FFIEC Cybersecurity Assessment Tool
Frequently Asked Questions
October 17, 2016

Purpose

The Federal Financial Institutions Examination Council (FFIEC)[1] members have received several requests to clarify points in the 2015 FFIEC Cybersecurity Assessment Tool (Assessment) and supporting materials. This document provides answers to frequently asked questions.

Frequently Asked Questions

1. Why did the FFIEC release the Assessment?

Financial institutions and their service providers are increasingly dependent on information technology (IT) and telecommunications to deliver services to consumers and businesses every day. Disruption, degradation, or unauthorized alteration of information and systems that support these services can affect operations, institutions, and their core processes, and undermine confidence in the nation's financial services sector. Cyber attacks have increased in frequency and severity with recent attacks involving extortion, destructive malware, and compromised credentials.

Management of financial institutions and management of third-party service providers are primarily responsible for assessing and mitigating their entities' cybersecurity risk. FFIEC members developed the Assessment to help institutions' management identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process that financial institutions' management may use to measure their cybersecurity preparedness over time.

2. Does my institution have to use the Assessment?

No. Use of the Assessment by institutions is voluntary. Institution management may choose to use the Assessment, or another framework, or another risk assessment process to identify inherent risk and cybersecurity preparedness. The FFIEC released the Assessment as a voluntary tool that institution management may use to determine the institution's inherent risk and cybersecurity preparedness.

[1] The Council consists of the following six voting members: a member of the Board of Governors of the Federal Reserve System; the Chairman of the Federal Deposit Insurance Corporation; the Director of the Consumer Financial Protection Bureau; the Comptroller of the Currency; the Chairman of the National Credit Union Administration; and the Chairman of the State Liaison Committee.

3. What is the value of the Assessment to management?

By using the Assessment, management will be able to enhance its 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 inherent risks.
- Determining risk management practices and controls that are needed or require enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies.

4. How does the Assessment align with the NIST Cybersecurity Framework?

The FFIEC Information Technology Examination Handbook (IT Handbook), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and industry-accepted cybersecurity practices were used in the development of the Assessment. A mapping of the NIST Cybersecurity Framework to the Assessment is included as Appendix B of the Assessment. NIST reviewed and provided input on the mapping to ensure consistency with NIST Cybersecurity Framework principles and to highlight the complementary nature of the two resources.

5. Will the FFIEC release an automated version of the Assessment?

The FFIEC does not intend to release an automated version of the Assessment at this time. FFIEC members are aware of a number of automated versions of the Assessment developed by financial institutions and industry groups. For example, the Financial Services Sector Coordinating Council (FSSCC) working in conjunction with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and trade associations developed an automated version.[2]

6. In using the Assessment, how do I determine my institution's Inherent Risk Profile?[3]

In completing the Assessment, management may determine the institution's overall Inherent Risk Profile based on the number of applicable statements in each risk level for all activities, products, and services. For example, when a majority of activities, products, or services fall within the Moderate Risk Level, management may determine that the institution has a

[2] Available at https://www.fsisac.com/article/fsscc-automated-cybersecurity-assessment-tool. Although the automated versions of the Assessment are not established or endorsed by FFIEC members, they may help financial institutions complete the Assessment.

[3] Inherent Risk Profile refers to part one of the Assessment and is used to identify the institution's inherent risk.

Moderate Inherent Risk Profile. Each category may, however, pose a different level of inherent risk. Therefore, in addition to evaluating the number of times an institution selects a specific risk level, management may also consider evaluating whether the specific category poses additional risk that should be factored into the overall assessment of inherent risk.

7. In using the Assessment, how do I determine my institution's Cybersecurity Maturity?[4]

Management may determine the institution's maturity level within each of the 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

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. Management determines the declarative statements that 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.

8. How should the Inherent Risk Profile align with Cybersecurity Maturity?

While there are no expected maturity levels for an institution, Inherent Risk levels should be balanced with maturity. 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 their levels of maturity.

Management may choose to evaluate the institution's inherent risk overall, as well as inherent risk for specific activities, services, or products. In general, when the inherent risk of an activity, service, or product rises the maturity level of related controls and risk mitigation activities should increase, as well.

[4] Cybersecurity Maturity refers to part two of the Assessment and is used to identify the institution's maturity level within each of the five domains.

9. How do I account for compensating controls or partial implementation of a declarative statement?

As the Assessment is voluntary, management may choose to customize the Assessment for its institution's needs. Customization may include identifying various methods for accounting for compensating controls or other means for attaining a declarative statement.

10. Can the Assessment be used as part of my institution's oversight of third parties?

Yes. As the Assessment is voluntary, management may choose to use it as a resource for the oversight of third parties as part of the institution's comprehensive third-party management program.

11. In completing the Assessment, how do I account for controls implemented by my institution's third-party service providers?

Management may consider declarative statements in all domains that are attained by a third-party service provider on behalf of the institution. Domain 4: External Dependency Management provides a structure for management to evaluate the institution's oversight of third-party service providers.

Management is responsible for the assessment of the risk associated with the nature, extent and complexity of its institution's third-party relationships. Such assessment includes evaluating the extent to which controls put in place by the institution's third-party service providers could be considered in the institution's mitigation of its overall cybersecurity risk, including the cybersecurity risk associated with its use of third-party service providers.

12. How are the FFIEC members using the Assessment?

To obtain additional information about a particular FFIEC member's use of the Assessment, financial institution management should contact its institution's regulator directly. Management of financial institutions and management of third-party service providers are primarily responsible for assessing and mitigating their entities' cybersecurity risk. FFIEC members developed the Assessment to help institutions' management identify their risks and determine their cybersecurity preparedness.

13. Where can I find more information on the Assessment?

The FFIEC Cybersecurity Assessment Tool web page[5] includes the Assessment as well as the following supplemental materials:

[5] http://www.ffiec.gov/cybersassessmenttool.htm.

- Overview for Chief Executive Officers and Boards of Directors
- User's Guide
- Appendix A: Mapping Baseline Statements to the FFIEC IT Handbook
- Appendix B: Mapping to NIST Cybersecurity Framework
- Appendix C: Glossary

In addition, management may contact its institution's regulator.

14. How can a community institution meet baseline declarative statements?

The Assessment was designed to help institution management identify its institution's inherent risks and determine its institution's cybersecurity maturity. The declarative statements at the baseline level of maturity reflect minimum expectations required by law and regulations or recommended in supervisory guidance. The following outlines an example of related baseline statements across the domains and how a community institution ("Institution A") could attain these statements. The footnotes provide the specific declarative statement.

Institution A belongs to the FS-ISAC's Community Institution Council and receives the weekly Risk Summary Report[6] (Domain 2: Threat Intelligence and Collaboration). In this case, the weekly Risk Summary Report highlighted an FFIEC Joint Statement on Cyber Attacks Involving Extortion.[7] Institution management discussed the statement and its institution's response at its regularly scheduled weekly management meeting[8] (Domain 1: Cyber Risk Management and Oversight). To respond to this risk, management reviewed its detective and corrective controls, including confirming that its systems are configured to protect against this risk through logical segmentation[9] (Domain 3: Cybersecurity Controls). While management reviewed the controls in place, it also reviewed the backup and recovery plans. This institution identified its key data for critical business lines and regularly backs up on an external drive (e.g., thumb drive)[10] (Domain 5: Cyber Incident Management and Resilience). In addition, management

[6] Statement D2.TI.Ti.B.1, "The institution belongs or subscribes to a threat and vulnerability information sharing source(s) that provides information on threats (e.g., FS-ISAC, U.S. Computer Emergency Readiness Team [US-CERT])."

[7] FFIEC Joint Statement on Cyber Attacks Involving Extortion.

[8] Statement D1.G.Ov.B.2, "Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts."

[9] Statement D3.PC.Im.B.5, "Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced." Logical segmentation refers to electronic controls put in place to separate parts of a network.

[10] Statement D5.IR.Pl.B.5, "A formal backup and recovery plan exists for all critical business lines."

reviewed its oversight of third parties and the inclusion of questions to understand the critical third parties' resilience plans[11] (Domain 4: External Dependency Management).

15. Further clarify what the following terms mean with respect to the Assessment.

Trust services: Thought of broadly to include fiduciary services for individual clients (e.g., personal trusts and investment management accounts) and corporate clients (e.g., employee benefit plans, endowments/foundations, and bond issuances), non-fiduciary services (e.g., retail brokerage, custody services [securities, cash and documents], and security-holder services [transfer agent]). Also may be referred to as asset management products and services.

Merchant acquirer: Merchant acquirers sponsor merchants in the retail payments system as members of the credit card association. (Source: FFIEC Retail Payment Systems Booklet)

Global remittance providers: A global remittance or a remittance transfer includes most electronic money transfers sent by consumers in the United States through remittance transfer providers to recipients in other countries. (Source: Regulation E, 12 CFR 205)

Treasury services: A broad collection of services, including but not limited to cash management, liquidity management, trade finance, and information services, offered to corporate or business clients. These services are typically offered through an investment bank.

Asset life-cycle process: This multi-step process starts with the initiation, analysis, design, and implementation of an asset, and continues through the maintenance and disposal of the asset or its system. (Source: NIST System Development Life Cycle)

16. What are the distinctions between declarative statements that repeat at different maturity levels (e.g., statements related to the budget process in Domain 1)?

Declarative statements within Cybersecurity Maturity are designed to build on each other through the maturity levels. Therefore, particular topics are covered at each level of maturity with more mature implementation described as maturity increases. The following outlines an example of budget-related statements across all maturity levels in Domain 1 and how institutions ("Institution B" and "Institution C") attain these statements. In these statements, each level builds upon the lower maturity level demonstrating an increasingly mature approach to responding to the cybersecurity threat. The footnotes provide the specific declarative statement.

[11] Statement D4.RM.Om.B.3, "Ongoing monitoring practices include reviewing critical third parties' resilience plans."

Institution B attained the baseline statement,[12] as it uses the formal budget process to request funding to purchase tools to prevent, detect, and correct information security events. In addition, Institution B attained the next level of maturity, evolving,[13] as it uses the budget process to request funding for cybersecurity tools and staff, which go beyond addressing particular information security events. For example, such tools and staff might include funding to increase business continuity staff or contracting with a third party to increase the institution's ability to rapidly respond to a cybersecurity event. In addition, Institution B has discussed and estimated expenses associated with a potential event.[14]

For Institution C, which attained the intermediate statement,[15] the budgeting for cybersecurity is not only part of the information security or IT group, but is integrated into individual business units of the institution. This integration may be based on the individual business unit's cybersecurity inherent risk from the activities, products, or services they participate in or offer. Then, at the advanced level,[16] Institution C's budget request related to cybersecurity is directly tied to the institution's overall cybersecurity strategy.

17. Does the FFIEC plan to update the Assessment?

FFIEC members plan to update the Assessment as threats, vulnerabilities and operational environments evolve. Updates may be made to incorporate new and updated regulatory guidance, address any identified gaps or enhancements in the Assessment, add or change declarative statements or incorporate feedback from the industry.

18. As the FFIEC IT Handbook is updated, will there be changes to the Assessment?

The booklets of the FFIEC IT Examination Handbook are undergoing revision to incorporate changes in the industry since the last publication, the evolving threat landscape, and concepts in the Assessment. "Appendix A: Mapping Baseline Statements to FFIEC IT Examination Handbook" will be updated to align with new or updated booklets after their release.

[12] Statement D1.G.Ov.B.4, "The budgeting process includes information security related expenses and tools."

[13] Statement D1.G.Ov.E.3, "Cybersecurity tools and staff are requested through the budget process."

[14] Statement D1.G.Ov.E.4, "There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process."

[15] Statement D1.G.Ov.Int.8, "The budget process for requesting additional cybersecurity staff and tools is integrated into business units' budget processes."

[16] Statement D1.G.Ov.A.3, "The budget process for requesting additional cybersecurity staff and tools maps current resources and tools to the cybersecurity strategy."