



CYBERSECURITY ASSESSMENT

Contents

- Introduction 2
- Definitions 3
 - Risk Levels 3
 - Maturity Levels 4
- Detailed Results 5
 - Inherent Risk Profile 5
 - Cybersecurity Maturity Assessment 7
- Appendix: Additional Resources 14

Introduction

The Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool so that institutions can identify their risks and determine their cybersecurity preparedness level. The assessment consists of two parts that measure a company's preparedness by comparing the organization's risk level against their cybersecurity program's maturity level.

The first part of the assessment identifies the institution's inherent risk using the Inherent Risk Profile. The profile outlines activities, services, and products of the organization and presents descriptions of risks for each item at each of five risk levels. The organization's Overall Inherent Risk Level is determined by the amount of activities, services, and products at each risk level.

The second part of the assessment, known as the Cybersecurity Maturity assessment, is used to determine the institution's maturity level within five major "domains" (or areas of concentration) of the organization's Information Technology/Information Security (IT/IS) programs. Within each domain, "assessment factors" describe specific areas to be evaluated. Each assessment factor is comprised of one or more contributing "components" that contain declarative statements describing an activity that supports the assessment factor at each level of maturity. A maturity level is determined for each component of the assessment and the maturity levels for all components of a domain are used to determine the domain's maturity level.

The FFIEC has provided a maturity matrix by which organizations can compare their risk and maturity levels. The blue section of the maturity matrices in the report below indicate the *generally expected* range in which the FFIEC expects an organization's Cybersecurity maturity level to be based on their Overall Inherent Risk Level.

Target inherent risk and maturity levels are defined by the organization according to the company's self-defined goals for maturing their IT/IS programs. The analysis of results sections of this report outline opportunities for growth so that the organization can mature into their target inherent risk and maturity levels.

Definitions

Risk Levels

- **Least Inherent Risk:** An institution with a Least Inherent Risk Profile generally has very limited use of technology. It has few computers, applications, systems, and no connections. The variety of products and services are limited. The institution has a small geographic footprint and few employees.
- **Minimal Inherent Risk:** An institution with a Minimal Inherent Risk Profile generally has limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services. The institution's mission-critical systems are outsourced. The institution primarily uses established technologies. It maintains a few types of connections to customers and third parties with limited complexity.
- **Moderate Inherent Risk:** An institution with a Moderate Inherent Risk Profile generally uses technology that may be somewhat complex in terms of volume and sophistication. The institution may outsource mission-critical systems and applications and may support elements internally. There is a greater variety of products and services offered through diverse channels.
- **Significant Inherent Risk:** An institution with a Significant Inherent Risk Profile generally uses complex technology in terms of scope and sophistication. The institution offers high risk products and services that may include emerging technologies. The institution may host a significant number of applications internally. The institution allows either a large number of personal devices or a large variety of device types. The institution maintains a substantial number of connections to customers and third parties. A variety of payment services are offered directly rather than through a third party and may reflect a significant level of transaction volume.
- **Most Inherent Risk:** An institution with a Most Inherent Risk Profile uses extremely complex technologies to deliver myriad products and services. Many of the products and services are at the highest level of risk, including those offered to other organizations. New and emerging technologies are utilized across multiple delivery channels. The institution may outsource some mission-critical systems or applications, but many are hosted internally. The institution maintains a large number of connection types to transfer data with customers and third parties.

Maturity Levels

- **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.

Detailed Results

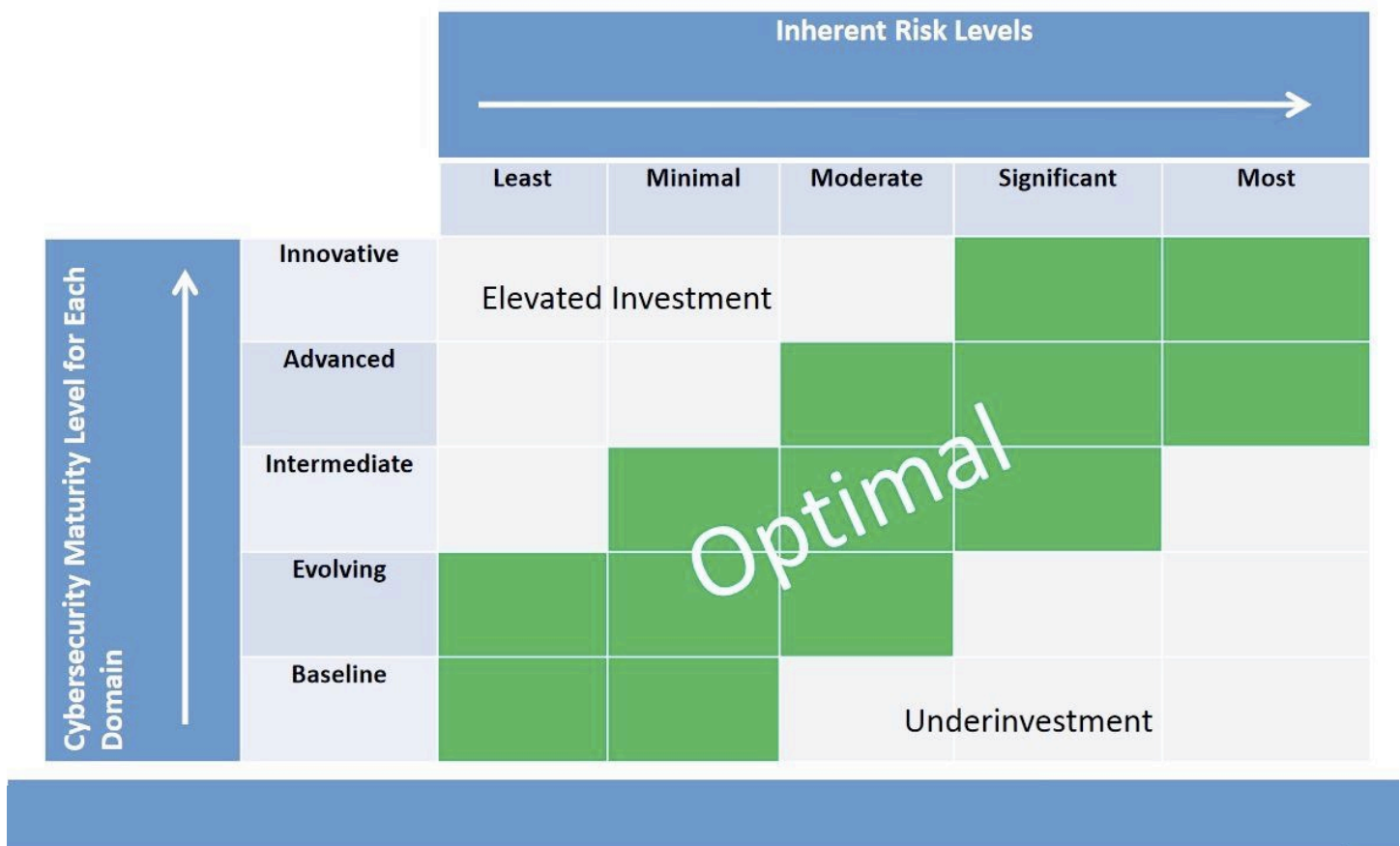
Inherent Risk Profile

INHERENT RISK LEVEL	NUMBER OF ANSWERS
Least	19
Minimal	12
Moderate	7
Significant	1
Most	0
Total	39

*Overall Inherent Risk Level: **Minimal***

Understanding the Charts

Management can review the institution's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain to understand whether they are aligned. The following table depicts the relationship between an institution's Inherent Risk Profile and its domain Maturity Levels, as there is no single expected level for an institution. In general, as inherent risk rises, an institution's maturity levels should increase. An institution's inherent risk profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change. Thus, management should consider reevaluating the institution's inherent risk profile and cybersecurity maturity periodically and when planned changes can affect its inherent risk profile (e.g., launching new products or services, new connections). Management



Management can then decide what actions are needed either to affect the inherent risk profile or to achieve a desired state of maturity. On an ongoing basis, management may use the Assessment to identify changes to the institution's inherent risk profile when new threats arise or when considering changes to the business strategy, such as expanding operations, offering new products and services, or entering into new third-party relationships that support critical activities. Consequently, management can determine whether additional risk management practices or controls are needed to maintain or augment the institution's cybersecurity maturity.

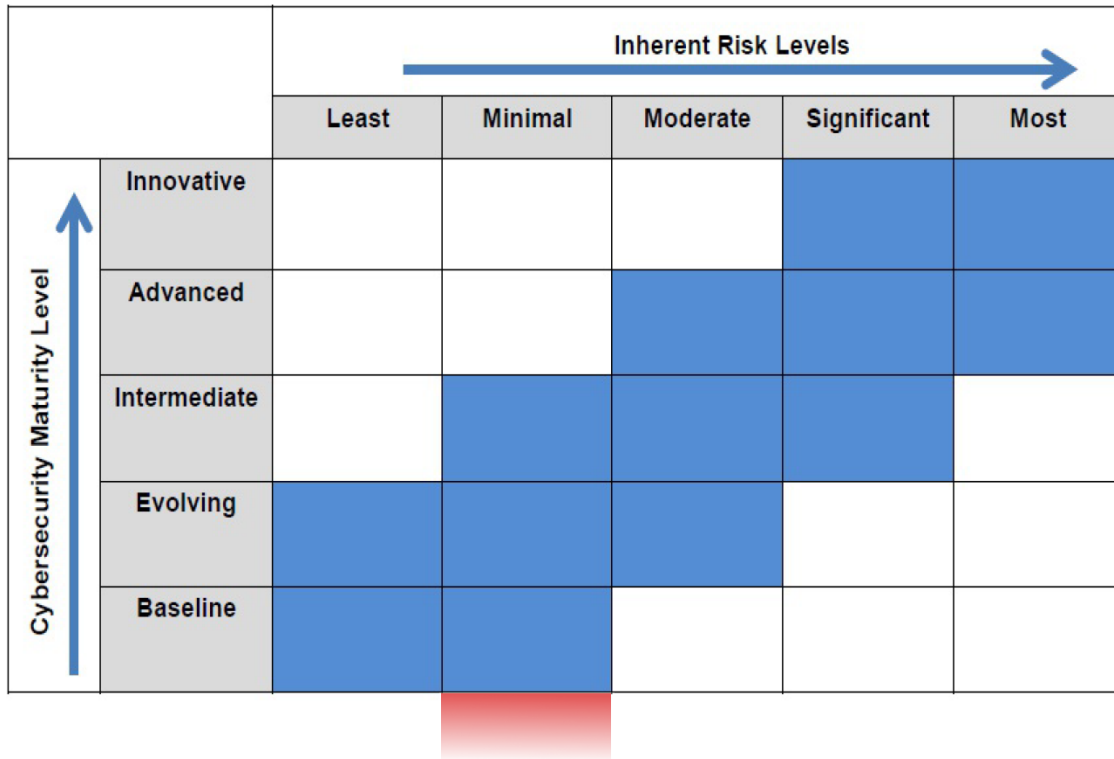
Cybersecurity Maturity Assessment

Based on the organization’s current calculated inherent risk, the organization has selected an initial target maturity level of “Baseline”. This assessment will determine the organization’s progress toward achieving the target level and provide recommendations for improvement where prescribed. Upon the achievement of its initial target maturity level, the organization may consider further improvements to achieve a maturity level of “Evolving” in order to be prepared to counter any evolving threats.

Domain 1: Cyber Risk Management and Oversight

Maturity Level: **Below Baseline**

Target Maturity Level: **Baseline**



COMPONENT	MATURITY LEVEL
IT Asset Management	Below Baseline
Oversight	Baseline
Strategy and Policies	Below Baseline
Staffing	Baseline
Audit	Baseline
Risk Assessment	Baseline
Risk Management Program	Baseline
Culture	Evolving
Training	Baseline

The credit union’s maturity level for Domain 1, Cyber Risk Management and Oversight, is below Baseline and improvement is needed in the IT Asset Management, and Strategy and Policies components to reach the Baseline maturity level. To reach the credit union’s target level of a Baseline maturity level, additional elements need to be implemented to improve the effectiveness of the program in the area of IT Asset Management and Strategy and Policies. To address the gap between the current maturity level and the desired level, the ISA conducted an analysis to determine the following results. This is presented as current gaps to meeting the Baseline maturity level.

Declarative Statements answered in the negative:

IT Asset Management:

- Management assigns accountability for maintaining an inventory of organizational assets. (FFIEC Information Security Booklet, page 9).

IMPACT: Assigning responsibility for asset inventory helps ensure that assets are available for business functions and facilitates effective lifecycle management.

RECOMMENDATION: TraceSecurity recommends assigning accountability for all organizational information assets and establish processes to maintain accurate asset inventories.

Strategy and Policies:

- The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management. (FFIEC Information Security Booklet, page, 16).

IMPACT: Defining risk management processes and responsibilities helps ensure accountability and more consistent implementation.

RECOMMENDATION: TraceSecurity recommends incorporating the roles, responsibilities and processes for risk management into the organization's information security policy.

- The institution has board-approved policies commensurate with its risk and complexity that address information security. (FFIEC Information Security Booklet, page 16).

IMPACT: Documenting board-approved information security policies helps to ensure proper accountability and facilitates management buy-in and support.

RECOMMENDATION: TraceSecurity recommends documenting all information security policies and gaining Board of Director approval in writing.

- The institution has policies commensurate with its risk and complexity that address the concepts of incident response and resilience. (FFIEC Information Security Booklet, page 83).

IMPACT: Defining incident response and resiliency policies, roles, and responsibilities helps ensure accountability and more consistent implementation.

RECOMMENDATION: TraceSecurity recommends defining policies that address the concepts of incident response and resilience.

Risk Assessment:

- A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, and customer information systems. (FFIEC Information Security Booklet, page 8).

IMPACT: Ensuring risk assessments follow a methodology to identify and analyze threats and controls helps to more accurately identify residual risk in order to prioritize remediation.

RECOMMENDATION: TraceSecurity recommends establishing a risk assessment methodology that identifies internal and external threats, the likelihood and impact of threats, and the sufficiency of control to reduce the risk to assets and information.



Recommendations:

Since the Baseline maturity level is based upon regulatory or industry guidance, TraceSecurity recommends that improvements to achieve Baseline cybersecurity maturity be the organization's first priority. This includes defining accountability for asset management, documenting the organization's risk management process, and ensuring that board-approved policies are defined to address all key elements of the cybersecurity program.

Domain 2: Threat Intelligence and Collaboration

Maturity Level: *Evolving*

Target Maturity Level: *Baseline*

		Inherent Risk Levels 				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level 	Innovative					
	Advanced					
	Intermediate					
	Evolving					
	Baseline					

COMPONENT	MATURITY LEVEL
Information Sharing	Evolving
Monitoring and Analyzing	Evolving
Threat Intelligence and Information	Evolving

The credit union's maturity level for Domain 2, Threat Intelligence and Collaboration is *Evolving*, and the target maturity level is *Baseline*. Currently, the organization's existing maturity level for this domain exceeds the target maturity level and helps prepare for dynamic and emerging threats.

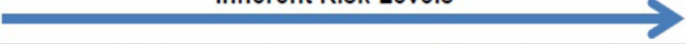

Recommendations:

Maintaining cybersecurity program components is an ongoing process. TraceSecurity recommends continued periodic evaluation of the organization's cybersecurity maturity. Changes or additions to the organization's program components should be considered when appropriate in response to changes in the threat landscape and the organization's associated inherent risk.

Domain 3: Cybersecurity Controls

Maturity Level: **Baseline**

Target Maturity Level: **Baseline**

		Inherent Risk Levels 				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level 	Innovative					
	Advanced					
	Intermediate					
	Evolving					
	Baseline					

COMPONENT	MATURITY LEVEL
Patch Management	Baseline
Remediation	Evolving
Anomalous Activity Detection	Baseline
Event Detection	Evolving
Threats and Vulnerability Detection	Baseline
Access and Data Management	Evolving
Device/Endpoint Security	Baseline
Infrastructure Management	Evolving
Secure Coding	Baseline

The credit union’s maturity level for Domain 3, Cybersecurity Controls, is assessed at the Baseline level, although a number of components are assessed at the Evolving maturity level. Currently, the organization’s existing maturity level for this domain meets the target maturity level.

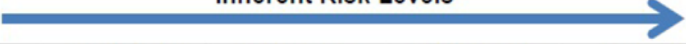

Recommendations:

Maintaining cybersecurity program components is an ongoing process. TraceSecurity recommends continued periodic evaluation of the organization’s cybersecurity maturity. Changes or additions to the organization’s program components should be considered when appropriate in response to changes in the threat landscape and the organization’s associated inherent risk.

Domain 4: External Dependency Management

Maturity Level: **Baseline**

Target Maturity Level: **Baseline**

		Inherent Risk Levels 				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level 	Innovative					
	Advanced					
	Intermediate					
	Evolving					
	Baseline					

COMPONENT	MATURITY LEVEL
Connections	Evolving
Contracts	Baseline
Due Diligence	Evolving
Ongoing Monitoring	Baseline

The credit union's maturity level for Domain 4, External Dependency Management, scored at a Baseline level although a number of components are assessed at the Evolving maturity level. Currently, the organization's existing maturity level for this domain meets the target maturity level.

Recommendations:

Maintaining cybersecurity program components is an ongoing process. TraceSecurity recommends continued periodic evaluation of the organization's cybersecurity maturity. Changes or additions to the organization's program components should be considered when appropriate in response to changes in the threat landscape and the organization's associated inherent risk.

Domain 5: Cyber Incident Management and Resilience

Maturity Level: **Below Baseline**

Target Maturity Level: **Baseline**

		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level	Innovative				Blue	Blue
	Advanced			Blue	Blue	Blue
	Intermediate		Blue	Blue	Blue	
	Evolving	Blue	Blue	Blue		
	Baseline	Blue	Blue			

COMPONENT	MATURITY LEVEL
Detection	Baseline
Response and Mitigation	Baseline
Escalation and Reporting	Below Baseline
Planning	Intermediate
Testing	Evolving

The credit union's maturity level for Domain 5, Cyber Incident Management and Resilience, is below Baseline and improvement is needed in incident management and tracking to reach the Baseline maturity level. Some components of this domain have achieved a maturity of Evolving or higher, which is commendable as it helps to ensure proper response and protections are employed. To address the gap between the current maturity level and the desired level, the ISA conducted an analysis to determine the following results. This is presented as current gaps to meeting the Baseline maturity level.

Declarative Statements answered in the negative (Baseline):

Escalation and Reporting:

- Incidents are classified, logged, and tracked. (FFIEC Operations Booklet, page 28).

IMPACT: Establishing a method to classify, log and track incidents helps to ensure accountability for response actions, supports post incident investigation, and facilitates trend analysis.

RECOMMENDATION: TraceSecurity recommends establishing a method or procedure to classify, log and track incidents from identification to resolution.

Recommendations:

Since the Baseline maturity level is based upon regulatory or industry guidance, TraceSecurity recommends that improvements to achieve Baseline cybersecurity maturity be the organization's first priority. This includes defining

how incidents are logged and tracked to support the Escalation and Reporting process. Documentation of these processes will help ensure accountability and consistent implementation.

Appendix: Additional Resources

FFIEC Cybersecurity Awareness Homepage

<http://www.ffiec.gov/cybersecurity.htm>

FFIEC Cybersecurity Assessment Tool User's Guide

http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_User_Guide_June_2015_PDF2_a.pdf

Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework

http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf

Mapping Cybersecurity Assessment Tool to FFIEC Handbook

http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_A_Map_to_FFIEC_Handbook_June_2015_PDF3.pdf

FFIEC CAT Glossary of Terms

http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf