
# Cybersecurity Assessment Tool

May 2017

# Contents



## Additional Resources

# User's Guide

## Overview

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council[1] (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**

**Risk Levels**

**Activity, Service, or Product**

| 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) |

## 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**<br>**Cyber Risk Management and Oversight**<br>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. | |
| **Assessment Factors** | **Governance** includes oversight, strategies, policies, and IT asset management to implement an effective governance of the cybersecurity program.<br><br>**Risk Management** includes a risk management program, risk assessment process, and audit function to effectively manage risk and assess the effectiveness of key controls.<br><br>**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.<br><br>**Training and Culture** includes the employee training and customer awareness programs contributing to an organizational culture that emphasizes the mitigation of cybersecurity threats. |
| **Domain 2**<br>**Threat Intelligence and Collaboration**<br>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. | |
| **Assessment Factors** | **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.<br><br>**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.<br><br>**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. |
| **Domain 3**<br>**Cybersecurity Controls**<br>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. | |
| **Assessment Factors** | **Preventative Controls** deter and prevent cyber attacks and include infrastructure management, access management, device and end-point security, and secure coding.<br><br>**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.<br><br>**Corrective Controls** are utilized to resolve system and software vulnerabilities through patch management and remediation of issues identified during vulnerability scans and penetration testing. |
| **Domain 4**<br>**External Dependency Management**<br>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. | |
| **Assessment Factors** | **Connections** incorporate the identification, monitoring, and management of external connections and data flows to third parties.<br><br>**Relationship Management** includes due diligence, contracts, and ongoing monitoring to help ensure controls complement the institution's cybersecurity program. |

| Domain 5<br>**Cyber Incident Management and Resilience**<br>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** | **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.<br><br>**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.<br><br>**Escalation & Reporting** ensures key stakeholders are informed about the impact of cyber incidents, and regulators, law enforcement, and customers are notified as required. |

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.

Figure 3: Cybersecurity Maturity Levels

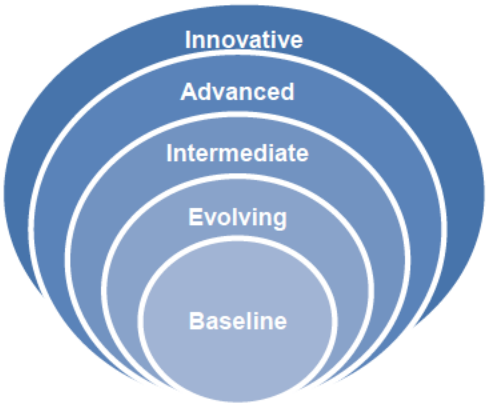


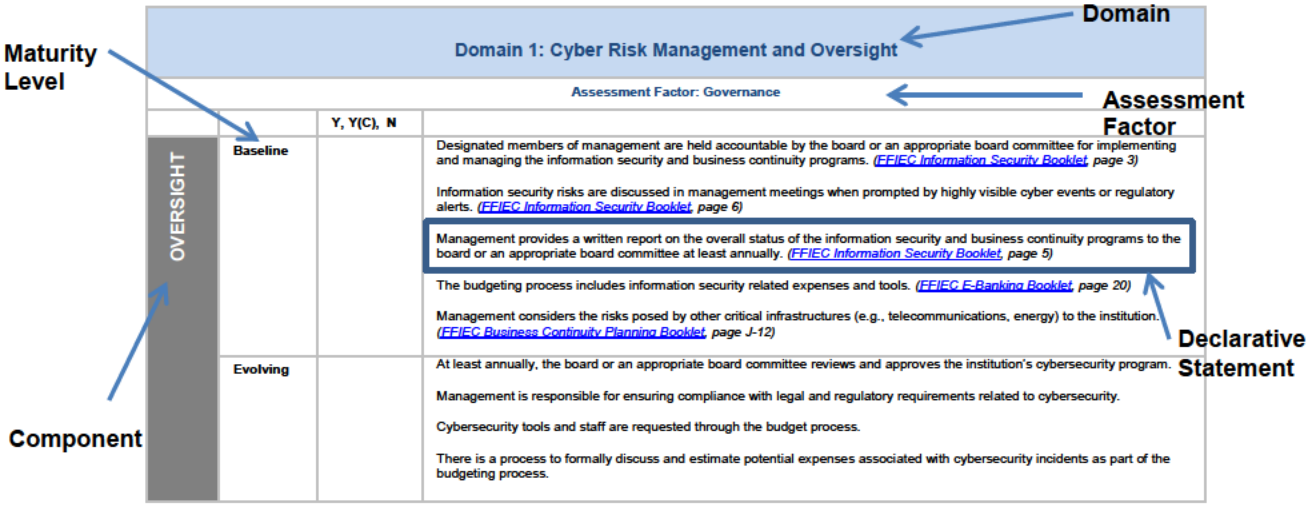

Table 2: Maturity Levels Defined

| 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**




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

[3]Compensating 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.

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 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**

| Cybersecurity Maturity Level for Each Domain | Inherent Risk Levels: Least | Minimal | Moderate | Significant | Most |
|---|---|---|---|---|---|
| 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** | | 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)*<br><br>Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. *(FFIEC Information Security Booklet, page 6)*<br><br>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)*<br><br>The budgeting process includes information security related expenses and tools. *(FFIEC E-Banking Booklet, page 20)*<br><br>Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. *(FFIEC Business Continuity Planning Booklet, page J-12)* |
| | **Evolving** | | At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program.<br><br>Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.<br><br>Cybersecurity tools and staff are requested through the budget process.<br><br>There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process. |
| | **Intermediate** | | The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities.<br><br>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.<br><br>The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.<br><br>Cyber risks that exceed the risk appetite are escalated to management.<br><br>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.<br><br>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.<br><br>The board or an appropriate board committee ensures management takes appropriate actions to address changing cyber risks or significant cybersecurity issues.<br><br>The budget process for requesting additional cybersecurity staff and tools is integrated into business units' budget processes. |
| | **Advanced** | | The board or board committee approved cyber risk appetite statement is part of the enterprise-wide risk appetite statement.<br><br>Management has a formal process to continuously improve cybersecurity oversight.<br><br>The budget process for requesting additional cybersecurity staff and tools maps current resources and tools to the cybersecurity strategy.<br><br>Management and the board or an appropriate board committee hold business units accountable for effectively managing all cyber risks associated with their activities.<br><br>Management identifies root cause(s) when cyber attacks result in material loss.<br><br>The board or an appropriate board committee ensures that management's actions consider the cyber risks that the institution poses to the financial sector. |
| | **Innovative** | | The board or an appropriate board committee discusses ways for management to develop cybersecurity improvements that may be adopted sector-wide.<br><br>The board or an appropriate board committee verifies that management's actions consider the cyber risks that the institution poses to other critical infrastructures (e.g., telecommunications, energy). |

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

| | | | |
|---|---|---|---|
| | **Advanced** | | The cybersecurity strategy outlines the institution's future state of cybersecurity with short-term and long-term perspectives.<br><br>Industry-recognized cybersecurity standards are used as sources during the analysis of cybersecurity program gaps.<br><br>The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructure in the financial services industry.<br><br>The risk appetite is informed by the institution's role in critical infrastructure.<br><br>Management is continuously improving the existing cybersecurity program to adapt as the desired cybersecurity target state changes. |
| | **Innovative** | | The cybersecurity strategy identifies and communicates the institution's role as it relates to other critical infrastructures. |
| **IT ASSET MANAGEMENT** | **Baseline** | | An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. *(FFIEC Information Security Booklet, page 9)*<br><br>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)*<br><br>Management assigns accountability for maintaining an inventory of organizational assets. *(FFIEC Information Security Booklet, page 9)*<br><br>A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools. *(FFIEC Information Security Booklet, page 56)* |
| | **Evolving** | | The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets.<br><br>The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards.<br><br>The institution proactively manages system EOL (e.g., replacement) to limit security risks.<br><br>Changes are formally approved by an individual or committee with appropriate authority and with separation of duties. |
| | **Intermediate** | | Baseline configurations cannot be altered without a formal change request, documented approval, and an assessment of security implications.<br><br>A formal IT change management process requires cybersecurity risk to be evaluated during the analysis, approval, testing, and reporting of changes. |

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

| | | | |
|---|---|---|---|
| | **Advanced** | | Cybersecurity metrics are used to facilitate strategic decision-making and funding in areas of need.<br><br>Independent risk management sets and monitors cyber-related risk limits for business units.<br><br>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.<br><br>A process is in place to analyze the financial impact cyber incidents have on the institution's capital.<br><br>The cyber risk data aggregation and real-time reporting capabilities support the institution's ongoing reporting needs, particularly during cyber incidents. |
| | **Innovative** | | The risk management function identifies and analyzes commonalities in cyber events that occur both at the institution and across other sectors to enable more predictive risk management.<br><br>A process is in place to analyze the financial impact that a cyber incident at the institution may have across the financial sector. |
| RISK ASSESSMENT | **Baseline** | | A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, and customer information systems. *(FFIEC Information Security Booklet, page 8)*<br><br>The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls. *(FFIEC Information Security Booklet, page 12)*<br><br>The risk assessment is updated to address new technologies, products, services, and connections before deployment. *(FFIEC Information Security Booklet, page 13)* |
| | **Evolving** | | Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships.<br><br>The focus of the risk assessment has expanded beyond customer information to address all information assets.<br><br>The risk assessment considers the risk of using EOL software and hardware components. |
| | **Intermediate** | | The risk assessment is adjusted to consider widely known risks or risk management practices. |

| | | | |
|---|---|---|---|
| | **Advanced** | | An enterprise-wide risk management function incorporates cyber threat analysis and specific risk exposure as part of the enterprise risk assessment. |
| | **Innovative** | | The risk assessment is updated in real time as changes to the risk profile occur, new applicable standards are released or updated, and new exposures are anticipated.<br><br>The institution uses information from risk assessments to predict threats and drive real-time responses.<br><br>Advanced or automated analytics offer predictive information and real-time risk metrics. |
| AUDIT | **Baseline** | | Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems. *(FFIEC Audit Booklet, page 4)*<br><br>The independent audit function validates controls related to the storage or transmission of confidential data. *(FFIEC Audit Booklet, page 1)*<br><br>Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance). *(FFIEC Operations Booklet, page 29)*<br><br>Issues and corrective actions from internal audits and independent testing/assessments are formally tracked to ensure procedures and control lapses are resolved in a timely manner. *(FFIEC Information Security Booklet, page 6)* |
| | **Evolving** | | The independent audit function validates that the risk management function is commensurate with the institution's risk and complexity.<br><br>The independent audit function validates that the institution's threat information sharing is commensurate with the institution's risk and complexity.<br><br>The independent audit function validates that the institution's cybersecurity controls function is commensurate with the institution's risk and complexity.<br><br>The independent audit function validates that the institution's third-party relationship management is commensurate with the institution's risk and complexity.<br><br>The independent audit function validates that the institution's incident response program and resilience are commensurate with the institution's risk and complexity. |

| | | | |
|---|---|---|---|
| | **Intermediate** | | A formal process is in place for the independent audit function to update its procedures based on changes to the institution's inherent risk profile.<br><br>The independent audit function validates that the institution's threat intelligence and collaboration are commensurate with the institution's risk and complexity.<br><br>The independent audit function regularly reviews management's cyber risk appetite statement.<br><br>Independent audits or reviews are used to identify gaps in existing security capabilities and expertise. |
| | **Advanced** | | A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across the sector.<br><br>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.<br><br>Independent audits or reviews are used to identify cybersecurity weaknesses, root causes, and the potential impact to business units. |
| | **Innovative** | | A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across other sectors the institution depends upon.<br><br>The independent audit function uses sophisticated data mining tools to perform continuous monitoring of cybersecurity processes or controls. |
| **Assessment Factor: Resources** | | | |
| STAFFING | **Baseline** | | Information security roles and responsibilities have been identified. *(FFIEC Information Security Booklet, page 7)*<br><br>Processes are in place to identify additional expertise needed to improve information security defenses. *(FFIEC Information Security Work Program, Objective I: 2-8)* |

| | | | |
|---|---|---|---|
| | **Evolving** | | A formal process is used to identify cybersecurity tools and expertise that may be needed.<br><br>Management with appropriate knowledge and experience leads the institution's cybersecurity efforts.<br><br>Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position.<br><br>Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk. |
| | **Intermediate** | | The institution has a program for talent recruitment, retention, and succession planning for the cybersecurity and resilience staffs. |
| | **Advanced** | | The institution benchmarks its cybersecurity staffing against peers to identify whether its recruitment, retention, and succession planning are commensurate.<br><br>Dedicated cybersecurity staff develops, or contributes to developing, integrated enterprise-level security and cyber defense strategies. |
| | **Innovative** | | The institution actively partners with industry associations and academia to inform curricula based on future cybersecurity staffing needs of the industry. |
| **Assessment Factor: Training and Culture** | | | |
| **TRAINING** | **Baseline** | | Annual information security training is provided. *(FFIEC Information Security Booklet, page 66)*<br><br>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)*<br><br>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)*<br><br>Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials). *(FFIEC E-Banking Work Program, Objective 6-3)* |

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

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

| Domain 2: Threat Intelligence and Collaboration | | | |
|---|---|---|---|
| Assessment Factor: Threat Intelligence | | | |
| | | Y, Y(C), N | |
| THREAT INTELLIGENCE AND INFORMATION | **Baseline** | | The institution belongs or subscribes to a threat and vulnerability information sharing source(s) that provides information on threats (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC], U.S. Computer Emergency Readiness Team [US-CERT]). *(FFIEC E-Banking Work Program, page 28)*<br><br>Threat information is used to monitor threats and vulnerabilities. *(FFIEC Information Security Booklet, page 83)*<br><br>Threat information is used to enhance internal risk management and controls. *(FFIEC Information Security Booklet, page 4)* |
| | **Evolving** | | Threat information received by the institution includes analysis of tactics, patterns, and risk mitigation recommendations. |
| | **Intermediate** | | A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources.<br><br>Protocols are implemented for collecting information from industry peers and government.<br><br>A read-only, central repository of cyber threat intelligence is maintained. |
| | **Advanced** | | A cyber intelligence model is used for gathering threat information.<br><br>Threat intelligence is automatically received from multiple sources in real time.<br><br>The institution's threat intelligence includes information related to geopolitical events that could increase cybersecurity threat levels. |
| | **Innovative** | | A threat analysis system automatically correlates threat data to specific risks and then takes risk-based automated actions while alerting management.<br><br>The institution is investing in the development of new threat intelligence and collaboration mechanisms (e.g., technologies, business processes) that will transform how information is gathered and shared. |

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

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

| | | | |
|---|---|---|---|
| | **Innovative** | | A mechanism is in place for sharing cyber threat intelligence with business units in real time including the potential financial and operational impact of inaction.<br><br>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.<br><br>The institution is leading efforts to create new sector-wide information-sharing channels to address gaps in external-facing information-sharing mechanisms. |

| Domain 3: Cybersecurity Controls | | | |
|---|---|---|---|
| Assessment Factor: Preventative Controls | | | |
| | | Y, Y(C), N | |
| INFRASTRUCTURE MANAGEMENT | **Baseline** | | Network perimeter defense tools (e.g., border router and firewall) are used. *(FFIEC Information Security Booklet, page 33)*<br><br>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)*<br><br>All ports are monitored. *(FFIEC Information Security Booklet, page 50)*<br><br>Up to date antivirus and anti-malware tools are used. *(FFIEC Information Security Booklet, page 78)*<br><br>Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced. *(FFIEC Information Security Booklet, page 56)*<br><br>Ports, functions, protocols and services are prohibited if no longer needed for business purposes. *(FFIEC Information Security Booklet, page 50)*<br><br>Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. *(FFIEC Information Security Booklet, page 56)*<br><br>Programs that can override system, object, network, virtual machine, and application controls are restricted. *(FFIEC Information Security Booklet, page 41)*<br><br>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)*<br><br>Wireless network environments require security settings with strong encryption for authentication and transmission. (*N/A if there are no wireless networks.) *(FFIEC Information Security Booklet, page 40)* |
| | **Evolving** | | There is a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and internal network(s).<br><br>Antivirus and intrusion detection/prevention systems (IDS/IPS) detect and block actual and attempted attacks or intrusions.<br><br>Technical controls prevent unauthorized devices, including rogue wireless access devices and removable media, from connecting to the internal network(s).<br><br>A risk-based solution is in place at the institution or Internet hosting |

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

| | | | |
|---|---|---|---|
| | | | Public-facing servers are routinely rotated and restored to a known clean state to limit the window of time a system is exposed to potential threats. |
| ACCESS AND DATA MANAGEMENT | **Baseline** | | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. *(FFIEC Information Security Booklet, page 19)*<br><br>Employee access to systems and confidential data provides for separation of duties. *(FFIEC Information Security Booklet, page 19)*<br><br>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)*<br><br>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)*<br><br>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)*<br><br>Identification and authentication are required and managed for access to systems, applications, and hardware. *(FFIEC Information Security Booklet, page 21)*<br><br>Access controls include password complexity and limits to password attempts and reuse. *(FFIEC Information Security Booklet, page 66)*<br><br>All default passwords and unnecessary default accounts are changed before system implementation. *(FFIEC Information Security Booklet, page 61)*<br><br>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)*<br><br>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)*<br><br>Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems. *(FFIEC Information Security Booklet, page 47)*<br><br>All passwords are encrypted in storage and in transit. *(FFIEC Information Security Booklet, page 21)* |

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

| | | | |
|---|---|---|---|
| | **Intermediate** | | The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.<br><br>Controls are in place to prevent unauthorized escalation of user privileges.<br><br>Access controls are in place for database administrators to prevent unauthorized downloading or transmission of confidential data.<br><br>All physical and logical access is removed immediately upon notification of involuntary termination and within 24 hours of an employee's voluntary departure.<br><br>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.<br><br>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.)<br><br>Confidential data are encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.<br><br>Controls are in place to prevent unauthorized access to collaborative computing devices and applications (e.g., networked white boards, cameras, microphones, online applications such as instant messaging and document sharing). (* N/A if collaborative computing devices are not used.) |
| | **Advanced** | | Encryption of select data at rest is determined by the institution's data classification and risk assessment.<br><br>Customer authentication for high-risk transactions includes methods to prevent malware and man-in-the-middle attacks (e.g., using visual transaction signing). |

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

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

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

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

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

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

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

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

| Domain 4: External Dependency Management | | | |
|---|---|---|---|
| Assessment Factor: Connections | | | |
| | | Y, Y(C), N | |
| CONNECTIONS | **Baseline** | | The critical business processes that are dependent on external connectivity have been identified. *(FFIEC Information Security Booklet, page 9)*<br><br>The institution ensures that third-party connections are authorized. *(FFIEC Information Security Booklet, page 17)*<br><br>A network diagram is in place and identifies all external connections. *(FFIEC Information Security Booklet, page 9)*<br><br>Data flow diagrams are in place and document information flow to external parties. *(FFIEC Information Security Booklet, page 10)* |
| | **Evolving** | | Critical business processes have been mapped to the supporting external connections.<br><br>The network diagram is updated when connections with third parties change or at least annually.<br><br>Network and systems diagrams are stored in a secure manner with proper restrictions on access.<br><br>Controls for primary and backup third-party connections are monitored and tested on a regular basis. |
| | **Intermediate** | | A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.<br><br>Security controls are designed and verified to detect and prevent intrusions from third-party connections.<br><br>Monitoring controls cover all external connections (e.g., third-party service providers, business partners, customers).<br><br>Monitoring controls cover all internal network-to-network connections. |
| | **Advanced** | | The security architecture is validated and documented before network connection infrastructure changes.<br><br>The institution works closely with third-party service providers to maintain and improve the security of external connections. |

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

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

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

| Domain 5: Cyber Incident Management and Resilience | | | |
|---|---|---|---|
| Assessment Factor: Incident Resilience Planning and Strategy | | | |
| | | Y, Y(C), N | |
| PLANNING | **Baseline** | | The institution has documented how it will react and respond to cyber incidents. *(FFIEC Business Continuity Planning Booklet, page 4)*<br><br>Communication channels exist to provide employees a means for reporting information security events in a timely manner. *(FFIEC Information Security Booklet, page 83)*<br><br>Roles and responsibilities for incident response team members are defined. *(FFIEC Information Security Booklet, page 84)*<br><br>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)*<br><br>A formal backup and recovery plan exists for all critical business lines. *(FFIEC Business Continuity Planning Booklet, page 4)*<br><br>The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. *(FFIEC Information Security Booklet, page 71)* |
| | **Evolving** | | The remediation plan and process outlines the mitigating actions, resources, and time parameters.<br><br>The corporate disaster recovery, business continuity, and crisis management plans have integrated consideration of cyber incidents.<br><br>Alternative processes have been established to continue critical activity within a reasonable time period.<br><br>Business impact analyses have been updated to include cybersecurity.<br><br>Due diligence has been performed on technical sources, consultants, or forensic service firms that could be called to assist the institution during or following an incident. |

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

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

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

| | | | |
|---|---|---|---|
| RESPONSE AND MITIGATION | **Baseline** | | Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information. *(FFIEC Information Security Booklet, page 84)* |
| | **Evolving** | | The incident response plan is designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities.<br><br>A process is in place to help contain incidents and restore operations with minimal service disruption.<br><br>Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware).<br><br>Procedures include containment strategies and notifying potentially impacted third parties.<br><br>Processes are in place to trigger the incident response program when an incident occurs at a third party.<br><br>Records are generated to support incident investigation and mitigation.<br><br>The institution calls upon third parties, as needed, to provide mitigation services.<br><br>Analysis of events is used to improve the institution's security measures and policies. |
| | **Intermediate** | | Analysis of security incidents is performed in the early stages of an intrusion to minimize the impact of the incident.<br><br>Any changes to systems/applications or to access entitlements necessary for incident management are reviewed by management for formal approval before implementation.<br><br>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.<br><br>Processes are in place to ensure that restored assets are appropriately reconfigured and thoroughly tested before being placed back into operation. |
| | **Advanced** | | The incident management function collaborates effectively with the cyber threat intelligence function during an incident.<br><br>Links between threat intelligence, network operations, and incident response allow for proactive response to potential incidents.<br><br>Technical measures apply defense-in-depth techniques such as deep-packet inspection and black holing for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns and/or DDoS attacks. |

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

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