided input on the mapping to ensure consistency with Framework principles and to highlight the complementary nature of the two resources. As the Assessment is based on a number of declarative statements that address similar concepts across maturity levels, the mapping references the first time the concept arises beginning with the lowest maturity level. As such, statements at higher levels of maturity may also map to the NIST Cybersecurity Framework.

References for the NIST Cybersecurity Framework are provided by page number and, if applicable, by the reference code given to the statement by NIST. The Assessment declarative statements are referenced by location in the tool. Following the mapping is the guide to the development of the reference codes for the Assessment Tool.

The mapping is in the order of the NIST Cybersecurity Framework.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
A clear understanding of the organization's business drivers and security considerations specific to use of informational technology and industrial control systems. (p. 4)	Accomplished by completing the Inherent Risk Profile part of the Assessment.
Describe current cybersecurity posture (p. 4)	Accomplished by completing the Cybersecurity Maturity part of the Assessment.
Describe target state for cybersecurity (p. 4)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Identify and prioritize opportunities for improvement with the context of a continuous and repeatable process (p. 4)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Assess progress toward the target state (p. 4)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Communicate among internal and external stakeholders about cybersecurity risk (p. 4)	<p>D1.TC.Tr.B.3: Situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts.</p> <p>D1.TC.Tr.B.4: Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials).</p>

Risk-based approach to managing cybersecurity risk (p. 4)	<p>D1.RM.RA.B.1: 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.</p> <p>D1.RM.RA.B.2: The risk assessment identifies Internet-based systems and high-risk transactions that warrant additional authentication controls.</p> <p>D1.RM.RA.B.3: The risk assessment is updated to address new technologies, products, services, and connections before deployment.</p>
Express a risk tolerance (p. 5)	D1.G.Ov.Int.1: The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.
Determine how to handle risk (mitigate, transfer, avoid, accept) (p. 5)	Accomplished by completing the Cybersecurity Maturity part of the Assessment Tool.
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities (p. 8)	Accomplished by completing the Cybersecurity Maturity Domain 1, Assessment Factor Governance.
Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services (p. 8)	Accomplished by completing the Cybersecurity Maturity Domain 3, Assessment Factor Preventative Controls.
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. (p. 8)	Accomplished by completing the Cybersecurity Maturity Domain 3, Assessment Factor Detective Controls, and Domain 5, Assessment Factor Detection, Response and Mitigation.
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. (p. 8)	Accomplished by completing the Cybersecurity Maturity Domain 5, Assessment Factor Detection, Response and Mitigation and Assessment Factor Escalation and Reporting.
Develop and implement the appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity event. (p. 9)	Accomplished by completing the Cybersecurity Maturity Domain 5, Assessment Factor Incident Resilience Planning and Strategy.

Tier 1: Partial

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Cybersecurity risk management is not formalized and risks are managed in an ad hoc and sometimes reactive manner. (p. 10)	This falls below Baseline.
Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment or business/mission requirements. (p. 10)	This falls below Baseline.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Limited awareness of cybersecurity risk at the organizational level. (p. 10)	This falls below Baseline.
Organization-wide approach to managing cybersecurity risk has not been established. (p. 10)	This falls below Baseline.
Organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. (p. 10)	This falls below Baseline.
Organization may not have processes that enable cybersecurity information to be shared within the organization. (p. 10)	This falls below Baseline.
Organization may not have the processes in place to participate in coordination or collaboration with other entities. (p. 10)	This falls below Baseline

Tier 2: Risk Informed

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Risk management practices are approved by management but may not be established as organizational-wide policy. (p. 10)	D1.RM.RMP.B.1: An information security and business continuity risk management function(s) exists within the institution.
Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements. (p. 10)	<p>D2.TI.Th.B.3: Threat information is used to enhance internal risk management and controls.</p> <p>D1.G.Ov.Int.5: 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.</p> <p>D1.G.SP.Int.2: Management periodically reviews the cybersecurity strategy to address evolving cyber threats and changes to the institution's inherent risk profile.</p>
There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. (p. 10)	<p>D1.G.Ov.B.2: Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.</p> <p>D1.TC.Tr.B.1: Annual information security training is provided.</p> <p>D1.TC.Tr.E.2: Management is provided cybersecurity training relevant to their job responsibilities.</p>
Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. (p. 10)	<p>D1.RM.RMP.E.1: The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring and reporting.</p> <p>D1.R.St.E.3: Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position.</p>

<p>Cybersecurity information is shared within the organization on an informal basis. (p. 10)</p>	<p>D1.TC.Tr.B.3: Situational awareness materials are made available to employees when prompted by highly visible cyber events or regulatory alerts.</p>
<p>The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally. (p. 10)</p>	<p>D1.G.SP.A.3: The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructure in the financial services industry.</p> <p>D1.G.SP.Inn.1: The cybersecurity strategy identifies and communicates the institution's role as it relates to other critical infrastructures.</p> <p>D2.TI.Th.B.1: 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).</p>

Tier 3: Repeatable

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>The organization's risk management practices are formally approved and expressed as policy. (p. 10)</p>	<p>D1.G.SP.B.2: The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management.</p>
<p>Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape. (p. 10)</p>	<p>D1.G.SP.E.3: A formal process is in place to update policies as the institution's inherent risk profile changes.</p>
<p>There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. (p. 10)</p>	<p>D1.G.SP.Int.4: Management links strategic cybersecurity objectives to tactical goals.</p> <p>D1.G.RM.Au.B.1: 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.</p>
<p>Consistent methods are in place to respond effectively to changes in risk. (p. 10)</p>	<p>D1.G.SP.E.3: A formal process is in place to update policies as the institution's inherent risk profile changes.</p>
<p>Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. (p. 10)</p>	<p>D1.R.St.E.2: Management with appropriate knowledge and experience leads the institution's cybersecurity efforts.</p> <p>D1.R.St.E.3: Staff with cybersecurity responsibilities has the requisite qualifications to perform the necessary tasks of the position.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events. (p. 10)</p>	<p>D4.C.Co.B.1: The critical business processes that are dependent on external connectivity have been identified.</p> <p>D2.TI.Th.B.1: 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).</p> <p>D2.TI.Th.Int.1: A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources.</p> <p>D4.RM.Co.E.2: Responsibility for notification of direct and indirect security incidents and vulnerabilities is documented in contracts or SLAs.</p>

Tier 4: Adaptive

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>Adapt cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. (p. 11)</p>	<p>D5.DR.Re.E.8: Analysis of events is used to improve the institution's security measures and policies.</p> <p>D5.IR.PI.Int.4: 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.</p> <p>D1.TC.Tr.Int.1: Management incorporates lessons learned from social engineering and phishing exercises to improve the employee awareness programs.</p>
<p>Continually incorporates advanced technologies and practices, adapting to a changing cybersecurity landscape. (p. 11)</p>	<p>D1.G.SP.A.5: Management is continuously improving the existing cybersecurity program to adapt as the desired cybersecurity target state changes.</p>
<p>Responds to evolving and sophisticated threats in a timely manner. (p. 11)</p>	<p>D5.IR.PI.B.1: The institution has documented how it will react and respond to cyber incidents.</p> <p>D5.IR.PI.A.2: 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.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>Manages cybersecurity risk through an organization-wide approach using risk-informed policies, processes, and procedures to address potential cybersecurity events. (p. 11)</p>	<p>D5.IR.PI.B.1: The institution has documented how it will react and respond to cyber incidents</p> <p>D1.TC.Cu.E.1: The institution has formal standards of conduct that hold all employees accountable for complying with all cybersecurity policies and procedures.</p> <p>D1.RM.RMP.Int.2: The risk management program specifically addresses cyber risks beyond the boundaries of the technological impacts (e.g., financial, strategic, regulatory, compliance).</p> <p>D1.G.Ov.A.5: Management and the board or an appropriate board committee hold business units accountable for effectively managing all cyber risks associated with their activities.</p>
<p>Encourage cybersecurity risk management as part of culture. (p. 11)</p>	<p>D1.TC.Cu.Int.2: The risk culture requires formal consideration of cyber risks in all business decisions.</p> <p>D1.TC.Cu.A.1: Management ensures continuous improvement of cyber risk cultural awareness.</p>
<p>Evolve process from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on systems and networks. (p. 11)</p>	<p>D1.G.Ov.A.2: Management has a formal process to continuously improve cybersecurity oversight.</p>
<p>Actively share information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs. (p. 11)</p>	<p>D2.IS.Is.Int.3: Information is shared proactively with the industry, law enforcement, regulators, and information-sharing forums.</p>

Framework Profile

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>Establish a roadmap for reducing cybersecurity risk. (p. 11)</p>	<p>Accomplished if an institution implements the Assessment as described in the User's Guide.</p>
<p>Develop a current profile. (p. 11)</p>	<p>Accomplished if an institution implements the Assessment as described in the User's Guide.</p>
<p>Develop a target profile. (p. 11)</p>	<p>Accomplished if an institution implements the Assessment as described in the User's Guide.</p>
<p>Identify and remediate gaps in current and target profiles. (p. 11)</p>	<p>Accomplished if an institution implements the Assessment as described in the User's Guide.</p>
<p>Develop a risk-management approach to achieve cybersecurity goals in a cost-effective, prioritized manner (p. 11)</p>	<p>Discussed in the User's Guide.</p>
<p>Executive leadership communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. (p. 12)</p>	<p>Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Business/Process managers collaborate with the implementation/operations level to communicate business needs and create a risk profile using the input from the executive leadership. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Business/process managers perform an impact assessment from the implementation progress provided by the implementation/operations group. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Business/process managers perform an impact assessment from the implementation progress provided by the implementation/operations group. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Business/process managers report the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Business/process managers notify the implementation/operations level to raise awareness of business impact. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Operations group communicates the risk Profile implementation progress to the business/process level. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Create or improve a cybersecurity program. (p. 13)	Discussed in the User's guide.
Organization identifies its business/mission objectives and high-level organizational priorities. (p. 14)	Discussed in the User's guide.
Organization identifies related systems and assets, regulatory requirements, and overall risk approach. (p. 14)	Accomplished by completing the Inherent Risk Profile part of the Tool.
Organization identifies threats to, and vulnerabilities of, identified systems and assets (p. 14)	Accomplished if an institution completes the Inherent Risk Profile part of the Assessment.
Develop a current profile. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Conduct a risk assessment. (p. 14)	Accomplished if an institution completes the Inherent Risk Profile part of the Assessment.
Create a target profile. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Compare the current and target profile to determine gaps. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Create a prioritized action plan to address gaps. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Implement action plan. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Repeat as needed to continuously assess and improve cybersecurity. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Communicate cybersecurity requirements with interdependent stakeholders responsible for the delivery of essential critical infrastructure services. (p. 15)	<p>D4.RM.Co.B.1: 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.</p> <p>D4.RM.Co.E.2: Responsibility for notification of direct and indirect security incidents and vulnerabilities is documented in contracts or SLAs.</p>
<p>Identify and address individual privacy and civil liberties implications that may result from cybersecurity operations (p. 15)</p> <p>Governance of cybersecurity risk.</p> <p>Identifying and authorizing access.</p> <p>Awareness and training measures.</p> <p>Anomalous activity detection reviewed for privacy concerns.</p> <p>Review of the sharing of personal information within and outside of the organization.</p>	<p>D4.RM.Co.B.1: 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.</p> <p>D1.G.Ov.E.2: Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.</p> <p>D2.IS.Int.2: Information-sharing agreements are used as needed or required to facilitate sharing threat information with other financial sector institutions or third parties.</p>

Appendix A: Framework Core

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
ID.AM-1: Physical devices and systems within the organization are inventoried. (p. 20)	D1.G.IT.B.1: An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
ID.AM-2: Software platforms and applications within the organization are inventoried. (p. 20)	D1.G.IT.B.1: An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
ID.AM-3: The organizational communication and data flow is mapped. (p. 20)	D4.C.Co.B.4: Data flow diagrams are in place and document information flow to external parties. D4.C.Co.Int.1: A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.
ID.AM-4: External information systems are mapped and catalogued. (p. 20)	D4.RM.Dd.B.2: A list of third-party service providers is maintained. D4.C.Co.B.3: A network diagram is in place and identifies all external connections.
ID.AM-5: Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software. (p. 20)	D1.G.IT.B.2: Institution assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.
ID.AM-6: Workforce roles and responsibilities for business functions, including cybersecurity, are established. (p. 20)	D1.R.St.B.1: Information security roles and responsibilities have been identified. D1.TC.Cu.B.1: Management holds employees accountable for complying with the information security program.
ID.BE-1: The organization's role in the supply chain is identified and communicated. (p. 21)	D1.G.SP.A.3: The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructure in the financial services industry.
ID.BE-2: The organization's place in critical infrastructure and their industry ecosystem is identified and communicated. (p. 21)	D1.G.SP.Inn.1: The cybersecurity strategy identifies and communicates its role as it relates to other critical infrastructures.
ID.BE-3: Priorities for organizational mission, objectives, and activities are established. (p. 21)	D1.G.SP.E.2: The institution has a formal cybersecurity program that is based on technology and security industry standards or benchmarks. D1.G.Ov.Int.5: 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. D1.G.SP.Int.3: The cybersecurity strategy is incorporated into, or conceptually fits within, the institution's enterprise-wide risk management strategy.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>ID.BE-4: Dependencies and critical functions for delivery of critical services are established. (p. 21)</p>	<p>D4.C.Co.B.1: The critical business processes that are dependent on external connectivity have been identified.</p> <p>D1.G.IT.B.2: Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.</p>
<p>ID.BE-5: Resilience requirements to support delivery of critical services are established. (p. 21)</p>	<p>D5.IR.PI.B.5: A formal backup and recovery plan exists for all critical business lines.</p> <p>D5.IR.PI.E.3: Alternative processes have been established to continue critical activity within a reasonable time period.</p>
<p>ID.GV-1: Organizational information security policy is established. (p. 21)</p>	<p>D1.G.SP.B.4: The institution has board-approved policies commensurate with its risk and complexity that address information security.</p>
<p>ID.GV-2: Information security roles & responsibility are coordinated and aligned with internal roles and external partners. (p. 21)</p>	<p>D1.G.SP.B.7: All elements of the information security program are coordinated enterprise-wide.</p> <p>D4.RM.Co.B.2: Contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits.</p> <p>D4.RM.Co.B.5: Contracts establish responsibilities for responding to security incidents.</p>
<p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. (p. 21)</p>	<p>D1.G.Ov.E.2: Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.</p>
<p>ID.GV-4: Governance and risk management processes address cybersecurity risks. (p. 22)</p>	<p>D1.G.Ov.B.1: 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.</p> <p>D1.G.Ov.B.3: Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate committee of the board at least annually.</p> <p>D1.G.Ov.E.1: At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program.</p> <p>D1.G.SP.E.1: The institution augmented its information security strategy to incorporate cybersecurity and resilience.</p> <p>D1.G.Ov.Int.1: The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>ID.RA-1: Asset vulnerabilities are identified and documented. (p. 22)</p>	<p>D2.TI.Ti.B.2: Threat information is used to monitor threats and vulnerabilities.</p> <p>D3.DC.Th.B.1: Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for the external-facing systems and the internal network.</p> <p>D1.RM.RA.E.2: The focus of the risk assessment has expanded beyond customer information to address all information assets.</p> <p>D3.DC.Th.E.5: Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices.</p> <p>D3.DC.Th.A.1: Weekly vulnerability scanning is rotated amongst environments to scan all environments throughout the year.</p>
<p>ID.RA-2: Threat and vulnerability information is received from information-sharing forums and sources. (p. 22)</p>	<p>D2.TI.Ti.B.1: 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).</p>
<p>ID.RA-3: Threats to organizational assets are identified and documented. (p. 22)</p>	<p>D3.DC.An.B.1: The institution is able to detect anomalous activities through monitoring across the environment.</p> <p>D2.MA.Ma.E.1: A process is implemented to monitor threat information to discover emerging threats.</p> <p>D2.MA.Ma.E.4: Monitoring systems operate continuously with adequate support for efficient incident handling.</p> <p>D2.MA.Ma.Int.2: A profile is created for each threat that identifies the likely intent, capability, and target of the threat.</p>
<p>ID.RA-4: Potential impacts are analyzed. (p. 22)</p>	<p>D5.RE.Re.B.1: Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information.</p> <p>D5.ER.Er.Ev.1: 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.</p>
<p>ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. (p. 22)</p>	<p>D1.RM.RA.B.1: 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.</p> <p>D1.RM.RA.E.2: The focus of the risk assessment has expanded beyond customer information to address all information assets.</p> <p>D1.RM.RA.E.1: Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>ID.RA-6: Risk responses are identified and prioritized. (p. 22)</p>	<p>D5.IR.PI.B.1: The institution has documented how it will react and respond to cyber incidents.</p> <p>D5.DR.Re.E.1: The incident response plan is designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities.</p> <p>D5.IR.PI.E.1: The remediation plan and process outlines the mitigating actions, resources, and time parameters.</p>
<p>ID.RM-1: Risk management processes are managed and agreed to by organizational stakeholders. (p. 23)</p>	<p>D1.G.Ov.B.1: 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.</p>
<p>ID.RM-2: Organizational risk tolerance is determined and clearly expressed. (p. 23)</p>	<p>D1.G.Ov.Int.3: The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.</p>
<p>ID.RM-3: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis. (p. 23)</p>	<p>D1.G.SP.A.4: The risk appetite is informed by the institution's role in critical infrastructure.</p>
<p>PR.AC-1: Identities and credentials are managed for authorized devices and users. (p. 23)</p>	<p>D3.PC.Im.B.7: Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.</p> <p>D3.PC.Am.B.6: Identification and authentication are required and managed for access to systems, applications, and hardware.</p>
<p>PR.AC-2: Physical access to assets is managed and protected. (p. 23)</p>	<p>D3.PC.Am.B.11: Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems.</p> <p>D3.PC.Am.B.17: Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software.</p>
<p>PR.AC-3: Remote access is managed. (p. 23)</p>	<p>D3.PC.Am.B.15: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.</p> <p>D3.PC.De.E.7: The institution wipes data remotely on mobile devices when a device is missing or stolen. (*N/A if mobile devices are not used.)</p> <p>D3.PC.Im.Int.2: Security controls are used for remote access to all administrative consoles, including restricted virtual systems.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. (p. 24)</p>	<p>D3.PC.Am.B.1: Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.</p> <p>D3.PC.Am.B.2: Employee access to systems and confidential data provides for separation of duties.</p> <p>D3.PC.Am.B.5: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.</p>
<p>PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate. (p. 24)</p>	<p>D3.DC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used.</p> <p>D3.DC.Im.Int.1: 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.</p>
<p>PR.AT-1: All users are informed and trained. (p. 24)</p>	<p>D1.TC.Tr.B.2: Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues.</p>
<p>PR.AT-2: Privileged users understand roles & responsibilities. (p. 24)</p>	<p>D1.TC.Tr.E.3: Employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility.</p>
<p>PR.AT-3: Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities. (p. 24)</p>	<p>D1.TC.Tr.B.4: Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials).</p> <p>D1.TC.Tr.Int.2: Cybersecurity awareness information is provided to retail customers and commercial clients at least annually.</p>
<p>PR.AT-4: Senior executives understand roles and responsibilities. (p. 24)</p>	<p>D1.TC.Tr.E.2: Management is provided cybersecurity training relevant to their job responsibilities.</p>
<p>PR.AT-5: Physical and information security personnel understand roles & responsibilities. (p. 25)</p>	<p>D1.TC.Tr.E.3: Employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility.</p> <p>D1.R.St.E.3: Staff with cybersecurity responsibilities has the requisite qualifications to perform the necessary tasks of the position.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>PR.DS-1: Data-at-rest is protected. (p. 25)</p>	<p>D1.G.IT.B.13: Confidential data is identified on the institution's network.</p> <p>D3.PC.Am.B.14: 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).</p> <p>D4.RM.Co.B.1: 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.</p> <p>D3.PC.Am.A.1: Encryption of select data at rest is determined by the institution's data classification and risk assessment.</p>
<p>PR.DS-2: Data-in-transit is protected. (p. 25)</p>	<p>D3.PC.Am.B.13: Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).</p> <p>D3.PC.Am.E.5: Controls are in place to prevent unauthorized access to cryptographic keys.</p> <p>D3.PC.Am.Int.7: Confidential data is encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.</p>
<p>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. (p. 25)</p>	<p>D1.G.IT.E.3: The institution proactively manages system end-of-life (e.g., replacement) to limit security risks.</p> <p>D1.G.IT.E.2: The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards.</p>
<p>PR.DS-4: Adequate capacity to ensure availability is maintained. (p. 25)</p>	<p>D5.IR.PI.B.5: A formal backup and recovery plan exists for all critical business lines.</p> <p>D5.IR.PI.B.6: The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.</p> <p>D5.IR.PI.E.3: Alternative processes have been established to continue critical activity within a reasonable time period.</p> <p>D3.PC.Im.E.4: A risk-based solution is in place at the institution or Internet-hosting provider to mitigate disruptive cyber attacks (e.g., DDoS attacks).</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>PR.DS-5: Protections against data leaks are implemented. (p. 26)</p>	<p>D3.PC.Am.B.15: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.</p> <p>D3.PC.Am.Int.1: The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.</p> <p>D3.PC.De.Int.1: Data loss prevention controls or devices are implemented for inbound and outbound communications (e.g., e-mail, FTP, Telnet, prevention of large file transfers).</p> <p>D3.DC.Ev.Int.1: Controls or tools (e.g., data loss prevention) are in place to detect potential unauthorized or unintentional transmissions of confidential data.</p>
<p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity. (p. 26)</p>	<p>D3.PC.Se.Int.3: Software code executables and scripts are digitally signed to confirm the software author and guarantee that the code has not been altered or corrupted.</p> <p>D3.PC.De.Int.2: Mobile device management includes integrity scanning (e.g., jailbreak/rooted detection). (*N/A if mobile devices are not used.)</p>
<p>PR.DS-7: The development and testing environment(s) are separate from the production environment. (p. 26)</p>	<p>D3.PC.Am.B.10: 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.)</p>
<p>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained. (p. 26)</p>	<p>D3.PC.Im.B.5: Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced.</p>
<p>PR.IP-2: A System Development Life Cycle to manage systems is implemented. (p. 26)</p>	<p>D3.PC.Se.B.1: Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards.</p> <p>D3.PC.Se.E.1: 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.)</p>
<p>PR.IP-3: Configuration change control processes are in place. (p. 27)</p>	<p>D1.G.IT.B.4: A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools.</p>
<p>PR.IP-4: Backups of information are conducted, maintained, and tested periodically. (p. 27)</p>	<p>D5.IR.PI.B.5: A formal backup and recovery plan exists for all critical business lines.</p> <p>D5.IR.Te.E.3: Information backups are tested periodically to verify they are accessible and readable.</p>
<p>PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met. (p. 27)</p>	<p>D3.PC.Am.B.11: Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
PR.IP-6: Data is destroyed according to policy. (p. 27)	D1.G.IT.B.19: Data is disposed of or destroyed according to documented requirements and within expected time frames.
PR.IP-7: Protection processes are continuously improved. (p. 27)	D1.RM.RMP.E.2: Management reviews and uses the results of audits to improve existing policies, procedures, and controls. D1.G.Ov.A.2: Management has a formal process to continuously improve cybersecurity oversight.
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties. (p. 28)	D2.IS.Is.B.1: Information security threats are gathered and shared with applicable internal employees. D2.IS.Is.E.2: A representative from the institution participates in law enforcement or information-sharing organization meetings.
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. (p. 28)	D5.IR.PI.B.1: The institution has documented how it will react and respond to cyber incidents.
PR.IP-10: Response and recovery plans are tested. (p. 28)	D5.IR.Te.B.1: Scenarios are used to improve incident detection and response. D5.IR.Te.B.3: Systems, applications, and data recovery is tested at least annually.
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). (p. 28)	D1.R.St.E.4: Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk.
PR.IP-12: A vulnerability management plan is developed and implemented. (p. 28)	D3.CC.Re.Ev.2: Formal processes are in place to resolve weaknesses identified during penetration testing.
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools (p. 28)	D3.CC.Re.Int.5: The maintenance and repair of organizational assets are performed by authorized individuals with approved and controlled tools. D3.CC.Re.Int.6: The maintenance and repair of organizational assets are logged in a timely manner.
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access (p. 28)	D3.PC.Im.B.7: Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. (p. 29)	D1.G.SP.B.3: The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing. D2.MA.Ma.B.1: Audit log records and other security event logs are reviewed and retained in a secure manner. D2.MA.Ma.B.2: Computer event logs are used for investigations once an event has occurred.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>PR.PT-2: Removable media is protected and its use restricted according to a specified policy. (p. 29)</p>	<p>D1.G.SP.B.4: The institution has board-approved policies commensurate with its risk and complexity that address information security.</p> <p>D3.PC.De.B.1: Controls are in place to restrict the use of removable media to authorized personnel.</p> <p>D3.PC.Im.E.3: Technical controls prevent unauthorized devices, including rogue wireless access devices and removable media from connecting to the internal network(s).</p>
<p>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. (p. 29)</p>	<p>D3.PC.Am.B.7: Access controls include password complexity and limits to password attempts and reuse.</p> <p>D3.PC.Am.B.4: User access reviews are performed periodically for all systems and applications based on the risk to the application or system.</p> <p>D3.PC.Am.B.3: Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls).</p> <p>D4.RM.Om.Int.1: Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.</p>
<p>PR.PT-4: Communications networks are secured. (p. 29)</p>	<p>D3.PC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used.</p> <p>D3.PC.Am.B.11: Physical security controls are used to prevent unauthorized access to information systems, and telecommunication systems.</p> <p>D3.PC.Im.Int.1: 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.</p>
<p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed. (p. 30)</p>	<p>D3.DC.Ev.B.1: A normal network activity baseline is established.</p> <p>D4.C.Co.B.4: Data flow diagrams are in place and document information flow to external parties.</p>
<p>DE.AE-2: Detected events are analyzed to understand attack targets and methods. (p. 30)</p>	<p>D5.IR.PI.Int.4: Lessons learned from real-life cyber risk incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan.</p>
<p>DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors. (p. 30)</p>	<p>D3.DC.Ev.E.1: A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>DE.AE-4: Impact of event is determined. (p. 30)</p>	<p>D5.IR.Te.E.1: Recovery scenarios include plans to recover from data destruction, and impacts to data integrity, data loss, and system and data availability.</p> <p>D5.ER.Es.E.1: 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.</p> <p>D1.RM.RMP.A.4: A process is in place to analyze the financial impact cyber incidents have on the institution's capital.</p>
<p>DE.AE-5: Incident alert thresholds are established. (p. 30)</p>	<p>D5.DR.De.B.1: Alert parameters are set for detecting information security incidents that prompt mitigating actions.</p> <p>D3.DC.An.E.4: Thresholds have been established to determine activity within logs that would warrant management response.</p> <p>D3.DC.An.Int.3: Tools actively monitor security logs for anomalous behavior and alert within established parameters.</p>
<p>DE.CM-1: The network is monitored to detect potential cybersecurity events. (p. 30)</p>	<p>D3.DC.An.B.2: Customer transactions generating anomalous activity alerts are monitored and reviewed.</p> <p>D3.DC.An.B.3: Logs of physical and/or logical access are reviewed following events.</p>
<p>DE.CM-2: The physical environment is monitored to detect potential cybersecurity events. (p. 30)</p>	<p>D3.PC.Am.E.4: Physical access to high-risk or confidential systems is restricted, logged, and unauthorized access is blocked.</p> <p>D3.Dc.Ev.B.5: The physical environment is monitored to detect potential unauthorized access.</p>
<p>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events. (p. 31)</p>	<p>D3.DC.An.A.3: A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.</p>
<p>DE.CM-4: Malicious code is detected. (p. 31)</p>	<p>D3.DC.Th.B.2: Antivirus and anti-malware tools are used to detect attacks.</p>
<p>DE.CM-5: Unauthorized mobile code is detected. (p. 31)</p>	<p>D3.PC.De.E.5: Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices).</p>
<p>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events. (p. 31)</p>	<p>D4.RM.Om.Int.1: Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.</p>
<p>DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed. (p. 31)</p>	<p>D3.DC.Ev.B.3: Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
DE.CM-8: Vulnerability scans are performed. (p. 31)	D3.DC.Th.E.5: Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices.
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. (p. 31)	D3.DC.Ev.B.4: Responsibilities for monitoring and reporting suspicious systems activity have been assigned.
DE.DP-2: Detection activities comply with all applicable requirements. (p. 32)	D1.G.Ov.E.2: Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.
DE.DP-3: Detection processes are tested. (p. 32)	D3.DC.Ev.Int.2: Event detection processes are proven reliable.
DE.DP-4: Event detection information is communicated to appropriate parties. (p. 32)	<p>D3.DC.Ev.B.2: Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks.</p> <p>D5.ER.Is.B.1: A process exists to contact personnel who are responsible for analyzing and responding to an incident.</p> <p>D5.ER.Is.E.1: 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.</p>
DE.DP-5: Detection processes are continuously improved. (p. 32)	D5.IR.PI.Int.3: 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.
RS.PL-1: Response plan is executed during or after an event. (p. 33)	D5.IR.PI.B.1: The institution has documented how it will react and respond to cyber incidents.
RS.CO-1: Personnel know their roles and order of operations when a response is needed. (p. 33)	D5.IR.PI.B.3: Roles and responsibilities for incident response team members are defined.
RS.CO-2: Events are reported consistent with established criteria. (p. 33)	<p>D5.IR.PI.B.2: Communication channels exist to provide employees a means for reporting information security events in a timely manner.</p> <p>D5.DR.Re.B.4: Incidents are classified, logged and tracked.</p> <p>D5.DR.Re.E.6: Records are generated to support incident investigation and mitigation.</p> <p>D5.ER.Es.B.4: Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.</p>
RS.CO-3: Information is shared consistent with established criteria. (p. 33)	D5.ER.Es.B.2: 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.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>RS.CO-4: Coordination with stakeholders occurs consistent with response plans. (p. 33)</p>	<p>D5.ER.Is.B.1: A process exists to contact personnel who are responsible for analyzing and responding to an incident.</p> <p>D5.IR.PI.Int.1: A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.</p>
<p>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. (p. 33)</p>	<p>D2.IS.Is.B.3: Information about threats is shared with law enforcement and regulators when required or prompted.</p> <p>D2.IS.Is.E.2: A representative from the institution participates in law enforcement or information-sharing organization meetings.</p>
<p>RS.AN-1: Notifications from the detection system are investigated. (p. 33)</p>	<p>D5.DR.De.B.3: Tools and processes are in place to detect, alert, and trigger the incident response program.</p> <p>D5.DR.De.Int.3: Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.</p>
<p>RS.AN-2: The impact of the incident is understood. (p. 34)</p>	<p>D1.RM.RMP.A.4: A process is in place to analyze the financial impact cyber incidents have on the institution's capital.</p> <p>D5.IR.Te.E.1: Recovery scenarios include plans to recover from data destruction, impacts to data integrity, data loss, and system and data availability.</p> <p>D5.ER.Es.E.1: 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.</p>
<p>RS.AN-3: Forensics are performed. (p. 34)</p>	<p>D3.CC.Re.Int.3: Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties.</p> <p>D3.CC.Re.Int.4: Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action.</p>
<p>RS.AN-4: Incidents are categorized consistent with response plans. (p. 34)</p>	<p>D5.ER.Es.B.4: Incidents are classified, logged and tracked.</p> <p>D5.DR.Re.E.1: The incident response plan is designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
RS.MI-1: Incidents are contained. (p. 34)	<p>D5.DR.Re.B.1: Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information.</p> <p>D5.DR.Re.E.4: Procedures include containment strategies and notifying potentially impacted third parties.</p> <p>D5.DR.Re.E.2: A process is in place to help contain incidents and restore operations with minimal service disruption.</p> <p>D5.DR.Re.E.3: Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware).</p>
RS.MI-2: Incidents are mitigated. (p. 34)	<p>D5.DR.De.B.1: Alert parameters are set for detecting information security incidents that prompt mitigating actions.</p> <p>D5.DR.Re.E.3: Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware).</p> <p>D3.PC.Im.E.4: A risk-based solution is in place at the institution or Internet-hosting provider to mitigate disruptive cyber attacks (e.g., DDoS attacks).</p>
RS.MI-3: Newly identified vulnerabilities are documented as accepted risks. (p. 34)	<p>D1.RM.RA.E.1: Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships.</p>
RS.IM-1: Response plans incorporate lessons learned. (p. 34)	<p>D5.IR.PI.Int.4: 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.</p>
RS.IM-2: Response strategies are updated. (p. 34)	<p>D5.IR.PI.Int.4: 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.</p> <p>D5.IR.Te.Int.5: The results of cyber event exercises are used to improve the incident response plan and automated triggers.</p>
RC.RP-1: Recovery plan is executed during or after an event. (p. 34)	<p>D5.IR.PI.B.6: The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.</p>
RC.IM-1: Recovery plans incorporate lessons learned. (p. 35)	<p>D5.IR.PI.Int.4: 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.</p>

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
<p>RC.IM-2: Recovery strategies are updated. (p. 35)</p>	<p>D5.IR.PI.Int.4: 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.</p> <p>D5.IR.Te.Int.5: The results of cyber event exercises are used to improve the incident response plan and automated triggers.</p>
<p>RC.CO-1: Public Relations are managed. (p. 35)</p>	<p>D5.ER.Es.Int.3: An external communication plan is used for notifying media regarding incidents when applicable.</p>
<p>RC.CO-2: Reputation after an event is repaired. (p. 35)</p>	<p>D5.IR.PI.Int.1: A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.</p>
<p>RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. (p. 35)</p>	<p>D5.ER.Is.B.1: A process exists to contact personnel who are responsible for analyzing and responding to an incident.</p> <p>D5.IR.PI.Int.1: A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.</p>

Explanation of Cybersecurity Assessment Tool References

To reference the Cybersecurity Assessment Tool declarative statements, each has a unique identifier that comprises the Domain, Assessment Factor, Component, Maturity Level, and statement number. Each portion is separated by a period.

The following table provides the codes used in the above references for the Cybersecurity Assessment Tool. For example, “D1.G.Ov.B.1” refers to Domain: 1, Assessment Factor: Governance, Component: Oversight, Maturity Level: Baseline, and statement 1.

Domain	Assessment Factor	Component	Maturity Level
Domain 1: Cyber Risk Management and Oversight (D1)	Governance (G)	Oversight (Ov)	Baseline (B)
		Strategy/Policies (SP)	Evolving (E)
		IT Asset Management (IT)	Intermediate (Int)
	Risk Management (RM)	Risk Management Program (RMP)	Advanced (A)
		Risk Assessment (RA)	Innovative (Inn)
		Audit (Au)	
	Resources (R)	Staffing (St)	
	Training and Culture (TC)	Training (Tr)	
		Culture (Cu)	
Domain 2: Threat Intelligence and Collaboration (D2)	Threat Intelligence (TI)	Threat Intelligence and Information (Ti)	
	Monitoring and Analyzing (MA)	Monitoring and Analyzing (Ma)	
	Information Sharing (IS)	Informational Sharing (Is)	
Domain 3: Cybersecurity Controls (D3)	Preventative Controls (PC)	Infrastructure Management (Im)	
		Access and Data Management (Am)	
		Device/End-Point Security (De)	
		Secure Coding (Se)	
	Detective Controls (DC)	Threat and Vulnerability Detection (Th)	
		Anomalous Activity (An)	
		Event Detection (Ev)	
	Corrective Controls (CC)	Patch Management (Pa)	

Domain	Assessment Factor	Component	Maturity Level
		Remediation (Re)	
Domain 4: External Dependency Management (D4)	Connections (C)	Connections (Co)	
	Relationship Management (RM)	Due Diligence (Dd)	
		Contracts (Co)	
		Ongoing Monitoring (Om)	
Domain 5: Cyber Incident Management and Resilience (D5)	Incident Resilience Planning and Strategy (IR)	Planning (PI)	
		Testing (Te)	
	Detection, Response and Mitigation (DR)	Detection (De)	
		Response and Mitigation (Re)	
	Escalation and Reporting (ER)	Escalation and Reporting (Es)	

Appendix C: Glossary

Administrator privileges: Allow computer system-access to resources that are unavailable to most users. Administrator privileges permit execution of actions that would otherwise be restricted. *Source:* [NSA/CSS Confidence in Cyber Space](#)

Air-gapped environment: Security measure that isolates a secure network from unsecure networks physically, electrically, and electromagnetically. *Source:* [FFIEC Joint Statement - Destructive Malware](#)

Anomalous activity: The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. *Source:* [NIST: SP 800-94](#)

Antivirus/Anti-malware software: A program that monitors a computer or network to identify all types of malware and prevent or contain malware incidents. *Source:* [NIST Guide to Malware Incident Prevention and Handling for Desktops and Laptops](#)

Asset: In computer security, a major application, general-support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems. *Source:* [NIST: CNSSI-4009](#)

Attack signature: A specific sequence of events indicative of an unauthorized access attempt. *Source:* [NIST: SP 800-12](#)

Authentication: The process of verifying the identity of an individual user, machine, software component, or any other entity. *Source:* [FFIEC Information Security Booklet](#)

Baseline configuration: A set of specifications for a system, or configuration item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and that can be changed only through change-control procedures. The baseline configuration is used as a basis for future builds, releases, or changes. *Source:* [NIST: SP 800-128](#)

Black holing: A method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. *Source:* [NCCIC/US-CERT DDoS Quick Guide](#)

Border router: A device located at the organization's boundary to an external network. *Source:* [NIST: SP 800-41](#)

Buffer overflow: A condition at an interface under which more input can be placed into a buffer or data-holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of a system. *Source:* [NISTIR 7298 Revision 2](#)

Business continuity: The ability to maintain operations and services—both technology and business—in the event of a disruption to normal operations and services. Ensures that any impact or disruption of services is within a documented and acceptable recovery time period and that system or operations are resumed at a documented and acceptable point in the processing cycle. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Change management: The broad processes for managing organizational change. Change management encompasses planning, oversight or governance, project management, testing, and implementation. *Source:* [FFIEC Operations Booklet](#)

CHIPS: A private-sector U.S.-dollar funds-transfer system, clearing and settling cross-border and domestic payments. *Source:* [CHIPS](#)

Cloud computing: Generally a migration from owned resources to shared resources in which client users receive information technology services on demand from third-party service providers via the Internet “cloud.” In cloud environments, a client or customer relocates its resources—such as data, applications, and services—to computing facilities outside the corporate firewall, which the end user then accesses via the Internet. *Source:* [FFIEC Statement on Outsourced Cloud Computing](#)

Crisis management: The process of managing an institution’s operations in response to an emergency or event that threatens business continuity. An institution’s ability to communicate with employees, customers, and the media, using various communications devices and methods, is a key component of crisis management. *Source:* [FFIEC Business Continuity Planning Booklet](#)

Critical system [infrastructure]: The systems and assets, whether physical or virtual, that are so vital that the incapacity or destruction of such may have a debilitating impact. *Source:* [NICCS Glossary](#)

Cyber attack: Attempts to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Cyber event: A cybersecurity change or occurrence that may have an impact on organizational operations (including mission, capabilities, or reputation). *Source:* [NIST Cybersecurity Framework](#)

Cyber incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein. *Source:* [NIST: CNSSI-4009](#)

Cyber threat: An internal or external circumstance, event, action, occurrence, or person with the potential to exploit technology-based vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. *Source:* [NICCS Glossary](#)

Cybersecurity: The process of protecting consumer and bank information by preventing, detecting, and responding to attacks. *Source:* *Derived from* [NIST Cybersecurity Framework](#)

Data classification program: A program that categorizes data to convey required safeguards for information confidentiality, integrity, and availability; establishes controls required based on value and level of sensitivity. *Source:* [Derived from SANS Institute InfoSec Reading Room](#)

Database: A collection of data that is stored on any type of computer storage medium and may be used for more than one purpose. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Data loss prevention (DLP): A comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data wherever it is stored, used, or in transit over the network and at the perimeter. *Source:* [NSA/CSS Securing Data and Handling Spillage Events](#)

Data mining: The process or techniques used to analyze large sets of existing information to discover previously unrevealed patterns or correlations. *Source:* [NICCS Glossary](#)

Deep packet inspection: The capability to analyze network traffic to compare vendor-developed profiles of benign protocol activity against observed events to identify deviations. *Source:* [NIST Guide to Intrusion Detection and Prevention Systems](#)

Defense-in-depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. *Source:* [NIST: CNSSI-4009](#)

Digital certificate: The electronic equivalent of an ID card that authenticates the originator of a digital signature. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Disaster recovery plan: A plan that describes the process to recover from major processing interruptions. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Distributed denial of service (DDoS): A type of attack that makes a computer resource or resources unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary, it generally consists of the concerted efforts of a group that intends to affect an institution's reputation by preventing an Internet site, service, or application from functioning efficiently. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Domain Name System Security Extensions (DNSSEC): A technology that was developed to, among other things, protect against such attacks by digitally 'signing' data so you can be assured it is valid. *Source:* [ICANN](#)

Encryption: A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appear as meaningless strings of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key. *Source:* [FFIEC IT Examination Handbook Glossary](#)

End-of-life: All software products have life cycles. End-of-life refers to the date when a software development company no longer provides automatic fixes, updates, or online technical assistance for the product. *Source:* [US-CERT alert TA-14-310A](#)

End-point security: Security controls that validate the security compliance of the client system that is attempting to use the Secure Sockets Layer (SSL) virtual private networks (VPN). Endpoint security controls also include security protection mechanisms, such as Web browser cache cleaners, that remove sensitive information from client systems. *Source:* [NIST: SP 800-113](#)

Enterprise network: The configuration of computer systems within an organization. Includes local area networks (LAN), wide area networks (WAN), bridges, and applications. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Enterprise-wide: An entire organization, rather than a single line of business or function. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Exploit: A technique or code that uses a vulnerability to provide system access to the attacker. An exploit is an intentional attack to impact an operating system or application program. *Source:* [FFIEC IT Examination Handbook Glossary](#)

External connections: An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. *Source:* [NIST: SP 800-53](#)

FTP (file transfer protocol): A standard high-level protocol for transferring files from one computer to another, usually implemented as an application level program. *Source:* [National Telecommunications and Information Administration](#)

Financial Services Information Sharing and Analysis Center (FS-ISAC): A nonprofit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information. *Source:* *Derived from* [FS-ISAC](#)

Firewall: Hardware or software link in a network that relays only data packets clearly intended and authorized to reach the other side. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Frame relay: A high-performance WAN protocol that operates at the physical and data link layers of the open systems interconnect (OSI) reference model. Frame relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. Frame relay uses existing T1 and T3 lines and provides connection speeds from 56 Kbps to T1. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Gap analysis: A comparison that identifies the difference between actual and desired outcomes. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Governance: In computer security, the setting of clear expectations for the conduct (behaviors and actions) of the entity being governed and directing, controlling, and strongly influencing the entity to achieve these expectations. Governance includes specifying a framework for

decision-making, with assigned decision rights and accountability, intended to consistently produce desired behaviors and actions. *Source: [FFIEC IT Examination Handbook Glossary](#)*

Hypervisor: A piece of software that provides abstraction of all physical resources (such as central processing units, memory, network, and storage) and thus enables multiple computing stacks (consisting of an operating system, middleware and application programs) called virtual machines to be run on a single physical host. *Source: [NIST SP 800-125a Draft](#)*

Incident response plan: A plan that defines the action steps, involved resources, and communication strategy upon identifying a threat or potential threat event, such as a breach in security protocol, power or telecommunications outage, severe weather, or workplace violence. *Source: [FFIEC IT Examination Handbook Glossary](#)*

Information security: The result of any system of policies or procedures for identifying, controlling, and protecting information from unauthorized disclosure. Also, the processes by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations. *Source: [FFIEC IT Examination Handbook Glossary](#)*

Information systems: Electronic and paper-based systems. Electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information systems can include networks (computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems). Other examples are backup tapes, portable computers, personal digital assistants, media such as compact disks, micro drives, and diskettes, and media used in software development and testing. *Source: [FFIEC Information Security Booklet](#)*

Infrastructure: Systems technologies, including operations such as central computer processing, distributed processing, end-user computing, local area networking, and telecommunications. Includes the transmission media (e.g., voice, data, and video), routers, aggregators, repeaters, and other devices that control transmission paths; also includes the software used to send, receive, and manage transmitted signals. These operations often represent critical services to financial institutions and their customers. *Source: [Based on FFIEC IT Examination Handbook Glossary](#)*

Internet service provider (ISP): A company that provides its customers with access to the Internet (e.g., AT&T, Verizon, CenturyLink). *Source: [FFIEC IT Examination Handbook Glossary](#)*

Intrusion detection system (IDS): Software and hardware that detect and log inappropriate, incorrect, or anomalous activity. IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses sensors to monitor packets on the network to which it is attached. *Source: [FFIEC IT Examination Handbook Glossary](#)*

Intrusion prevention systems (IPS): A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its target. *Source:* [NISTIR 7298 Revision 2](#)

Life-cycle process: The multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system. *Source:* [NIST System Development Life Cycle](#)

Malware: Designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Man-in-the-middle attack (MITM): Places the attacker's computer in the communication line between the server and the client. The attacker's machine can monitor and change communications. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Metrics: A quantitative measurement. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Mobile device: A portable computing and communications device with information-storage capability. Examples include notebook and laptop computers, cellular telephones and smart phones, tablets, digital cameras, and audio recording devices. *Source:* [NISTIR 7298 Revision 2](#)

Multifactor authentication: The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number); something you have (e.g., cryptographic identification device or token); and something you are (e.g., biometric). *Source:* [NISTIR 7298 Revision 2](#)

National Institute of Standards and Technology (NIST): An agency of the U.S. Department of Commerce that works to develop and apply technology, measurements, and standards; developed a voluntary cybersecurity framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructures. *Source:* [NIST](#)

Network: Two or more computer systems grouped together to share information, software, and hardware. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Network activity baseline: A base for determining typical utilization patterns so that significant deviations can be detected. *Source:* [NIST: SP 800-61](#)

Network administrator: An individual responsible for the installation, management, and control of a network. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Network diagram: A description of any kind of locality in terms of its physical layout. In the context of communication networks, a topology describes pictorially the configuration or

arrangement of a network, including its nodes and connecting communication lines. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Operating system: A system that supports and manages software applications. Operating systems allocate system resources, provide access and security controls, maintain file systems, and manage communications between end users and hardware devices. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Outsourcing: The practice of contracting with another entity to perform services that might otherwise be conducted in-house. Contracted relationship with a third party to provide services, systems, or support. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Patch: Software code that replaces or updates other code frequently to correct security flaws. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Penetration test: The process of using approved, qualified personnel to conduct real-world attacks against a system to identify and correct security weaknesses before they are discovered and exploited by others. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Person-to-Person payments: Online payments using electronic messaging invoke a transfer of value between the parties over existing proprietary networks as “on-us” transactions. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Phishing: A digital form of social engineering that uses authentic-looking—but bogus—e-mail to request information from users or direct them to fake Web sites that request information. *Source:* [NIST: SP 800-83](#)

Principles of least privilege: The security objective of granting users only the access needed to perform official duties. *Source:* [NISTIR 7298 Revision 2](#)

Privileged access: Individuals with the ability to override system or application controls. *Source:* [FFIEC Information Security Booklet](#)

Real-time network monitoring: Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access. *Source:* [NISTIR 7298 Revision 2](#)

Red team: A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The red team’s objective is to improve enterprise information assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders in an operational environment. *Source:* [NIST: CNSI-4009](#)

Remote access: The ability to obtain access to a computer or network from a remote location. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Remote deposit captures (RDC): A service that enables users at remote locations to scan digital images of checks and transmit the captured data to a financial institution or a merchant that is a customer of a financial institution. *Source:* [FFIEC IT Examination Handbook Glossary](#)

- Removable media:** Portable electronic storage media, such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device and which is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar storage devices. *Source:* [NIST: CNSSI-4009](#)
- Resilience:** The ability of an organization to recover from a significant disruption and resume critical operations. *Source:* [FFIEC IT Examination Handbook Glossary](#)
- Resilience testing:** Testing of an institution's business continuity and disaster recovery resumption plans. *Source:* [FFIEC IT Examination Handbook Glossary](#)
- Risk assessment:** A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat. *Source:* [FFIEC IT Examination Handbook Glossary](#)
- Risk management:** The total process required to identify, control, and minimize the impact of uncertain events. The objective of a risk management program is to reduce risk and obtain and maintain appropriate management approval. *Source:* [FFIEC IT Examination Handbook Glossary](#)
- Rlogin:** Remote login. A UNIX utility that allows a user to login to a remote host on a network, as if it were directly connected, and make use of various services. Remote login is an information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. *Source:* [NIST Electronic Authentication Guidance](#)
- Rogue wireless access:** An unauthorized wireless node on a network. *Source:* [NISTIR 7298 Revision 2](#)
- Router:** A hardware device that connects two or more networks and routes incoming data packets to the appropriate network. *Source:* [FFIEC IT Examination Handbook Glossary](#)
- Sandbox:** A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized. *Source:* [NIST: CNSSI-4009](#)
- Security log:** A record that contains login and logout activity and other security-related events and that is used to track security-related information on a computer system. *Source:* [NIST: SP 800-92](#)
- Security posture:** The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, and policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. *Source:* [NISTIR 7298 Revision 2](#)

Sensitive customer information: A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number. *Source:* [Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#)

Server: A computer or other device that manages a network service. An example is a print server, which is a device that manages network printing. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Service-level agreement (SLA): An agreement that details the responsibilities of an IT service provider, the rights of the service provider's customers, and the penalties assessed when the service provider violates any element of the SLA. SLAs also identify and define the service, plus the supported products, evaluation criteria, and quality of service customers should expect. SLAs are typically measured in terms of metrics. Examples include processing completion times and systems availability times. *Source:* [FFIEC IT Examination Handbook Glossary](#)

Social engineering: A general term for trying to trick people into revealing confidential information or performing certain actions. *Source:* [NIST SP 800-114](#)

Spear phishing: An attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into the targeted network. *Source:* [Guidelines for Secure Use of Social Media by Federal Departments and Agencies](#)

SQL injection attack: An exploit of target software that constructs structure query language (SQL) statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended. SQL injection enables an attacker to talk directly to the database, thus bypassing the application completely. Successful injection can cause information disclosure as well as ability to add or modify data in the database. *Source:* [MITRE Common Attack Pattern Enumeration and Classification](#)

System development lifecycle process: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. *Source:* [NIST System Development Life Cycle](#)

T1: A special type of telephone line for digital communication and transmission. T1 lines provide for digital transmission with signaling speed of 1.544 Mbps (1,544,000 bits per

second). This is the standard for digital transmissions in North America. Usually delivered on fiber optic lines. *Source: [FFIEC IT Examination Handbook Glossary](#)*

Telnet: An interactive, text-based communications session between a client and a host. It is used mainly for remote login and simple control services to systems with limited resources or to systems with limited needs for security. *Source: [Guide to Industrial Control Systems \(ICS\) Security](#)*

Third-party relationship: Any business arrangement between a financial institution and another entity, by contract or otherwise. *Source: [OCC Bulletin 2013-29](#)*

Third-party service provider: Any type of company, including affiliated entities, non-affiliated entities, and alliances of companies providing products and services to the financial institution. Other terms used to describe service providers include vendors, subcontractors, external service providers, application service providers, and outsourcers. *Source: [FFIEC IT Examination Handbook Glossary](#)*

Threat intelligence: The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision-making. *Source: [SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project](#)*

Token: A small device with an embedded computer chip that can be used to store and transmit electronic information. *Source: [FFIEC IT Examination Handbook Glossary](#)*

Trusted zone: A channel in which the end points are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include secure socket layer, internet protocol security and a secure physical connection. *Source: [CNSSI Glossary](#)*

US-CERT: The U.S. Computer Emergency Readiness Team, part of the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center. US-CERT is a partnership between the Department of Homeland Security and the public and private sectors, established to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation. *Source: [US-CERT](#)*

Virtual machine: A software emulation of a physical computing environment. *Source: [Webster's Dictionary](#)*

VPN (virtual private network): A computer network that uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. *Source: [FFIEC IT Examination Handbook Glossary](#)*

Vulnerability: A hardware, firmware, or software flaw that leaves an information system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to information or to disrupt critical processing. *Source: [FFIEC IT Examination Handbook Glossary](#)*

Zero-day attack: An attack on a piece of software that has a vulnerability for which there is no known patch. *Source:* [*DHS Continuous Diagnostics and Mitigation*](#)