FFIEC Releases Cybersecurity Assessment Tool

By David G. Ries, Thomas A. Brooks / Jul 09, 2015

On June 30, the Federal Financial Institutions Examination Council (FFIEC) released its Cybersecurity Assessment Tool (Assessment Tool) for financial institutions to use in measuring their cybersecurity readiness. The FFIEC developed the Assessment Tool "[i]n light of the increasing volume and sophistication of cyber threats ... to help institutions identify their risks and determine their cybersecurity preparedness." The Assessment "provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time."

While it is described as optional - at least for now - the Assessment will be a very helpful resource for covered institutions. First, it provides an overview of what the FFIEC and its members expect in a cybersecurity program, along with steps for identifying risks and measuring preparedness to manage them. In addition, it will assist in preparing for successful examinations since it is likely to become the roadmap for examiners in their review of cybersecurity risk and preparedness. Third, it can help to demonstrate compliance and "reasonable security" in the event of a security incident or data breach. The Office of the Comptroller of the Currency (OCC) has announced that it will "gradually incorporate the Assessment into examinations" of institutions the OCC regulates.

The Assessment has two parts. Part One - Inherent Risk Profile - measures the institution's risk profile in five areas: (1) Technologies and Connection Types, (2) Delivery Channels, (3) Online/Mobile Products and Technology Services, (4) Organizational Characteristics, and (5) External Threats. For each area, the institution's management assigns a risk profile across a range of Inherent Risk: Least, Minimal, Moderate, Significant, or Most.

Part Two - Cybersecurity Maturity - measures an institution's preparedness to manage the identified risks, i.e., its cybersecurity maturity. It includes five domains: (1) Cyber Risk Management and Oversight, (2) Threat Intelligence and Collaboration, (3) Cybersecurity Controls, (4) External Dependence Management, and (5) Cyber Incident Management and Resilience. For each category, the institution's management assesses a level of preparedness (maturity level), from a range of levels: Baseline, Evolving, Intermediate, Advanced, or Innovative.

Based on the results of Parts One and Two, the institution's management then reviews its inherent risk profile and cybersecurity maturity level for each domain and determines whether the maturity level is appropriate in light of the risk. If it is not appropriate for any category, management should take steps to reduce the risks, increase preparedness, or both. The Assessment Tool states that the "results should be communicated to the chief executive officer (CEO) and board."

The FFIEC notes that 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," including "when introducing new products and services..."

The Assessment Tool is 59 pages long, including a User's Guide. It provides an assessment process rather than an automated methodology. FFIEC has also prepared an Overview for Chief Executive Officers and Boards of Directors, which it recommends as the first step in the process. In addition to laying out directions for completing the Assessment and interpreting and analyzing results, it includes three appendices:

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

Appendix A maps the Assessment's baseline maturity levels to the risk management and control expectations in the FFIEC Information Technology Examination Handbook. Appendix B provides a mapping of the Assessment to the National Institute of Standards and Technology's (NIST) 2014 Cybersecurity Framework that provides standards, guidelines, and practices for all critical infrastructure sectors, including financial services. The Handbook and Framework are both publications that institutions should already be considering in their security programs.

Incorporating the results from the Assessment Tool into a financial institution's existing program to identify its risks and determine its cybersecurity preparedness can be a complex and daunting task. The federal financial institution regulators will examine the institution to determine how effectively it has used the Assessment Tool. If the regulator determines that an institution's compliance with minimally required elements to protect against cyber risks is lacking, the institution could be subject to an enforcement action. Clark Hill attorneys have substantial experience in working with financial institution regulators and have developed an interdisciplinary team to assist financial institutions in preparing cybersecurity programs.

To connect with our Cybersecurity, Data Protection and Privacy Team, contact Tommy Brooks at 202.552.2356, tbrooks@clarkhill.com or Dave Ries at 412.394.7787, dries@clarkhill.com or another member of the Team.