

Cybersecurity Assessment Report to Board of Directors

Quinnipiac University

EricNoga-October 2024

Table of Contents

[1 Introduction 3](#_Toc185066053)

[1.1 Definitions 4](#_Toc185066054)

[2 Inherent Risk Profile 6](#_Toc185066055)

[3 Cybersecurity Maturity 8](#_Toc185066056)

[4 Analysis 12](#_Toc185066057)

[5 Management and Board Questions 14](#_Toc185066058)

# Introduction

On June 30, 2015, the FFIEC released a Cybersecurity Assessment Tool to help financial institutions of all sizes identify their cybersecurity risks (Inherent Risk Profile) and assess their cybersecurity preparedness (Cybersecurity Maturity).

This report produced for Quinnipiac University includes responsibilities, definitions, results from the assessment, analysis of results, and questions to assist management and the Board when reviewing results.

#### Responsibility

The following roles and responsibilities are taken from the *FFIEC Cybersecurity Assessment Tool, Overview for Chief Executive Officers and Boards of Directors*.

The role of the chief executive officer (CEO), with management's support, may include the responsibility to do the following:

* Develop a plan to conduct the assessment.
* Lead employee efforts during the assessment to facilitate timely responses from across the institution.
* Set the target state of cybersecurity preparedness that best aligns to the board of directors' (board) stated (or approved) risk appetite.
* Review, approve, and support plans to address risk management and control weaknesses.
* Analyze and present results for executive oversight, including key stakeholders and the board, or an appropriate board committee.
* Oversee the performance of ongoing monitoring to remain nimble and agile in addressing evolving areas of cybersecurity risk.
* Oversee changes to maintain or increase the desired cybersecurity preparedness.

The role of the board, or an appropriate board committee, may include the responsibility to do the following:

* Engage management in establishing the institution's vision, risk appetite, and overall strategic direction.
* Approve plans to use the assessment.
* Review management's analysis of the assessment results, inclusive of any reviews or opinions on the results issued by independent risk management or internal audit functions regarding those results.
* Review management's determination of whether the institution's cybersecurity preparedness is aligned with its risks.
* Review and approve plans to address any risk management or control weaknesses.
* Review the results of management's ongoing monitoring of the institution's exposure to and preparedness for cyber threats.

#### Peer Analysis

In the Inherent Risk Profile and Cybersecurity Maturity sections of this report, peer data is provided for reference. Peer data is generated based upon the most current completed assessment of institutions who have opted into the Tandem **Peer Analysis** feature. A total of 780 completed assessments are included in the full data set.

## Definitions

#### Inherent Risk Level Definitions

According to the FFIEC, inherent risk is categorized using the following five levels:

* **Least:** 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:** 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:** 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:** 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:** 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 Level Definitions

According to the FFIEC, cybersecurity preparedness is categorized using the following five 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.

#### Sub-Baseline

A **Sub-Baseline** level is utilized as part of this assessment model for organizational reasons. Sub-Baseline is not a maturity level defined in the FFIEC Cybersecurity Assessment Tool. Baseline maturity is defined as meeting the “minimum expectations required by law and regulations.” For the purposes of this assessment, Sub-Baseline indicates the minimum legal and regulatory expectations are not being met by the organization.

# Inherent Risk Profile

Inherent risk incorporates the type, volume, and complexity of the institution’s operations including cybersecurity threats directed at the institution Inherent risk can range from *Least* to *Most* and does not include mitigating controls. The inherent risk below was calculated for Quinnipiac University by answering 39 questions taken from the FFIEC Cybersecurity Assessment Tool. Each question is specific to one of five categories also defined by the FFIEC. Risk level definitions have been included for reference on both the overall risk and the risk by category.

#### **Overall Inherent Risk**

|  |  |  |
| --- | --- | --- |
| Identified Risk | ⚫  Minimal | 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. |
| Target Risk | ⚫  Moderate | 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. |

#### **Inherent Risk by Category**

|  |  |  |
| --- | --- | --- |
| Category | Inherent Risk | Peer Risk |
| **Technologies and Connection Types**  Certain types of connections and technologies may pose a higher inherent risk depending on the complexity and maturity, connections, and nature of the specific technology products or services. This category includes the number of Internet service provider (ISP) and third-party connections, whether systems are hosted internally or outsourced, the number of unsecured connections, the use of wireless access, volume of network devices, end-of-life systems, extent of cloud services, and use of personal devices. | ⚫  Moderate | ⚫  Minimal |
| **Delivery Channels**  Various delivery channels for products and services may pose a higher inherent risk depending on the nature of the specific product or service offered. Inherent risk increases as the variety and number of delivery channels increases. This category addresses whether products and services are available through online and mobile delivery channels and the extent of automated teller machine (ATM) operations. | ⚫  Most | ⚫  Moderate |
| **Online/Mobile Products and Technology Services**  Different products and technology services offered by institutions may pose a higher inherent risk depending on the nature of the specific product or service offered. This category includes various payment services, such as debit and credit cards, person-to-person payments, originating automated clearing house (ACH), retail wire transfers, wholesale payments, merchant remote deposit capture, treasury services and clients and trust services, global remittances, correspondent banking, and merchant acquiring activities. This category also includes consideration of whether the institution provides technology services to other organizations. | ⚫  Minimal | ⚫  Minimal |
| **Organizational Characteristics**  This category considers organizational characteristics, such as mergers and acquisitions, number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged access, changes in information technology (IT) environment, locations of business presence, and locations of operations and data centers. | ⚫  Minimal | ⚫  Minimal |
| **External Threats**  The volume and type of attacks (attempted or successful) affect an institution’s inherent risk exposure. This category considers the volume and sophistication of the attacks targeting the institution. | ⚫  Moderate | ⚫  Minimal |

# Cybersecurity Maturity

The *Cybersecurity Maturity* levels below were determined for Quinnipiac University by answering 494 declarative statements organized into five domains taken from the FFIEC Cybersecurity Assessment Tool. Each declarative statement describes activities supporting assessment factors for each domain. To reach a maturity level in a domain, all declarative statements in that maturity level as well as previous maturity levels must not only be attained, but also sustained.

#### Cyber Risk Management and Oversight (D1)

Cyber risk management and oversight addresses the board of directors’ (board’s) oversight and management’s development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.

| Target Maturity | Recommended Maturity | Maturity | Peer Maturity\* |
| --- | --- | --- | --- |
| ⚫Evolving | ⚫Baseline | ⚫Intermediate | ⚫Evolving |

*\*The peer maturity for a domain is calculated by averaging the domain ratings from peers. Since it is not calculated by averaging the peer maturity of each component (below), it is possible for the peer maturity at the domain level to be lower than the peer maturity of all of its components.*

**Components**

| Component | Maturity Level | Peer Maturity |
| --- | --- | --- |
| Audit | ⚫Innovative | ⚫Intermediate |
| Culture | ⚫Innovative | ⚫Intermediate |
| IT Asset Management | ⚫Innovative | ⚫Evolving |
| Oversight | ⚫Innovative | ⚫Evolving |
| Risk Assessment | ⚫Innovative | ⚫Intermediate |
| Staffing | ⚫Innovative | ⚫Evolving |
| Training | ⚫Innovative | ⚫Evolving |
| Risk Management Program | ⚫Intermediate | ⚫Evolving |
| Strategy / Policies | ⚫Intermediate | ⚫Evolving |

#### Threat Intelligence and Collaboration (D2)

Threat intelligence and collaboration includes processes to effectively discover, analyze, and understand cyber threats, with the capability to share information internally and with appropriate third parties.

| Target Maturity | Recommended Maturity | Maturity | Peer Maturity\* |
| --- | --- | --- | --- |
| ⚫Advanced | ⚫Baseline | ⚫Sub-Baseline | ⚫Evolving |

*\*The peer maturity for a domain is calculated by averaging the domain ratings from peers. Since it is not calculated by averaging the peer maturity of each component (below), it is possible for the peer maturity at the domain level to be lower than the peer maturity of all of its components.*

**Components**

| Component | Maturity Level | Peer Maturity |
| --- | --- | --- |
| Monitoring & Analyzing | ⚫Evolving | ⚫Evolving |
| Information Sharing | ⚫Sub-Baseline | ⚫Evolving |
| Threat Intelligence & Information | ⚫Sub-Baseline | ⚫Intermediate |

#### Cybersecurity Controls (D3)

Cybersecurity controls are the practices and processes used to protect assets, infrastructure, and information by strengthening the institution’s defensive posture through continuous, automated protection and monitoring.

| Target Maturity | Recommended Maturity | Maturity | Peer Maturity\* |
| --- | --- | --- | --- |
| ⚫Evolving | ⚫Baseline | ⚫Sub-Baseline | ⚫Baseline |

*\*The peer maturity for a domain is calculated by averaging the domain ratings from peers. Since it is not calculated by averaging the peer maturity of each component (below), it is possible for the peer maturity at the domain level to be lower than the peer maturity of all of its components.*

**Components**

| Component | Maturity Level | Peer Maturity |
| --- | --- | --- |
| Anomalous Activity Detection | ⚫Innovative | ⚫Evolving |
| Device / End-Point Security | ⚫Innovative | ⚫Evolving |
| Event Detection | ⚫Innovative | ⚫Intermediate |
| Patch Management | ⚫Innovative | ⚫Intermediate |
| Remediation | ⚫Innovative | ⚫Intermediate |
| Threat & Vulnerability Detection | ⚫Innovative | ⚫Evolving |
| Access & Data Management | ⚫Advanced | ⚫Evolving |
| Infrastructure Management | ⚫Sub-Baseline | ⚫Evolving |
| Secure Coding | ⚫Sub-Baseline | ⚫Evolving |

#### External Dependency Management (D4)

External dependency management involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the institution’s technology assets and information.

| Target Maturity | Recommended Maturity | Maturity | Peer Maturity\* |
| --- | --- | --- | --- |
| ⚫Intermediate | ⚫Baseline | ⚫Sub-Baseline | ⚫Evolving |

*\*The peer maturity for a domain is calculated by averaging the domain ratings from peers. Since it is not calculated by averaging the peer maturity of each component (below), it is possible for the peer maturity at the domain level to be lower than the peer maturity of all of its components.*

**Components**

| Component | Maturity Level | Peer Maturity |
| --- | --- | --- |
| Connections | ⚫Innovative | ⚫Intermediate |
| Contracts | ⚫Innovative | ⚫Evolving |
| Ongoing Monitoring | ⚫Innovative | ⚫Evolving |
| Due Diligence | ⚫Sub-Baseline | ⚫Evolving |

#### Cyber Incident Management and Resilience (D5)

Cyber incident management includes establishing, identifying, and analyzing cyber events; prioritizing the institution’s containment or mitigation; and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber incident.

| Target Maturity | Recommended Maturity | Maturity | Peer Maturity\* |
| --- | --- | --- | --- |
| ⚫Intermediate | ⚫Baseline | ⚫Intermediate | ⚫Evolving |

*\*The peer maturity for a domain is calculated by averaging the domain ratings from peers. Since it is not calculated by averaging the peer maturity of each component (below), it is possible for the peer maturity at the domain level to be lower than the peer maturity of all of its components.*

**Components**

| Component | Maturity Level | Peer Maturity |
| --- | --- | --- |
| Detection | ⚫Innovative | ⚫Intermediate |
| Escalation & Reporting | ⚫Innovative | ⚫Intermediate |
| Planning | ⚫Innovative | ⚫Intermediate |
| Response & Mitigation | ⚫Innovative | ⚫Intermediate |
| Testing | ⚫Intermediate | ⚫Evolving |

# Analysis

The table below depicts the relationship between the Inherent Risk Profile and the domain maturity levels (D1, D2, etc.) calculated by the assessment for Quinnipiac University as well as the target levels (T1, T2, etc.) determined by management. Domain maturity is located under the assessment inherent risk column of Minimal, based on the institution’s overall inherent risk level. Guidance recommends domain maturity fall within the sections marked in blue. Any domain with a rating of Sub-Baseline should be addressed immediately.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | Inherent Risk | | | | |
| Least | Minimal | Moderate | Significant | Most |
| Cybersecurity Maturity | Innovative |  |  |  |  |  |
| Advanced |  |  | T2 |  |  |
| Intermediate |  | D1, D5 | T4, T5 |  |  |
| Evolving |  |  | T1, T3 |  |  |
| Baseline |  |  |  |  |  |
| Sub-Baseline |  | D2, D3, D4 |  |  |  |

(1 = Cyber Risk Management and Oversight, 2 = Threat Intelligence and Collaboration, 3 = Cybersecurity Controls, 4 = External Dependency Management, and 5 = Cyber Incident Management and Resilience)

#### Recommended Remediation

The following declarative statements were marked as “No” in the assessment causing domain maturity levels to fall below the assessment recommended maturity level. In order for Quinnipiac University to achieve the FFIEC recommended maturity level in each domain, each of the following declarative statements must be marked as “Yes.” Declarative statements causing the institution to have a maturity level of Sub-Baseline are emphasized with bold text and should be addressed immediately.

* **Threat information is used to monitor threats and vulnerabilities.**
* **Threat information is used to enhance internal risk management and controls.**
* **Information security threats are gathered and shared with applicable internal employees.**
* **Contact information for law enforcement and the regulator(s) is maintained and updated regularly.**
* **Information about threats is shared with law enforcement and regulators when required or prompted.**
* **All ports are monitored.**
* **Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards.**
* **The security controls of internally developed software are periodically reviewed and tested. (\*N/A if there is no software development.)**
* **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.)**
* **Intellectual property and production code are held in escrow. (\*N/A if there is no production code to hold in escrow.)**
* **A list of third-party service providers is maintained.**

# Management and Board Questions

The following questions were taken from the *FFIEC Cybersecurity Assessment Tool, Overview for Chief Executive Officers and Boards of Directors.* The questions were designed as optional discussion points to assist management and the Board when evaluating results from the assessment.

#### Cybersecurity Management & Oversight

1. What are the potential cyber threats to the institution?
2. Is the institution a direct target of attacks?
3. Is the institution’s cybersecurity preparedness receiving the appropriate level of time and attention from management and the board or an appropriate board committee?
4. Do the institution’s policies and procedures demonstrate management’s commitment to sustaining appropriate *Cybersecurity Maturity* levels?
5. What is the ongoing process for gathering, monitoring, analyzing, and reporting risks?
6. Who is accountable for assessing and managing the risks posed by changes to the business strategy or technology?
7. Are the accountable individuals empowered with the authority to carry out these responsibilities?
8. 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?
9. 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

1. What is the process for gathering and validating the information for the *Inherent Risk Profile* and *Cybersecurity Maturity*?
2. How can management and the board, or an appropriate board committee, support improvements to the institution’s process for conducting the assessment?
3. What do the results of the assessment mean to the institution as it looks at its overall risk profile?
4. What are the institution’s areas of highest inherent risk?
5. Is management updating the institution’s *Inherent Risk Profile* to reflect changes in activities, services, and products?

#### Cybersecurity Maturity

1. How effective are the institution’s risk management activities and controls identified in the assessment?
2. Are there more efficient or effective means for attaining or improving the institution’s risk management and controls?
3. What third parties does the institution rely on to support critical activities?
4. What is the process to oversee third parties and understand their *Inherent Risk Profile* and *Cybersecurity Maturity*?
5. How does management validate the type and volume of attacks?
6. Is the institution sharing threat information with peers, law enforcement, and critical third parties through information-sharing procedures?