Interpreting the FFIEC Cybersecurity Assessment Tool

Wayne H. Trout, CISA, CRISC, CBCA, CBRA, CBRITP
NCUA Supervisor,
Critical Infrastructure and Cybersecurity
What We’ll Cover

• Cyber risk management
• Cybersecurity Assessment Tool
  – Inherent risk profile
  – Cybersecurity maturity
• Interpret and analyze results
• Issues & FAQs
Primary Objective: help institutions identify their risks and determine their cybersecurity maturity

Emphasis: cybersecurity risk management concepts

Assessment: provides institutions with a repeatable and measureable process to inform management of their institution’s risks and cybersecurity preparedness.

Interpret and analyze results: Gap analysis
Cyber Risk Management

- Enterprise-wide
- Identifies policies, procedures, processes, and controls
- Develop action plan following gap analysis
Cybersecurity Assessment Tool

Inherent Risk Profile

Cybersecurity Maturity
Inherent risk

The amount of risk a credit union’s activities and connections pose, notwithstanding any controls in place to mitigate risk.
Inherent risk profile

Type, volume, and complexity of operations and threats directed at the institution
Inherent Risk Levels

- Most Risk
- Significant Risk
- Moderate Risk
- Minimal Risk
- Least Risk
<table>
<thead>
<tr>
<th>Category: Technologies and Connection Types</th>
<th>Least</th>
<th>Minimal</th>
<th>Moderate</th>
<th>Significant</th>
<th>Most</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of internet service provider (ISP) connections (including branch connections)</td>
<td>No connections</td>
<td>Minimal complexity (1–20 connections)</td>
<td>Moderate complexity (21–100 connections)</td>
<td>Significant complexity (101–200 connections)</td>
<td>Substantial complexity (&gt;200 connections)</td>
</tr>
<tr>
<td>Unsecured external connections, number of connections not users (e.g., file transfer prototype (FTP), Telnet, rlogin)</td>
<td>None</td>
<td>Few instances of unsecured connections (1–5)</td>
<td>Several instances of unsecured connections (6–10)</td>
<td>Significant instances of unsecured connections (11–25)</td>
<td>Substantial instances of unsecured connections (&gt;25)</td>
</tr>
</tbody>
</table>
## Example: Inherent Risk Excerpt

### Category: Technologies and Connection Types

<table>
<thead>
<tr>
<th>Risk Levels</th>
<th>Least</th>
<th>Minimal</th>
<th>Moderate</th>
<th>Significant</th>
<th>Most</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wireless network access</strong></td>
<td>No wireless access</td>
<td>Separate access points for guest wireless and corporate wireless</td>
<td>Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)</td>
<td>Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)</td>
<td>Wireless corporate network access; all employees have access; substantial number of access points (&gt;1,000 users; &gt;100 access points)</td>
</tr>
<tr>
<td><strong>Personal devices allowed to connect to the corporate network</strong></td>
<td>None</td>
<td>Only one device type available; available to &lt;5% of employees (staff, executives, managers); e-mail access only</td>
<td>Multiple device types used; available to &lt;10% of employees (staff, executives, managers) and board; e-mail access only</td>
<td>Multiple device types used; available to &lt;25% of authorized employees (staff, executives, managers) and board; e-mail and some applications accessed</td>
<td>Any device type used; available to &gt;25% of employees (staff, executives, managers) and board; all applications accessed</td>
</tr>
</tbody>
</table>

### Category: Delivery Channels

<table>
<thead>
<tr>
<th>Risk Levels</th>
<th>Least</th>
<th>Minimal</th>
<th>Moderate</th>
<th>Significant</th>
<th>Most</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online presence (customer)</strong></td>
<td>No Web-facing applications or social media presence</td>
<td>Serves as an informational Web site or social media page (e.g., provides branch and ATM locations and marketing materials)</td>
<td>Serves as a delivery channel for retail online banking; may communicate to customers through social media</td>
<td>Serves as a delivery channel for wholesale customers; may include retail account origination</td>
<td>Internet applications serve as a channel to wholesale customers to manage large value assets</td>
</tr>
<tr>
<td><strong>Mobile presence</strong></td>
<td>None</td>
<td>SMS text alerts or notices only; browser-based access</td>
<td>Mobile banking application for retail customers (e.g., bill payment, mobile check capture, internal transfers only)</td>
<td>Mobile banking application includes external transfers (e.g., for corporate clients, recurring external transactions)</td>
<td>Full functionality, including originating new transactions (e.g., ACH, wire)</td>
</tr>
<tr>
<td><strong>Automated Teller Machines (ATM) (Operation)</strong></td>
<td>No ATM services</td>
<td>ATM services offered but no owned machines</td>
<td>ATM services managed by a third party; ATMs at local and regional branches; cash reload services outsourced</td>
<td>ATM services managed internally; ATMs at U.S. branches and retail locations; cash reload services outsourced</td>
<td>ATM services managed internally; ATM services provided to other financial institutions; ATMs at domestic and international branches and retail locations; cash reload services managed internally</td>
</tr>
</tbody>
</table>
Inherent Risk Levels

- Parameters, not rigid rules
- Select higher risk level if assessment indicates level is between two levels
- Do not factor in mitigating controls when assigning risk levels
Considerations

• Gathering and validating information
• Interacting with management, the board, or committees
• Previously completed risk profile status
Cybersecurity Maturity 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
Cybersecurity Maturity Levels

Interpreting the FFIEC Cybersecurity Assessment Tool
## Domain 3: Cybersecurity Controls

### Assessment Factor: Preventative Controls

<table>
<thead>
<tr>
<th>Y, N</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

#### Baseline

Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards. ([FFIEC Information Security Booklet, page 56](#))

The security controls of internally developed software are periodically reviewed and tested. (*N/A if there is no software development.*) ([FFIEC Information Security Booklet, page 59](#))

The security controls in internally developed software code are independently reviewed before migrating the code to production. (*N/A if there is no software development.*) ([FFIEC Development and Acquisition Booklet, page 2](#))

Intellectual property and production code are held in escrow. (*N/A if there is no production code to hold in escrow.*) ([FFIEC Development and Acquisition Booklet, page 39](#))

#### Evolving

Security testing occurs at all post-design phases of the SDLC for all applications, including mobile applications. (*N/A if there is no software development.)*

#### Intermediate

Processes are in place to mitigate vulnerabilities identified as part of the secure development of systems and applications.

The security of applications, including Web-based applications connected to the Internet, is tested against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes.
## Domain - Maturity Levels

### Domain 3: Cybersecurity Controls

#### Assessment Factor: Preventative Controls

<table>
<thead>
<tr>
<th>Y, N</th>
<th>Baseline</th>
<th>Evolving</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The institution is able to detect anomalous activities through monitoring across the environment. (<a href="#">FFIEC Information Security Booklet, page 32</a>)</td>
<td>Systems are in place to detect anomalous behavior automatically during customer, employee, and third-party authentication.</td>
</tr>
<tr>
<td></td>
<td>Customer transactions generating anomalous activity alerts are monitored and reviewed. (<a href="#">FFIEC Wholesale Payments Booklet, page 12</a>)</td>
<td>Security logs are reviewed regularly.</td>
</tr>
<tr>
<td></td>
<td>Logs of physical and/or logical access are reviewed following events. (<a href="#">FFIEC Information Security Booklet, page 73</a>)</td>
<td>Logs provide traceability for all system access by individual users.</td>
</tr>
<tr>
<td></td>
<td>Access to critical systems by third parties is monitored for unauthorized or unusual activity. (<a href="#">FFIEC Outsourcing Booklet, page 26</a>)</td>
<td>Thresholds have been established to determine activity within logs that would warrant management response.</td>
</tr>
<tr>
<td></td>
<td>Elevated privileges are monitored. (<a href="#">FFIEC Information Security Booklet, page 19</a>)</td>
<td></td>
</tr>
</tbody>
</table>

---

Interpreting the FFIEC Cybersecurity Assessment Tool
## Domain 3: Cybersecurity Controls

### Assessment Factor: Preventative Controls

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intermediate</td>
<td>Online customer transactions are actively monitored for anomalous behavior. Tools to detect unauthorized data mining are used. Tools actively monitor security logs for anomalous behavior and alert within established parameters. Audit logs are backed up to a centralized log server or media that is difficult to alter. Thresholds for security logging are evaluated periodically. Anomalous activity and other network and system alerts are correlated across business units to detect and prevent multifaceted attacks (e.g., simultaneous account takeover and DDoS attack).</td>
</tr>
<tr>
<td>Advanced</td>
<td>An automated tool triggers system and/or fraud alerts when customer logins occur within a short period of time but from physically distant IP locations. External transfers from customer accounts generate alerts and require review and authorization if anomalous behavior is detected. A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities. An automated tool(s) is in place to detect and prevent data mining by insider threats. Tags on fictitious confidential data or files are used to provide advanced alerts of potential malicious activity when the data is accessed.</td>
</tr>
</tbody>
</table>
INTERPRET AND ANALYZE RESULTS
Interpreting the FFIEC Cybersecurity Assessment Tool

<table>
<thead>
<tr>
<th>Cybersecurity Maturity Level for Each Domain</th>
<th>Inherent Risk Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innovative</td>
<td>Elevated</td>
</tr>
<tr>
<td>Advanced</td>
<td>Investment</td>
</tr>
<tr>
<td>Intermediate</td>
<td></td>
</tr>
<tr>
<td>Evolving</td>
<td></td>
</tr>
<tr>
<td>Baseline</td>
<td>Underinvestment</td>
</tr>
</tbody>
</table>
Addressing Misalignments

- Determine target maturity levels
- Conduct gap analysis
- Prioritize and plan actions
- Implement changes
- Reevaluate
- Communicate results
Read declarative statements to find policies, processes, procedures and controls that can be adopted for use by the credit union to increase cybersecurity preparedness.
Share Assessment Results

- Meet with CEO and board of directors
- Review assessment results
- Provide additional information
When to Reassess

• Periodically
• Following significant operational or technological changes
• Before new products, services, or initiatives are introduced
Benefits to Credit Unions

• Identify Risk Drivers
• Assess Level of Preparedness
• Identify Misalignments in Risk
• Determine Optimal Enhancements to Align
• Inform Risk Management Strategies
• Understand Risk with Third Parties and Partners
• Measure and Monitor Progress
• Connect Strategic with Operational Functions
ISSUES & FAQS
CAT Issue: Limited Resources to Implement

• Tailor use of the tool to size and complexity
• Can be implemented in stages and over time
• Start with the Baseline
• Target higher maturity levels in some Domains, Assessment Factors, or Components than others
• Can weight the results, factor in compensating controls, customize a scoring system, etc.
• Don’t artificially limit to Baseline
  – Many CUs already operate above the Baseline due to vendor cybersecurity control products
    • i.e. network and online banking security
Do we have to meet all declarative statements in order to move up to the next maturity level?

- Example: If we meet 100% of Baseline, then 80% of Evolving. Can we state that we are in the Evolving maturity level? If so, than do we need to reach 100% on Evolving before moving to Intermediate?

**Answer:** The CAT was designed so that all statements at a maturity level need to be achieved.

- For example, deeming statements as not applicable for the environment (NA), or opting out/accepting risk for some statements.

- Higher maturity levels can be worked on without completing lower levels, but the CAT is designed to be a maturity progression.
CAT Issue: Consulting Your Vendors

- CAT not specifically designed to trigger contact with service providers
- Fully completing the Assessment may necessitate such contact
  - For example, CUs outsourced technical expertise to Managed Security Service Providers
- Service provider contact can improve management’s oversight of the third party relationship/service
- CUs should expect to find vendor controls and practices commensurate to those in the CAT
Some Applicable CAT Statements
• Risk-based due diligence is performed (Baseline)
• Board reviews due diligence when 3rd party affects risk profile (Evolving)
• Audits of high-risk vendors are conducted on an annual basis (Advanced)

Other Key Considerations
— Does the vendor store PII?
— SOC 2 Type II performed?
— Private or public cloud?
— Offshore or U.S based?

• Remember, for the IRP we are measuring inherent rather than residual risk
CAT Issue: Alternative Frameworks

• The CAT is voluntary and CUs can use other frameworks to assess cybersecurity preparedness

• However, the CAT is customized to our industry and draws from numerous sources such as:
  – Existing regulations and regulatory guidance
  – The FFIEC IT Handbooks
  – NIST Cybersecurity Framework and NIST Special Publication 800-53
  – U.K. Prudential Regulation Authority 2014 cybersecurity assessment
  – Canada’s Office of Superintendent of Financial Institutions 2013 cybersecurity assessment
  – Department of Energy’s Cybersecurity Capability Maturity Model Program

• And others, as the CAT was designed to provide considerable benefit and efficiency to financial institutions
CAT FAQ: Risk Assessment Replacement?

• The CAT is not designed to be a risk assessment
• CAT does not replace risk assessment requirement required by GLBA Guidelines
  – Notation of threats to customer information.
• Other areas that require a risk assessment process include:
  – New products or services
  – Vendors
  – Business continuity planning
CAT FAQ: Risk Assessment Replacement?

Does the Assessment replace the risk assessment process outlined in the GLBA Guidelines?

• No. The Assessment was designed to complement, not replace, an institution's risk management process and cybersecurity program. Therefore it does not replace the risk assessment of threats to customer information required by the GLBA Guidelines.

• To comply with the GLBA Guidelines, this risk assessment process must:
  – Identify all reasonably foreseeable threats to customer information.
  – Assess the risk (likelihood of occurrence and potential impact).
  – Assess the sufficiency of controls in place to control risks.
CAT FAQ: Recommended IT Audits?

- External vulnerability assessments
- Internal vulnerability assessments
  - Supplement outsourced with internal scanning
- IT general controls audit
- Social engineering testing
  - Phishing
  - Pretext calling
  - Site visits to attempt unauthorized physical access
- Penetration testing at higher maturity levels
QUESTIONS
Contact for Questions

For Credit Unions:
CU_cybersecurity@ncua.gov
Feel free to contact our office with questions or comments.

Primary Staff: Wayne H. Trout, Supv.

email: wtrout@ncua.gov

Office Phone: 703-664-3412
1. FFIEC Cyber Assessment Tool & Supporting Materials
   – https://www.ffiec.gov/cyberassessmenttool.htm

2. FFIEC IT Handbook InfoBase
   – http://ithandbook.ffiec.gov/