Office of the Comptroller of the Currency
U.S. Department of the Treasury

OCC BULLETIN 2016-34

Subject: Cybersecurity
Date: October 17, 2016

To: Chief Executive Officers of All National Banks, Federal Branches and Agencies, and Federal Savings Associations; Technology Service Providers; Department and Division Heads; All Examining Personnel; and Other Interested Parties

Description: Frequently Asked Questions on the FFIEC Cybersecurity Assessment Tool

Summary

On June 30, 2015, the Federal Financial Institutions Examination Council (FFIEC),[1] on behalf of its members, issued a Cybersecurity Assessment Tool (Assessment) that financial institutions may use to evaluate their risks and cybersecurity preparedness. At the same time, the Office of the Comptroller of the Currency (OCC) announced that examiners will gradually incorporate the Assessment into examinations of national banks, federal savings associations, and federal branches and agencies (collectively, banks) of all sizes. Appendix A of this bulletin contains answers to frequently asked questions (FAQ) that bankers have posed to OCC examiners and policy staff members. Separately, this bulletin includes additional answers to FAQs that the FFIEC recently issued on behalf of its members. The OCC and FFIEC answers are designed to foster further industry and examiner understanding of the Assessment.

Note for Community Banks

The Assessment is designed for banks of all sizes and incorporates concepts and principles contained in the *FFIEC Information Technology Examination Handbook,* regulatory guidance, applicable laws and regulations, FFIEC joint statements, and well-known industry standards, such as the National Institute of Standards and Technology's Cybersecurity Framework.

The FAQs incorporate questions from bankers, including community bankers, on how to use the Assessment.

Highlights

This bulletin includes

- the OCC FAQs for OCC examiners and banks that choose to use the Assessment.
- the FFIEC FAQs for banks that choose to use the Assessment.

Background

The OCC has implemented the Assessment as part of the bank examination process to benchmark and assess bank cybersecurity efforts. While use of the Assessment is optional for banks, OCC examiners will continue to use the Assessment to supplement examination work to gain a more complete understanding of banks' inherent risk, risk management practices, and controls related to cybersecurity.

The Assessment comprises two parts: an inherent risk profile and cybersecurity maturity.

- **Inherent risk profile** identifies the amount of risk posed to a bank by the types, volume, and complexity of the bank's technologies and connections, delivery channels, products and services,

organizational characteristics, and external threats, notwithstanding the bank's risk-mitigating controls.

- **Cybersecurity maturity** is evaluated in five domains: cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resilience. Each domain has five levels of maturity: baseline, evolving, intermediate, advanced, and innovative. A bank's appropriate cybersecurity maturity levels depend on its inherent risk profile.

Further Information

Please contact the Operational Risk Division at (202) 649-6550.

Bethany A. Dugan
Deputy Comptroller for Operational Risk

---

[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.

Related Link

- "FFIEC Cybersecurity Assessment Tool Frequently Asked Questions" [http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT%20FAQs.pdf] (PDF)

Appendix A: OCC Frequently Asked Questions Regarding the FFIEC Cybersecurity Assessment Tool

Purpose

The OCC examiners and policy staff members have received several requests from bankers to clarify points on the OCC's use of the Assessment and supporting materials. This bulletin provides answers to FAQs from bankers.

1. **When will my OCC examiner use the Assessment?**

   OCC examiners began incorporating the Assessment into safety and soundness and information technology examinations in late 2015. Examiners will continue to use the Assessment to supplement examination processes going forward and will have completed the first iteration at all banks by the end of supervisory year 2017.

   Banks' ability to understand and mitigate cyber threats is critical to the safe and sound operation of those banks and the federal banking system. That is why the OCC is incorporating the Assessment into its examination process.

   While use of the Assessment is optional for banks, OCC examiners will continue to use the Assessment to supplement examination work to gain a more complete understanding of banks' inherent risk, risk management practices, and controls related to cybersecurity, as well as to inform future supervisory work and policy development.

2. **What do I need to do to prepare for an OCC examination of my bank that incorporates the Assessment?**

   Before examinations, examiners will send banks request letters that highlight specific information that examiners will need to conduct the examinations efficiently and effectively using the Assessment.

   The OCC is sensitive to the time and effort new examination procedures and processes may necessitate. The OCC is prepared to work with banks to minimize that burden when possible while ensuring bank management and staff members have an appropriate level of cyber awareness and

banks have appropriate processes and controls in place for their inherent risk profiles and risk tolerances.

3. **Does my bank have to use the Assessment?**

   Banks' use of the Assessment is optional. OCC examiners will not require banks to complete the Assessment. For banks that have completed the Assessment, however, examiners may ask for a copy of the Assessment as they would for any risk self-assessment that banks perform. Banks may use the Assessment or any other framework or process to identify their inherent risk and cybersecurity preparedness.

4. **Do I need to submit my completed Assessment?**

   No. Completion of the Assessment by banks is voluntary, and there is no requirement to submit an Assessment to the OCC. For banks that voluntarily complete the Assessment, in total or in part, or any other cyber risk assessment, however, examiners may ask for a copy as they would for any other risk self-assessment that banks perform.

5. **What can I expect out of my examination?**

   OCC examiners will discuss any observations derived from the Assessment and other examination procedures with bank management. OCC examiners will update the Assessment data during subsequent examinations.

   During examinations, if examiners identify issues or concerns that banks do not meet existing legal requirements or supervisory expectations established through FFIEC or OCC guidance for safe and sound operations, the examiners will inform bank management of the concerns and necessary corrective actions.

6. **What maturity level does my bank need to attain?**

   There is no maturity level expectation for banks. Examiners will discuss observations derived from the Assessment and other examination procedures with bank management. If examiners identify policies or practices that do not meet existing legal requirements or supervisory expectations for safe and sound operations, the examiners will inform bank management of the concerns and necessary corrective actions. Examiners generally will not cite levels of maturity per se as concerns identified for bank management's attention. Also see question 10.

   Declarative statements at the baseline maturity level include legal and regulatory requirements and minimum risk management and control expectations outlined in the *FFIEC Information Technology (IT) Examination Handbook*. Most banks should be capable of achieving the baseline maturity in each domain. When a bank has not achieved a baseline declarative statement or, on a broader scale, has not achieved a baseline maturity in a domain, OCC examiners will discuss the situation with bank management to understand what steps management is taking to implement compensating controls to address cybersecurity risk.

7. **How is the Assessment different from IT audit coverage or other process and control tests and assessments?**

   The Assessment and IT audit serve similar purposes involving sound governance, risk management, and controls. An IT audit program evaluates risk management practices, internal control systems, and compliance with corporate policies concerning IT-related risks. The Assessment is a repeatable process that focuses on cybersecurity preparedness based on a bank's inherent risk. To assist in voluntary completion of the Assessment, bank management may find audits, control tests, and other assessments helpful in deciding which declarative statements apply in their environment.

8. **If the bank identifies weaknesses or areas in need of improvement, should the bank report its remediation plans to the OCC?**

   The OCC always encourages banks to have open dialogue with their examiners regarding self-identified issues. Sharing this information helps the examiners understand banks' self-identified strengths and concerns.

9. **How will examiners address differences between their Assessment results and the bank's results?**

   The examiners will discuss those differences with bank management to understand the basis for the variance.

10. **If examiners identify process or control weaknesses when completing the Assessment, will they cite a matter requiring attention or violation of law?**

    The purpose of citing matters requiring attention or violations of law is to communicate the OCC's concerns with bank practices to banks' boards of directors and management. Matters requiring attention describe practices that deviate from sound governance, internal controls, or risk management principles that have the potential to adversely affect the bank's condition, including its financial performance or risk profile. Matters requiring attention may also be cited for bank practices that are inconsistent with laws and regulations, enforcement actions, supervisory guidance, or conditions imposed in writing in connection with the approval of any application or other request by banks.

    Matters requiring attention address deficient practices, including the lack of practices that could adversely affect banks' condition. While deficient practices may result in an adverse condition, banks normally will not be able to remedy the adverse condition unless they address the deficient practices.

    Neither matters requiring attention nor violations of law are cited solely because banks do not achieve a particular declarative statement or maturity level. Because the baseline declarative statements are aligned with existing laws, regulations, and regulatory guidance, however, failure to achieve baseline maturity could indicate concerns warranting matters requiring attention or indicate violations of law have occurred.

11. **How should I account for activities conducted by third-party service providers?**

    Bank management may consider declarative statements in all domains that are attained by a third-party service provider on the bank's behalf. For example, in Domain 3, statements[2] involving a system development life cycle may be attained by the bank's third-party service provider, if the bank outsources secure coding. Domain 4 provides a structure for bank management to evaluate the bank's third-party oversight if management so chooses.

    During examinations of supervised technology service providers, OCC examiners will assess the risk management and control principles communicated in the Assessment.

12. **What if I have other questions on the Assessment?**

    The FFIEC Cybersecurity Assessment Tool web page [http://www.ffiec.gov/cyberassessmenttool.htm] includes the Assessment as well as the following supplemental materials:

    - 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, bank management is encouraged to contact the bank's examiner or portfolio manager with any questions or feedback regarding the Assessment.

[2] D3.PC.SC.B.1: "Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards." D3.PC.SC.E.1: "Security testing occurs at all post-design phases of the SDLC for all applications, including mobile applications."