

Larry Schoeberl, Supervisory Examiner
National Credit Union Administration



FFIEC Cybersecurity Assessment Tool

Michigan CU League & Affiliates
Conference

February 11, 2016

Agenda

- Risk Trends
- FFIEC Cybersecurity Efforts
- Cybersecurity Assessment Tool

Risk Trends

- **Existing vulnerabilities continue to be exploited**

Easily exploitable vulnerabilities persist

- **New platforms create new cyber attack opportunities**

New ways to exploit financial institutions and their customers

- **Lines between cyber actors are blurring**

Commercialization of tools, resources, and infrastructure

Risk Trends

- **Tactics evolve in response to online behavior**

Social networks enable more effective and targeted attacks
- **Trends in malware are evolving**

Destructive malware and cryptographic ransomware
- **Global unrest results in changing motivations**

Regions that either have cyber capabilities or resources to purchase them may turn their focus towards U.S. financial institutions during political and social unrest.

Risk Trends

Potential Impacts

- Financial
- Operational
- Legal
- Reputational

FFIEC CYBERSECURITY EFFORTS



FFIEC Cybersecurity Efforts

- Cybersecurity and Critical Infrastructure Working Group
- Joint statements and alerts
- Cybersecurity awareness website and CEO webinar
- Cybersecurity assessment of community institutions

FFIEC Cybersecurity Efforts

- Issue a Cybersecurity Assessment Tool
- Enhance incident analysis
- Align, update and test crisis management protocols
- Develop training programs for staff
- Update and supplement the *Information Technology Examination Handbook*
- Enhance focus on Technology Service Providers
- Collaborate with law enforcement and intelligence agencies

FFIEC CYBERSECURITY ASSESSMENT TOOL



FFIEC Cybersecurity Assessment Tool

Objective

To help institutions identify their risks and determine their cybersecurity maturity.

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

FFIEC Cybersecurity Assessment Tool

Consistent with the principles in

- *FFIEC Information Technology Examination Handbook (IT Handbook)*
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Industry accepted cybersecurity practices

FFIEC Cybersecurity Assessment Tool

Consists of two parts

Part One: Inherent Risk Profile

Part Two: Cybersecurity Maturity

FFIEC Cybersecurity Assessment Tool

Inherent Risk Profile Categories

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

FFIEC Cybersecurity Assessment Tool

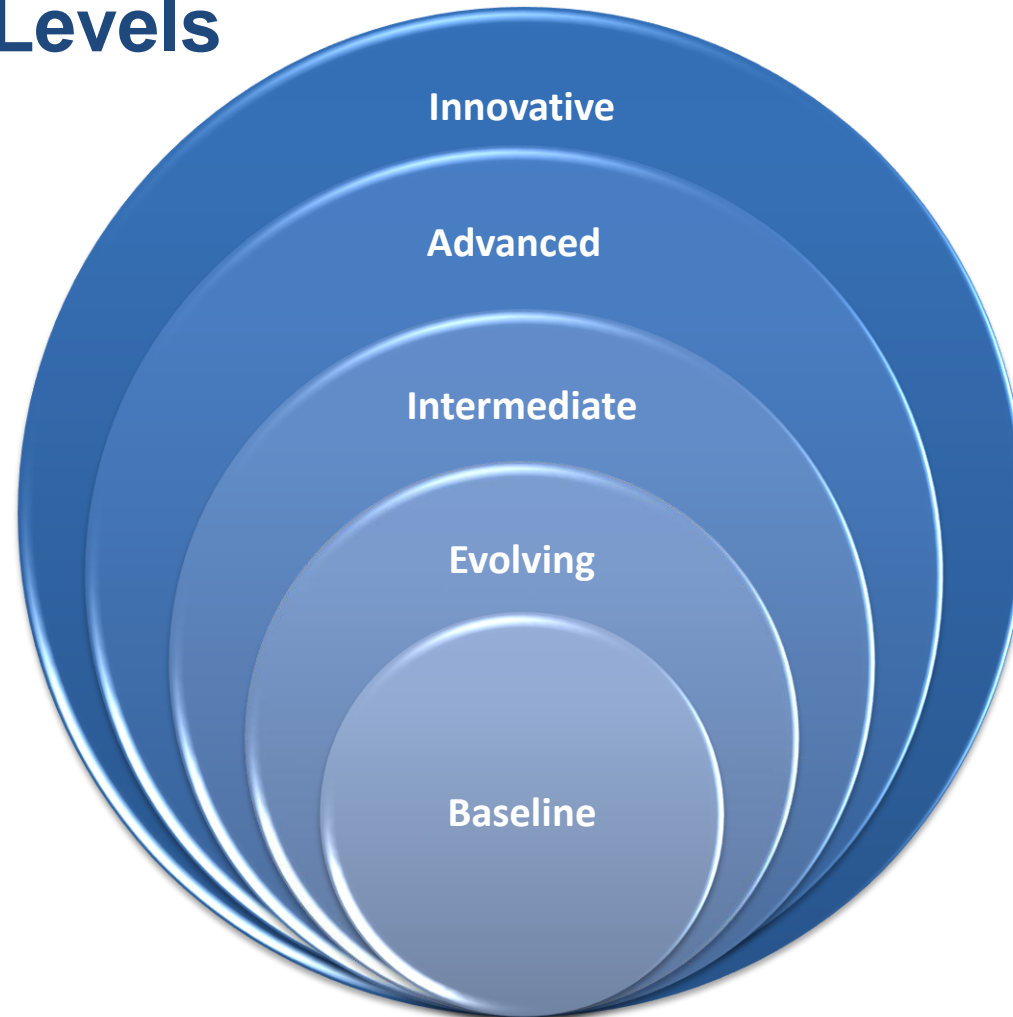
Inherent Risk Profile Risk Levels



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

FFIEC Cybersecurity Assessment Tool

Maturity Levels



FFIEC Cybersecurity Assessment Tool

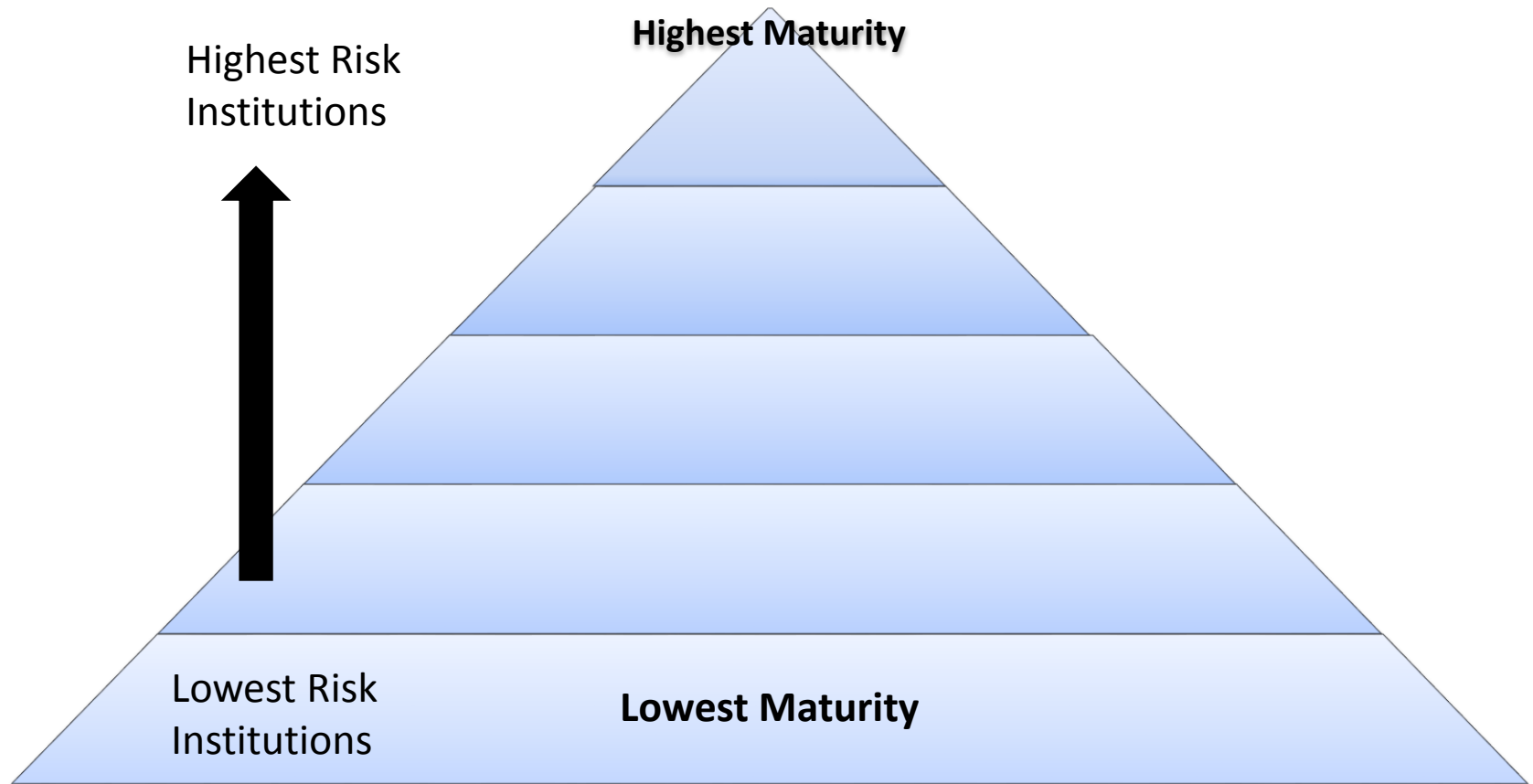
Cybersecurity Domains

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience

FFIEC Cybersecurity Assessment Tool

Domain	Assessment Factors
1 Cyber Risk Management & Oversight	<ul style="list-style-type: none">• Governance• Risk Management• Resources• Training and Culture
2 Threat Intelligence & Collaboration	<ul style="list-style-type: none">• Intelligence Sourcing• Monitoring and Analyzing• Information Sharing
3 Cybersecurity Controls	<ul style="list-style-type: none">• Preventative Controls• Detective Controls• Corrective Controls
4 External Dependency Management	<ul style="list-style-type: none">• Connections• Relationships Management
5 Cyber Incident Management & Resilience	<ul style="list-style-type: none">• Incident Resilience Planning and Strategy• Detection, Response and Mitigation• Escalation and Reporting

Cybersecurity Maturity/Risk Relationship



Patch Management

MATURITY PROGRESSION

INNOVATIVE

ADVANCED

INTERMEDIATE

EVOLVING

BASELINE

- Timely Patching
- Patch Testing
- Missing Patch Report Review

- Formal Program
- Impact Evaluated
- Automated Retrieval
- Missing Patches: Automated Comprehensive Tracking/Prioritization

- High-Risk Patches Tested/Applied or Accountability Assigned

- Comprehensive Patch Software on Servers
- Aggressive Testing & Application (0-30 days)

- Develops Patches, Fixes or Open Source Code.
- Redundant Systems for Testing, Deployment, and Fallback.

FFIEC Cybersecurity Assessment Tool

		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Levels	Innovative	Elevated Investment				
	Advanced					
	Intermediate					
	Evolving					
	Baseline				Underinvestment	

Optimal

Assessment Process

1. Identify Critical Functions & Vendors

2. Complete Inherent Risk Profile

3. Assess Maturity

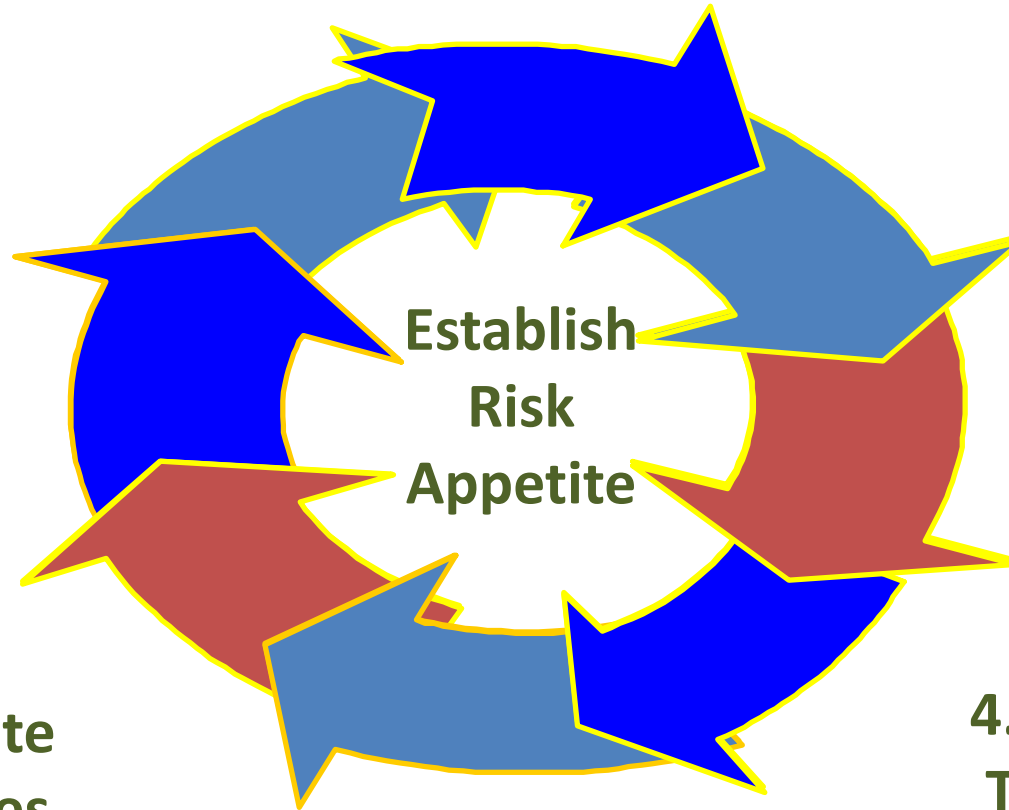
4. Determine Target State

5. Develop Plan to Address Gaps

6. Allocate Resources

7. Adjust Program

Involve
BOD
Throughout



FFIEC Cybersecurity Assessment Tool

Supporting Materials

- User's Guide
- Overview for CEOs and Boards of Directors
- Appendix A: Mapping Baseline Statements to *FFIEC IT Handbook*
- Appendix B: Mapping Cybersecurity Assessment Tool to the NIST Cybersecurity Framework
- Appendix C: Glossary

FFIEC Cybersecurity Assessment Tool

Benefits to Institutions

- Identifying factors contributing to and determining the institution's overall cyber risk.
- Assessing the institution's cybersecurity preparedness.
- Evaluating whether the institution's cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that could be enhanced and actions that could be taken to achieve the institution's desired state of cyber preparedness.
- Informing risk management strategies.

Thanks For Your Time!

Questions/Comments About the Tool

Dedicated NCUA email for your questions:

CU_cybersecurity@ncua.gov

Office Contact Page

Feel free to contact our office with questions or comments.

Presenter Larry Schoeberl
Supervisory Examiner-Detroit
lschoeberl@ncua.gov

Questions Tim Segerson
Deputy E&I Director
segerson@ncua.gov
703-518-6397