

## Cybersecurity Assessment Report



Organization Name  
Date  
TraceSecurity

Table of Contents

Introduction..... 3

Definitions..... 4

    Risk Levels..... 4

    Maturity Levels..... 5

Detailed Results..... 6

    Inherent Risk Profile..... 6

    Cybersecurity Maturity Assessment..... 7

Appendix: Additional Resources..... 15

## 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 front line business 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.

## Definitions

### Inherent Risk Profile

INHERENT RISK LEVEL	NUMBER OF ANSWERS
Least	15
Minimal	16
Moderate	7
Significant	1
Most	0
Total	39

Overall Inherent Risk Level: Minimal

## Cybersecurity Maturity Assessment

### Domain 1: Cyber Risk Management and Oversight

Maturity Level: Below Baseline

Target Maturity Level: Baseline

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

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

### Summary

The maturity level for Domain 1, Cyber Risk Management and Oversight, is Below Baseline and improvement is needed in the audit component to reach the target level of Baseline. To address the gap between the current maturity level and the desired level a review and analysis have been made and the following were found. If the statements answered in the negative are implemented, the will achieve the desired maturity level of Baseline.

## Declarative Statements Answered in the Negative:

- The independent audit function validates controls related to the storage or transmission of confidential data. (FFIEC Audit Booklet, page 1)
- Issues and corrective actions from internal audits and independent testing/assessments are formally tracked to ensure procedures and control lapses are resolved in a timely manner. (FFIEC Information Security Booklet, page 6)
- Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information.

## Recommendations:

Independent internal audit and qualified third party audits are critical functions in the risk management process. Internal auditors, reporting directly to the Board of Directors or to the Audit Committee, are able to be objective in determining if controls are implemented and if the implemented controls sufficiently address inherent risk. Third party auditors should have the technical expertise to review the controls to determine the implementation level and give an unbiased opinion.

From the answers provided in the assessment, the analyst notes that the [REDACTED] does not perform audits on data storage or the transmission of data. By identifying storage locations, access restrictions, and environmental controls on electric and physical media, as well as the encryption level of electronically stored and transmitted data, the organization can determine if confidential information can be exposed or lost.

The review should include policies, procedures, and controls from across the organization to determine risks and improperly implemented or missing controls. The assessment should include all operations and include new business products, new technologies, and information systems.



Once issues are identified in audits, processes to correct deficiencies and track progress are needed to ensure that the findings are properly managed and in a timely manner.



## Domain 2: Threat Intelligence and Collaboration

Maturity Level: Below Baseline

Target Maturity Level: Evolving

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

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

### Summary

The ██████████ maturity level for Domain 2, Threat Intelligence and Collaboration, is Below Baseline, but the target maturity level is Evolving. To address the gap between the baseline and target maturity level a review and analysis have been made and the following were found. If the unimplemented controls are implemented, the ██████████ will achieve the desired maturity level of Evolving.

### Declarative Statements Answered in the Negative:

- A formal and secure process is in place to share threat and vulnerability information with other entities.
- The institution belongs or subscribes to a threat and vulnerability information sharing source(s) that provides information on threats (e.g. Financial Services Information Sharing and Analysis Center [FS-ISAC], U.S. Computer Emergency Readiness Team [US-C...])
- Threat information received by the institution includes analysis of tactics, patterns, and risk mitigation.

## Recommendations:

The [REDACTED] has no process for exchanging threat and vulnerability information to its peers, trade associations, or security agencies. Communications with peer and security organizations is the best method for learning about new threats, their impacts, and best defense methods. Threats such as malware, system vulnerabilities, hacking methods, and social engineering tactics are often published or presented in webcasts and regional meetings of various security, financial, and regulatory organizations or in trade publications.
















Such information is beneficial in learning the methods and mitigating steps necessary to protect organizational data and assets. By sharing information confidentially, the credit union can aid other organizations facing the same issues or receive feedback to improve its own security posture.

TraceSecurity recommends determining the best methods for learning about new threats and mitigation procedures and exchanging data with other similar organizations and trade associations to enhance security for its organization and industry.

## Domain 3: Cybersecurity Controls

Maturity Level: **Below Baseline**

Target Maturity Level: **Evolving**

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

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

### Summary

The            maturity level for Domain 3, Cybersecurity Controls, is Below Baseline, but the target maturity level is Evolving. An analysis was made to determine the variation between the maturity levels and the results are listed below. If the statements listed are fully implemented by the           , the maturity level of Evolving can be achieved. It should be noted that controls related to each other will appear as one analysis and recommendation.

The analyst also notes that once the Evolving maturity level is met, the            is one answer away from Intermediate and an additional two more from Advanced. TraceSecurity recommends reviewing the declarative statements to determine if improving the maturity level is achievable and consistent with the goals of the organization.

### Declarative Statements Answered in the Negative:

- Security Logs are reviewed regularly
- Firewall rules are audited or verified at least quarterly. (FFIEC Information Security Booklet, page 82)
- Firewall rules are updated routinely
- Administrators have two accounts: one for administrative use and one for general purpose, on-administrative tasks
- A process is in place to correlate event information from multiple sources (e.g. network, application, or firewall)

## Recommendations:

Security logs are the baseline source for detection of attacks and unauthorized attempts to access data. Multiple failed single user authentication attempts could indicate a password guessing attack and a large quantity of failed attempts would likely indicate a password brute force attack. Resource access failure is also logged allowing staff to determine if access to confidential information is attempted by a user or attacker. Syslog servers are capable of collecting the logs of all critical systems and communication devices, which includes security devices, enabling staff to determine attack methods, source, and correlate the information to allow technical staff to more quickly respond to the threat. Results from logging systems should be reviewed frequently. Other systems are available that allow technical staff to view critical security events in a graphical time line to determine if an attack is in progress or not.

Firewall rules should be audited on a regular basis to ensure the blocking of unwanted traffic from entering the network. Access lists can be very granular, blocking access by source, target, or network traffic type based on port number. By reviewing the controls, management can be sure that the access lists have been approved and have a documented reason for having each entry and that none of the rules explicitly allow unauthorized traffic. Firewall rule change should follow change management procedures, having each entry approved by management. The review could then compare the rule entries to the approved list.

Firewall rules should also be updated regularly as new threats arise or as new technologies are implemented. By updating the access lists, technical staff can block outbound traffic for known malicious sites, malware exploits, and inbound traffic from hostile nation-states. Access-list rules are often used on internal networks, implemented on routers or layer 3 switches to filter traffic between VLAN's and secure subnets such as DMZ.

Network administrators have a single account for all functions. Ideally, administrators have two accounts, one for administrative purposes and the other for normal user activity. Administrative accounts that are actively logged in are a prime target for attackers since a session or captured cached credentials would yield access to all systems and data. With the administrator logged in with a user account, the attacker would be forced to use other methods. A password breach for an administrative account would also present a rogue employee or visitor with access to sensitive data and systems. Ideally, the administrative account would not be used for logging into a work station since the credentials could be cached, but use the 'run-as' feature instead when performing technical functions that require elevated privileges.

TraceSecurity recommends implementing aggregate logging on critical servers and communications equipment to collect authentication failures and to determine attempted security breaches. TraceSecurity also recommends reviewing the logs often.

Firewall access lists are the first line of defense between external attackers and the [REDACTED] data. TraceSecurity recommends updating the firewall rules as new threats are discovered and audit the rules on a regular basis, comparing the rules to approved change management processes.

By having two accounts, one for administrative purposes and the other for daily use, network administrators can significantly improve the [REDACTED] security posture. TraceSecurity recommends implementing and enforcing the use of dual accounts for network administrators.

## Domain 4: External Dependency Management

Maturity Level: Innovative

Target Maturity Level: Innovative

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

COMPONENT	MATURITY LEVEL
Connections	Innovative
Contracts	Innovative
Due Diligence	Innovative
Ongoing Monitoring	Innovative

### Summary

The  maturity level for Domain 4, External Dependency Management, is innovative and is in line with its target maturity level.

### Declarative Statements Answered in the Negative:

None.



### Recommendations:

None.

## 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				✓	✓
	Advanced			✓	✓	✓
	Intermediate		✓	✓	✓	
	Evolving	✓	✓	✓		
	Baseline	✓	✓			

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

### Summary

The ██████ maturity level for Domain 5, Cyber Incident Management and Resilience, is Below Baseline and is below its target maturity level of Baseline. For the ██████ to reach its desired target maturity level, testing of the Incident Resilience Planning and Strategy should be improved. Once Baseline has been achieved, the analyst determined that only three answers are needed in the affirmative to gain the maturity level of Evolving. TraceSecurity recommends reviewing the declarative statements to determine if the improved maturity level is obtainable or desired.

### Declarative Statements Answered in the Negative:

- Scenarios are used to improve incident detection and response. (FFIEC Information Security Booklet, page 71)

### Recommendations:

Too often disaster recovery and incident response procedures are based on complete system outages or physical destruction of the organization's data center. The plan, if implemented, would provide a means to resume operations at the recovery site. Many scenarios exist that would place operations at risk that could render recovery operations ineffective, or would not be necessary for the current incident. TraceSecurity recommends using a multitude of scenarios in the planning of incident detection and response, and disaster recovery to determine the staff needed for each scenario, whether the mitigation involves isolating systems or implementing the recovery plan. TraceSecurity also recommends testing different scenarios as part of resilience planning.

## 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](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](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](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](http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf)