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 **Cyber Risk Management and Oversight** 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. **Risk Management** includes a risk management program, risk assessment process, and audit function to effectively manage risk and assess the effectiveness of key controls. **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. **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 **Threat Intelligence and Collaboration** 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. **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. **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 **Cybersecurity Controls** 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. **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. **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 **External Dependency Management** 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. **Relationship Management** includes due diligence, contracts, and ongoing monitoring to help ensure controls complement the institution's cybersecurity program.

Domain 5 **Cyber Incident Management and Resilience** Cyber incident management includes establishing, identifying, and analyzing cyber events; prioritizing the institution's containment or mitigation; and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber incident.	
Assessment Factors	**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. **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. **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

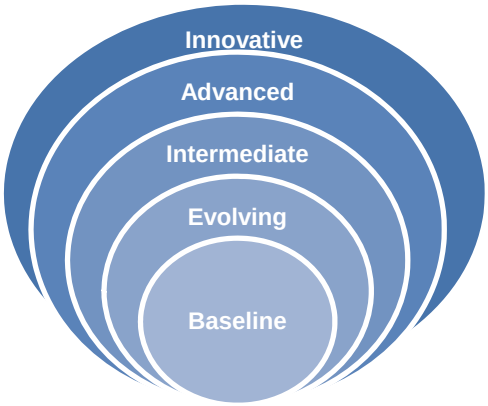


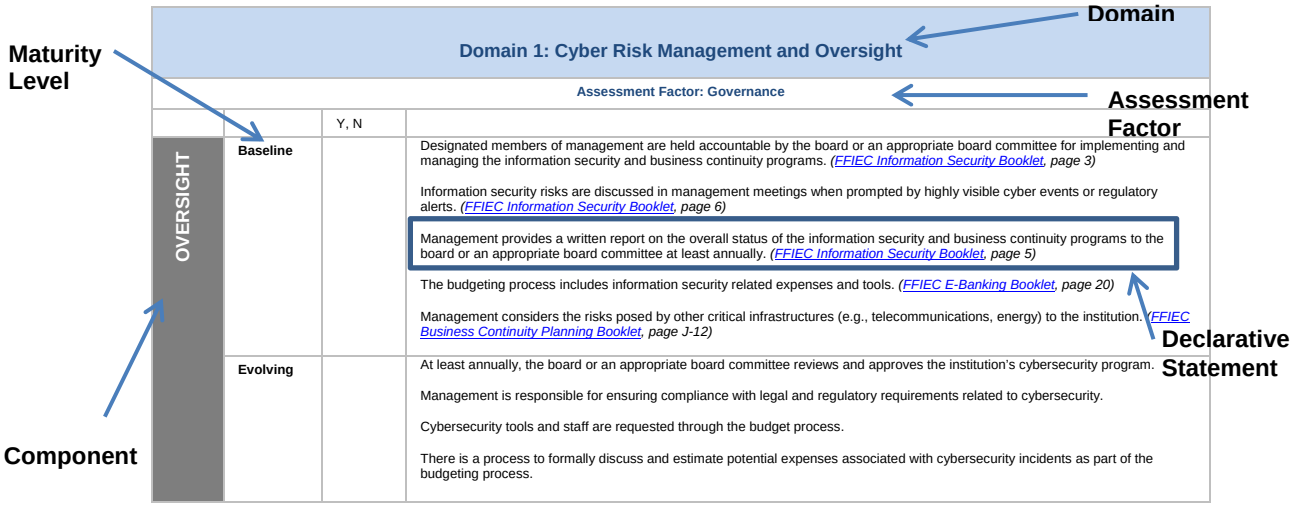
Table 2: Maturity Levels Defined

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.*** 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 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

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

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

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

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

Using the maturity levels in each domain, management can identify potential actions that would increase the institution's overall cybersecurity preparedness. Management can review declarative statements at maturity levels beyond what the institution has achieved to determine the actions needed to reach the next level and implement changes to address gaps. Management's periodic reevaluations of the inherent risk profile and maturity levels may further assist the institution in maintaining an appropriate level of cybersecurity preparedness. In addition, management may also seek an independent validation, such as by the internal audit function, of the institution's Assessment process and findings.

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

Resources

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

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