FFIEC Cybersecurity Assessment Tool

Overview for Chief Executive Officers and Boards of Directors

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council[1] (FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time. The Assessment incorporates cybersecurity-related principles from the *FFIEC Information Technology (IT) Examination Handbook* and regulatory guidance, and concepts from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[2]

Benefits to the Institution

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

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

CEO and Board of Directors

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

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

---

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

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

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

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

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

Assessment's Parts and Process

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

Inherent Risk Profile

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

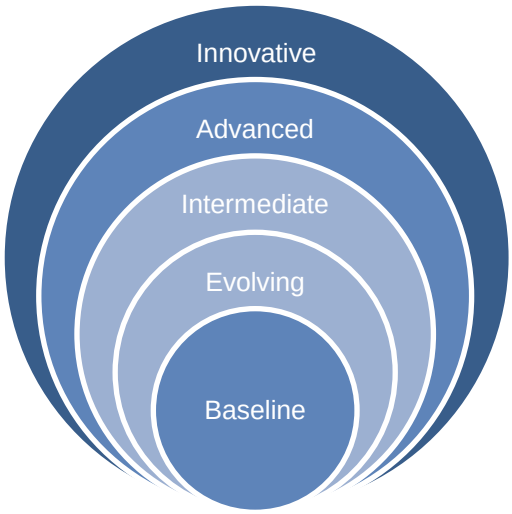
- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

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

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

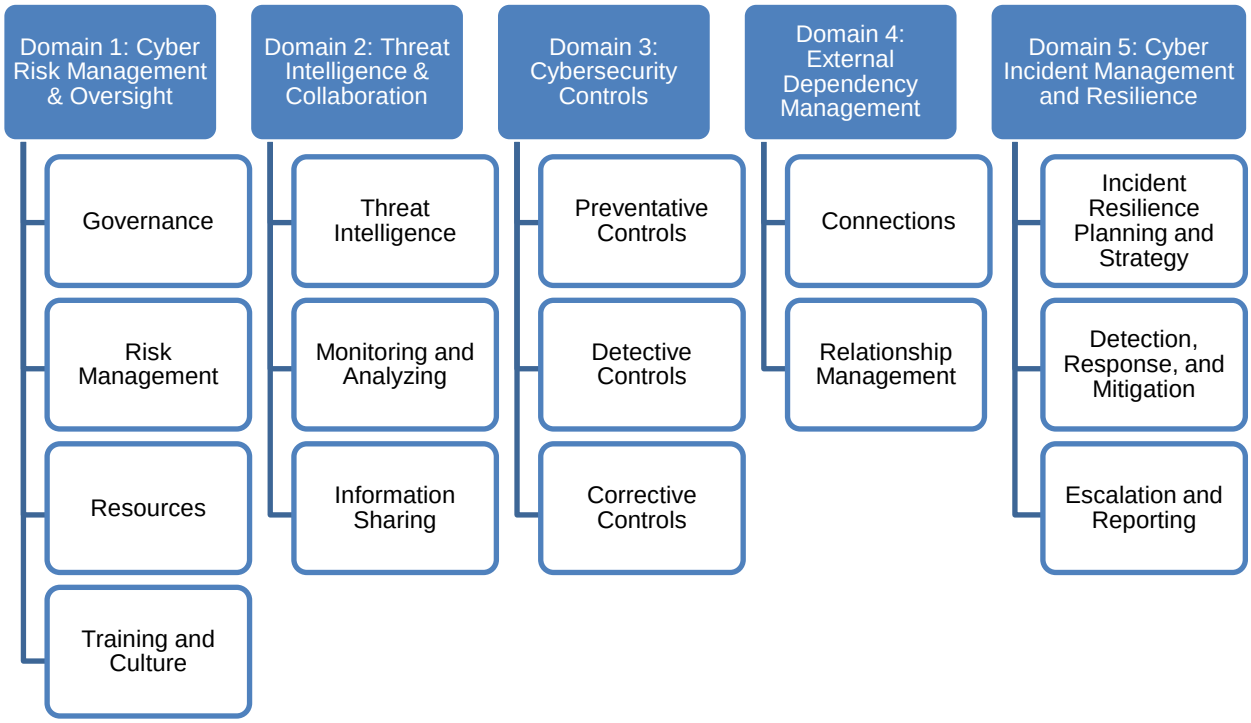
Cybersecurity Maturity

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



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

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



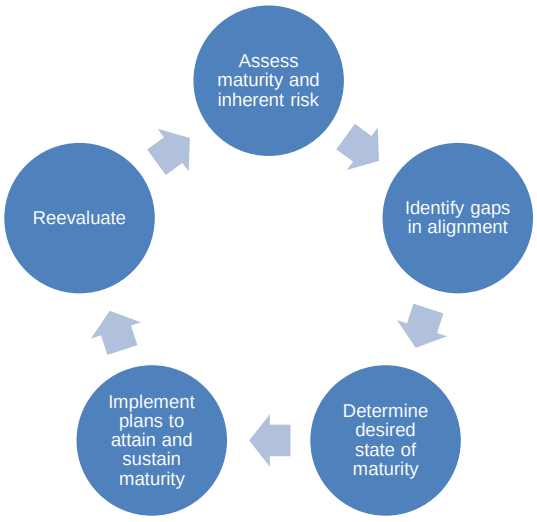
Management can review the institution's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain to understand whether they are aligned. The following table depicts the relationship between an institution's Inherent Risk Profile and its domain Maturity Levels, as there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

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

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

Supporting Implementation

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



Cybersecurity Management & Oversight

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

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

Inherent Risk Profile

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

Cybersecurity Maturity

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

Summary

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