ICBA
Independent Community Bankers of America®
www.icba.org

ICBA Summary of FFIEC Cybersecurity Assessment Tool (May 2017 Update)

June 2017

Contact Information:
Jeremy Dalpiaz
AVP, Cyber and Data Security Policy
Jeremy.Dalpiaz@icba.org

ICBA Summary of FFIEC Cybersecurity Assessment Tool Update (May 2017)

BACKGROUND

On June 30, 2015, the Federal Financial Institution Examinations Council ("FFIEC") published a Cybersecurity Assessment Tool ("Assessment Tool," "Tool" or "CAT") to provide all financial institutions with a repeatable and measureable process to inform management of their institution's risks (Inherent Risk Profile) and cybersecurity preparedness in relation to that risk (Cybersecurity Maturity). If the level of preparedness is not adequate, the institution may take action either to reduce the level of risk or to increase the levels of maturity (a "target" state). This Tool is meant to be used on an enterprise-wide level periodically or as technology changes. The Tool is mapped to both the *FFIEC Information Technology Examination Handbook (FFIEC IT Handbook),* as well as the *National Institute of Standards and Technology (NIST) Cybersecurity Framework*.[1]

In May 2017, the FFIEC updated the CAT to include updated references to the *FFIEC IT Handbook* and update some responses in the Cybersecurity Maturity section.

The FFIEC offers several resources to assist financial institutions with cybersecurity risk assessment and preparedness.

- An executive overview
- A user's guide
- An online presentation
- Appendices mapping the Tool's baseline maturity statements to the *FFIEC IT Handbook,* mapping all maturity statements to the *NIST Cybersecurity Framework*
- Glossary of terms

FFIEC's Cybersecurity Assessment Tool website

May 2017 FFIEC CAT Update

The May 2017 update to the CAT did not include any changes in the Inherent Risk Profile. The mappings in Appendix A were updated to reflect recent changes to the FFIEC IT Handbook. This was a change sought by ICBA.

In the Cybersecurity Maturity section, rather than the binary "yes" or "no" responses in the previous version, banks may now select between, "yes," "no" and "yes – with compensating controls". The addition of the "yes – with compensating controls" response is a welcomed change to the CAT; one that ICBA and member banks strongly advocated for before the FFIEC. Additionally, a combination of "yes" or "yes- with compensating controls" being selected in any one domain level will qualify as meeting that level of maturity. Like the previous version, if "no" is indicated anywhere within a particular level, that level will not be considered met.

[1] National Institute of Standards and Technology (NIST). 12 February 2014. "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0. Available on the NIST Cybersecurity Framework website.

CYBERSECURITY ASSESSMENT TOOL DETAILS

There are two parts to the Assessment Tool. First, the institution performs an inherent risk profile which portrays the institution's risk based on several categories. Second, the institution determines the cybersecurity maturity (i.e. preparedness) level within five different domains and underlying assessment factors. The result will be an evaluation of the institution's preparedness in relation to its risk for each of the five domains, which can be scaled up or down depending on the institution's desired level of preparedness. At a minimum, institutions should be able to meet the basic level of cybersecurity maturity as this particular level reflects what is currently required by the *FFIEC IT Handbook* and the *NIST Cybersecurity Framework*. Appendix A of the Tool illustrates how the baseline maturity levels and domains correspond to the *FFIEC IT Handbook*. Appendix B maps the Tool to the *NIST Cybersecurity Framework.*

Part I, the "Inherent Risk Profile," identifies activities, services, and products organized in categories with a brief description of what is included in each category. The institution selects the most appropriate risk level (least, minimal, moderate, significant and most) for each activity, service or product. Following this part of the exercise, the institution will then tally up its results to determine its risk profile. For instance, a very small institution will likely be in the least-moderate inherent risk categories. Larger institutions will likely be in the two higher categories of risk.

Below are the categories evaluated in the risk profile:

- *Technologies and Connection Types* – It is inevitable that some connections are riskier than others. Accordingly, this category asks institutions to evaluate the number of Internet Service Providers (ISPs) connections, unsecured external connections, wireless network access, whether personal devices are allowed to connect to the corporate network and an evaluation of third party connections, including the number of organizations and number of individuals with access to internal systems and externally-hosted cloud computing services.
- *Delivery Channels* – This category asks institutions to evaluate their online presence (i.e. whether the institution has a website, social media, online banking, etc.), mobile presence and the extent of ATM operations.
- *Online/Mobile Products and Technology Services* – This category reviews the volume of credit, debit and prepaid cards issued; types of emerging payments technologies offered; whether the organization offers: peer-to-peer payments (and the monthly transaction volume), the origination of ACH payments, wholesale payments, wire transfers, merchant remote deposit capture, global remittances, Treasury services and clients, trust services and correspondent bank services; whether the institution is a merchant acquirer or if it hosts IT services for another organization.
- *Organizational Characteristics* – This category focuses on how the institution is organized, including whether any mergers and acquisitions have occurred or are planned, the number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged, any changes in the IT environment, the number of network administrators (internal and external), and the locations of branches/business presence and operations/data centers.
- *External Threats* – Volume and types of attacks (successful or attempted) – This category focuses exclusively on the sophistication and volume of attempted cyberattacks.

Part I: Risk Levels – For each of the categories above, there is a risk level that the institution can choose based on descriptions provided in the Tool. For instance, in reviewing External Threats, institutions are given five risk levels to choose from, which are defined for each category. The table below illustrates the various risk levels.

Category: External Threats	Risk Levels				
	Least	**Minimal**	**Moderate**	**Significant**	**Most**
Attempted cyber attacks	No attempted attacks or reconnaissance.	Few attempts monthly (<100); may have had generic phishing campaigns by employees and customers.	Several attempts monthly (101-500); phishing campaigns targeting employees or customers at the institution or third parties supporting critical activities; may have experienced an attempted Distributed Denial of Service (DDoS) attack within the last year.	Significant number of attempts monthly (501-100,000); spear phishing campaigns targeting high net worth customers and employees at the institution or third parties supporting critical activities; Institution specifically is named in threat reports; may have experienced multiple DDoS attacks within the last year.	Substantial number of attempts monthly (> 100,000); persistent attempts to attack senior management and/or network administrators; frequently targeted for DDoS attacks.

After reviewing each category and the various statements, the institutions will tally the risk columns. The column with the most responses will result in the Inherent Risk Profile.

- Least Inherent Risk: These types of institutions have limited use of technology; zero connections; products and services are limited; and a small footprint and few employees.
- Minimal Inherent Risk: Institutions within this category have limited variety of less risky products/services; mission-critical systems are outsourced; use established technologies; and maintain few types of connections with limited complexity.
- Moderate Inherent Risk: These institutions use somewhat complex technology in terms of volume and sophistication; may outsource mission-critical systems; have a greater variety of products and services offered through diverse channels.
- Significant Inherent Risk: These types of institutions use complex technology; offer high-risk products/services that may include emerging technologies; may host significant number of applications internally; have a substantial number of connections to customers and third parties; offer a variety of payments directly or through a third party; and may have significant volume.
- Most Inherent Risk: These institutions use extremely complex technologies to deliver a myriad of products and services which may be at highest level of risk, including being offered to other organizations; new and emerging technologies are used across multiple delivery channels; outsource some mission critical systems of applications but most are hosted internally; and maintain a large number of connections.

In addition to the cumulative total, institutions may also wish to tally the risk columns for each category in order to fully understand which categories may pose additional risks for the institution.

Part II: Cybersecurity Maturity Level - Following the Risk Profile, institutions will next determine their cybersecurity maturity level by reviewing each domain (or section) and the assessment factors and components identified for each domain. 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.

In order to be considered at a particular maturity level, <u>all</u> declarative statements for that level must be selected. For instance, to be considered at the Baseline level for Domain 1, Governance, the institution must be able to affirmatively respond to all declarative statements within that level. If the institution moves on to the next level, Evolving, and can only answer three of four declarative statements affirmatively, it does not meet the Evolving level. Below are the domains (or sections) and their respective assessment factors:

- *Domain 1: Cyber Risk Management and Oversight* – This domain addresses the Board of Directors' 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, IT asset management to implement 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 the knowledge and experience commensurate with the institution's risk profile.
        - Training and Culture includes employee training and customer awareness programs contributing to an organizational culture that emphasizes mitigation of cybersecurity threats.

- *Domain 2: Threat Intelligence and Collaboration* – This domain 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 is performed to identify threats specific to the institution and 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* – This domain includes 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, such as infrastructure management, access management, device and end-point security and secure coding, deter and prevent cyber-attacks.
        - Detective Controls, such as threat and vulnerability detection, anomalous activity detection, 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* –This domain involves establishing and maintaining a comprehensive program to oversee and manage external connections and third party relationships with access to an 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* –This domain includes establishing 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 and Strategy incorporates resilience planning and testing into existing business continuity and disaster recovery plans to minimize service disruption and 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.
- Escalating & Reporting ensures key stakeholders are informed about cyber incidents and regulators, law enforcement, and customers are notified as required.

Part II: Maturity Levels – To determine maturity levels, institutions will select a set of declarative statements that describes their behaviors in the various assessment factors (i.e. for Domain 1, this is governance, risk management, resources, and training and culture). This will result in the institutions assigning one of five baselines, shown below, in order of least to most mature for each domain.

- Baseline – Characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed the evaluated guidance.
- Evolving – 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 the protection of customer information and incorporates information assets and systems.
- Intermediate – Characterized by detailed, formal processes. Controls are validated and consistent. Risk management practices and analysis are integrated into business strategies.
- Advanced – Characterized by cybersecurity practices and analytics that are integrated across the lines of business. The majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline business is formally assigned.
- Innovation – Characterized by driving innovation in people, processes, and technology for the bank 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.

In responding to the declarative statements, banks have the option of selecting between three answers:

- Yes;
- Yes – with compensating controls; or
- No.

In the previous CAT version, a bank had to respond “yes” to all statements within a category level to achieve that level (i.e. Domain 1: Governance: Oversight: Baseline – yes would need to be answered to all five statements in order to meet the requirements of the baseline level. To meet the Evolving level, all statements in the Baseline level would need affirmative responses as well as affirmative responses to the four statements in the Evolving category). In this updated version, however, banks have the option of selecting a new response, “yes-with compensating controls.” A compensating control is defined within the Assessment as “a management, operational, and/or technical control (e.g. safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate or high baselines that provides equivalent or comparable protection for an information system”.

Consistent with the previous version, all declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain’s maturity level. Under the new version, however, attained an sustained requires affirmative response to either “yes” or “yes-with compensating controls” for each of the declarative questions within a maturity level.

Interpreting and Analyzing the Assessment Results: Generally speaking, as the risk profile increases, so should the institution’s maturity level. If the maturity level does not meet the inherit risk profile, management should consider 1) reducing the risk profile or 2) developing a strategy to improve maturity levels.