SECURE THE VILLAGE

Financial Services Security Forum

FFIEC Cybersecurity Assessment Tool
http://www.ffiec.gov/cyberassessmenttool.htm

Stan Stahl, Ph.D.
President, Secure The Village
July 24, 2015

From the FFIEC

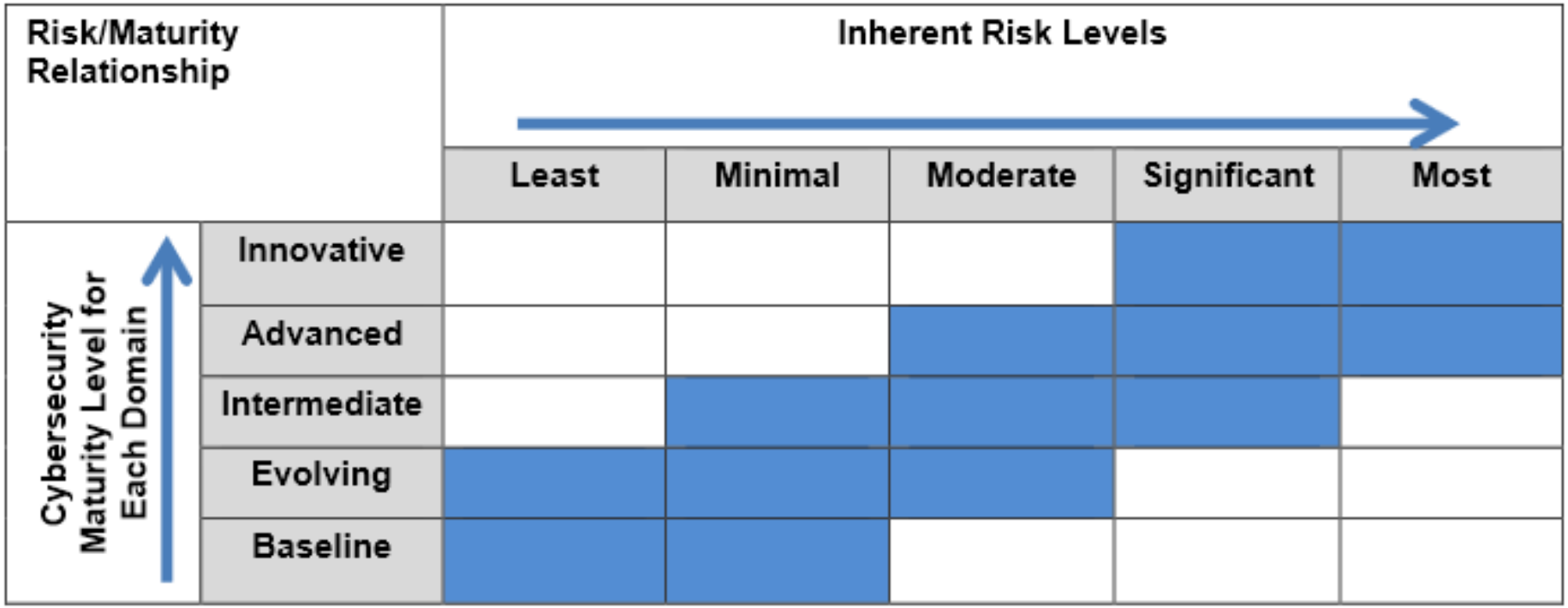
In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (Assessment) to help institutions identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.

The … resources can help management and directors of financial institutions understand supervisory expectations, increase awareness of cybersecurity risks, and assess and mitigate the risks facing their institutions.

When Do Regulators Plan to Start Using the Cybersecurity Assessment Tool?

- FDIC: Plan to discuss the Assessment with institution management during examinations.
  - https://www.fdic.gov/news/news/financial/2015/fil15028.html
- Federal Reserve: Utilize the assessment tool as part of examination process, starting in late 2015 or early 2016.
  - http://www.federalreserve.gov/bankinforeg/srletters/sr1509.htm
- OCC: Begin incorporating the Assessment into examinations in late 2015.
  - http://www.occ.gov/news-issuances/bulletins/2015/bulletin-2015-31.html
- NCUA: Plan to incorporate the tool into cyber exam processes as early as June 2016.
  - http://www.bankinfosecurity.com/interviews/ffiec-issues-cyber-assessment-tool-i-2781

The Risk / Maturity Relationship: Aligning the Pieces



The Cybersecurity Assessment Tool has Three Main Components

- **Inherent Risk Profile**: A risk profile assessment to help institutions understand how each activity, service and product can impact risk and affect inherent risk
- **Cybersecurity Maturity**: An assessment tool to determine an institution's cybersecurity maturity level
- **Users' Guide**: Explains the tool and how it can be used by institutions to interpret and analyze their internal cybersecurity capacity

The Tool Includes Guidance for Use and Understanding

- Overview for CEOs and Boards of Directors
- Appendices
  - Appendix A: Mapping Baseline Statements to FFIEC IT Handbook
  - Appendix B: Mapping how the cybersecurity assessment tool aligns with the NIST Cybersecurity Framework
  - Appendix C: Glossary of common cyber-related terms

Inherent Risk Profile

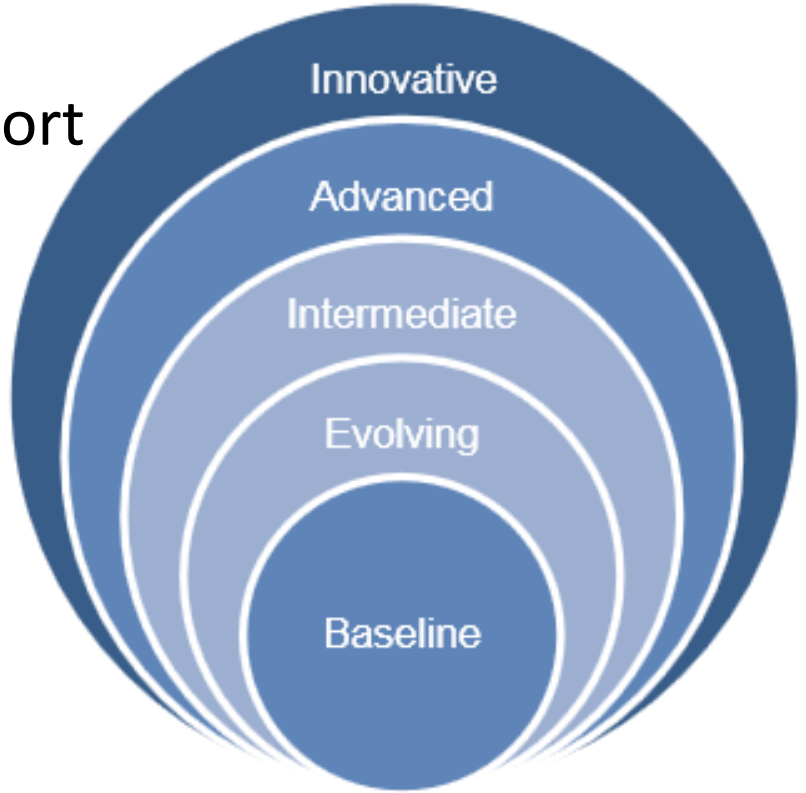
- Cybersecurity inherent risk is the level of risk posed to the institution by the following:
  - Technologies and Connection Types
  - Delivery Channels
  - Online/Mobile Products and Technology Services
  - Organizational Characteristics
  - External Threats
- The profile helps management determine exposure to risk that the institution's activities, services, and products individually and collectively pose to the institution

Example: Inherent Risk Profile Analysis

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)
Personal devices allowed to connect to the corporate network	None	Only one device type available; available to <5% of employees (staff, executives,	Multiple device types used; available to <10% of employees (staff, executives,	Multiple device types used; available to <25% of authorized employees (staff,	Any device type used; available to >25% of employees (staff, executives, managers)

Cybersecurity Maturity

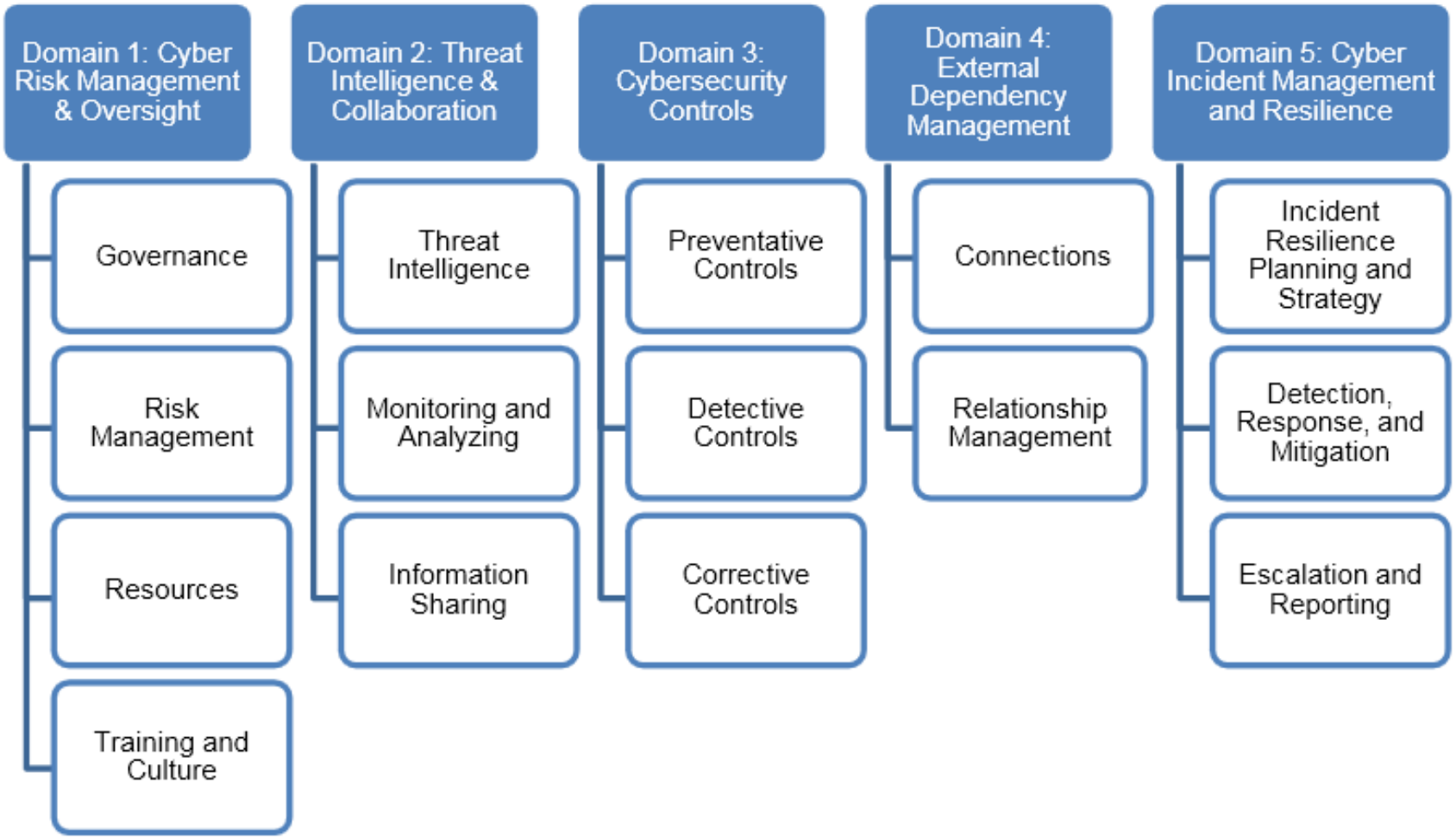
- Extent to which behaviors, practices and processes support cybersecurity preparedness
  - Cyber Risk Management and Oversight
  - Threat Intelligence and Collaboration
  - Cybersecurity Controls
  - External Dependency Management
  - Cyber Incident Management and Resilience



Maturity Levels Defined

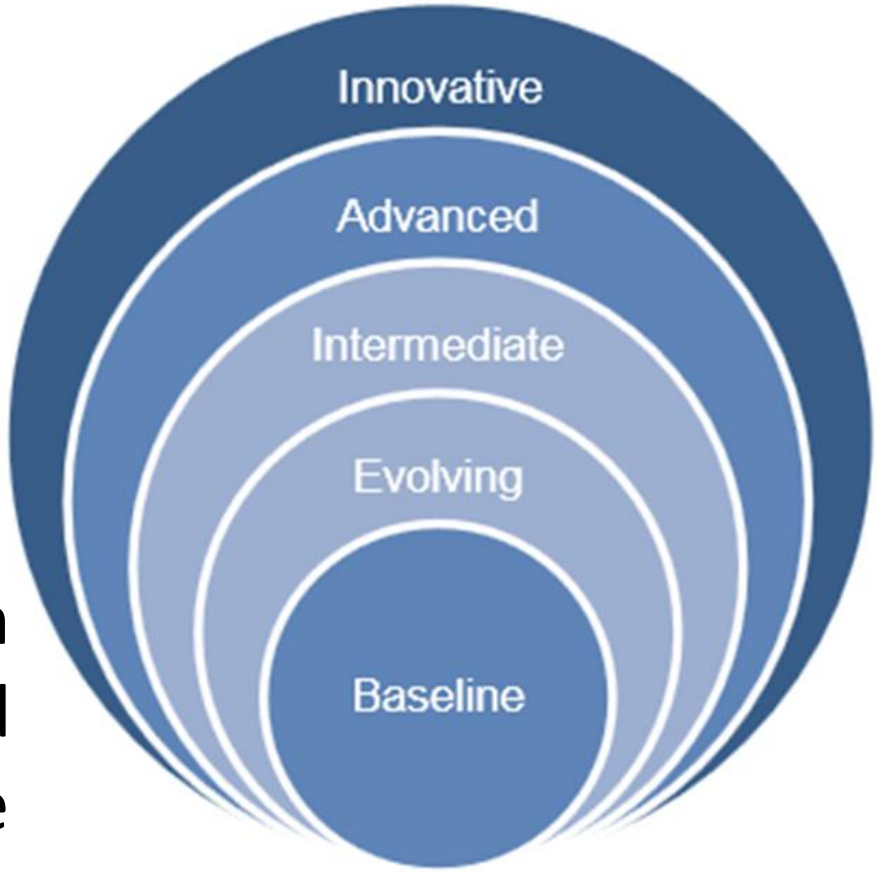
Maturity Levels Defined	
Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized 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 protection of customer information to incorporate information assets and systems.
Intermediate	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
Advanced	Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry 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.

Maturity Assessment Factors for Each of Five Domains

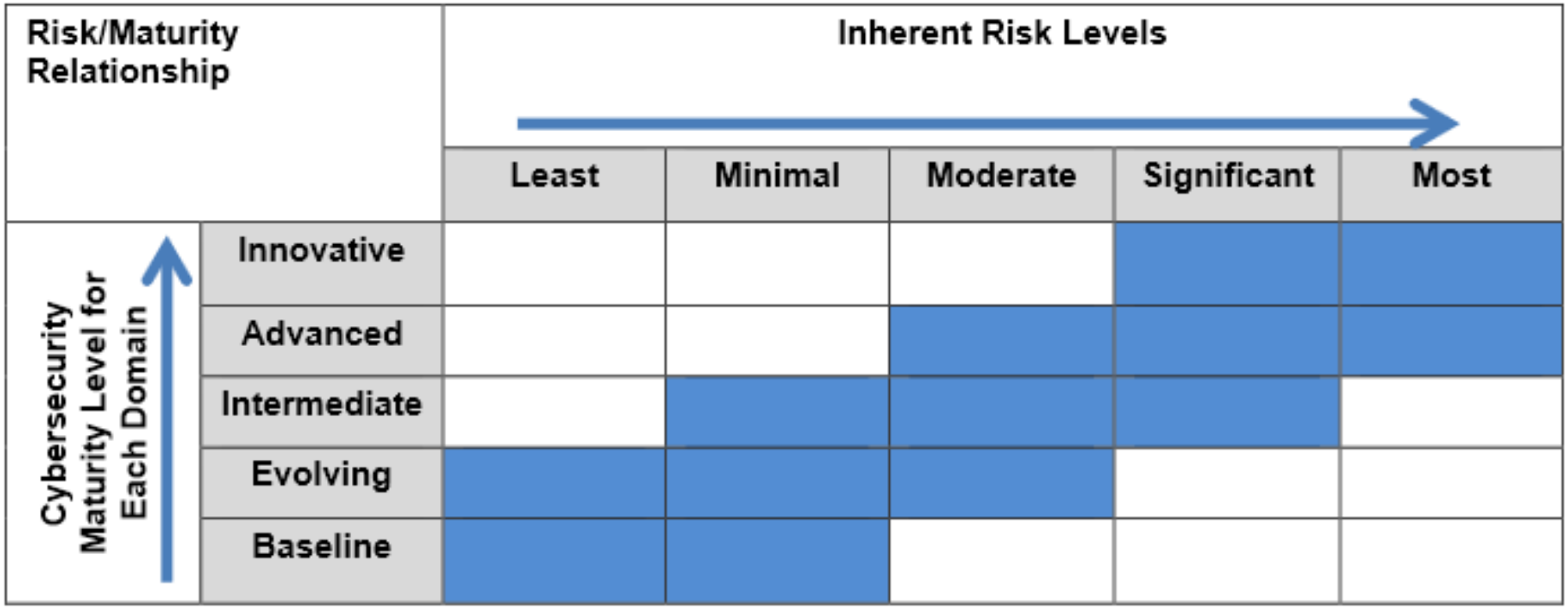


Each Domain Gets Own Maturity Assessment Score

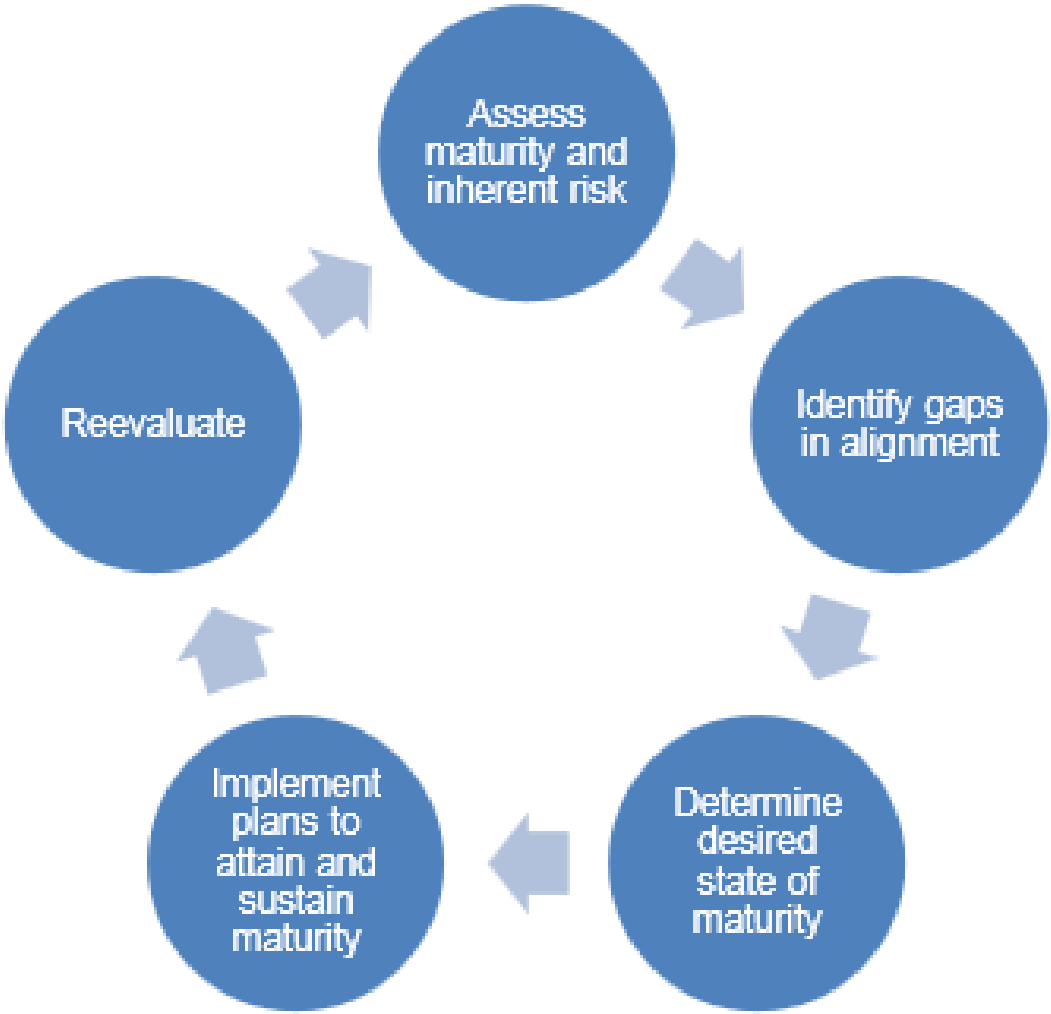
- Tool not designed to provide an overall cybersecurity maturity level
- To achieve a particular maturity level, all declarative statements in each maturity level—and previous levels—must be attained and sustained



The Risk / Maturity Relationship: Aligning the Pieces



Using the Tool as a Planning Vehicle



Cybersecurity Management & Oversight: Questions to Assist Management and the Board

- What are the potential cyber threats to the institution?
- Is the institution a direct target of attacks?
- Is the institution's cybersecurity preparedness receiving the appropriate level of time and attention from management and the board or an appropriate board committee?
- Do the institution's policies and procedures demonstrate management's commitment to sustaining appropriate cybersecurity maturity levels?
- What is the ongoing process for gathering, monitoring, analyzing, and reporting risks?
- Who is accountable for assessing and managing the risks posed by changes to the business strategy or technology?
  - Are the accountable individuals empowered with the authority to carry out these responsibilities?
- Do the inherent risk profile and cybersecurity maturity levels meet management's business and risk management expectations?
  - If there is misalignment, what are the proposed plans to bring them into alignment?
- How can management and the board, or an appropriate board committee, make this process part of the institution's enterprise-wide governance framework?

Inherent Risk Profile: Questions to Assist Management and the Board

- What is the process for gathering and validating the information for the inherent risk profile and cybersecurity maturity?
- How can management and the board, or an appropriate board committee, support improvements to the institution's process for conducting the Assessment?
- What do the results of the Assessment mean to the institution as it looks at its overall risk profile?
- What are the institution's areas of highest inherent risk?
- Is management updating the institution's inherent risk profile to reflect changes in activities, services, and products?

Cybersecurity Maturity: Questions to Assist Management and the Board

- How effective are the institution's risk management activities and controls identified in the Assessment?
- Are there more efficient or effective means for attaining or improving the institution's risk management and controls?
- What third parties does the institution rely on to support critical activities?
- What is the process to oversee third parties and understand their inherent risks and cybersecurity maturity?
- How does management validate the type and volume of attacks?
- Is the institution sharing threat information with peers, law enforcement, and critical third parties through information-sharing procedures?

Financial Services Security Forum

The Financial Services Security Forum is a cross-organizational, cross-functional "learning organization" committed to working together to better protect our community from bank fraud, credit card theft, identity theft and other forms of cyber crime.

Forum Members

- Information security, treasury &risk officers at commercial financial institutions
- Relationship managers &other-customer-centric professionals in the financial services industry
- Law enforcement personnel engaged in financially-related cyber crime

Forum Meetings: 4th Friday of Each Month, 8:00 – 9:30AM

To Register: Stan@SecureTheVillage.org

https://securethevillage.org/fssf/