

EricNoga-October 2024: Gap Analysis (Overall)

Quinnipiac University

12/12/2024

Table of Contents

[1 Cyber Risk Management and Oversight 3](#_Toc184920347)

[2 Threat Intelligence and Collaboration 4](#_Toc184920348)

[3 Cybersecurity Controls 5](#_Toc184920349)

[4 External Dependency Management 6](#_Toc184920350)

[5 Cyber Incident Management and Resilience 7](#_Toc184920351)

# Cyber Risk Management and Oversight

|  |  |  |
| --- | --- | --- |
| Current Maturity Level | Target Maturity Level | Recommended Maturity Level |
| ⚫Intermediate | ⚫Evolving | ⚫Baseline |

|  |
| --- |
| Showing Plan for Improving Maturity Level to: |
| ⚫Baseline |

The organization has already attained a maturity level of Baseline for this domain.

# Threat Intelligence and Collaboration

|  |  |  |
| --- | --- | --- |
| Current Maturity Level | Target Maturity Level | Recommended Maturity Level |
| ⚫Sub-Baseline | ⚫Advanced | ⚫Baseline |

|  |
| --- |
| Showing Plan for Improving Maturity Level to: |
| ⚫Baseline |

## Plan of Action

#### To Improve to Baseline

1. Information security threats are gathered and shared with applicable internal employees.
2. Threat information is used to monitor threats and vulnerabilities.
3. Contact information for law enforcement and the regulator(s) is maintained and updated regularly.
4. Threat information is used to enhance internal risk management and controls.
5. Information about threats is shared with law enforcement and regulators when required or prompted.

# Cybersecurity Controls

|  |  |  |
| --- | --- | --- |
| Current Maturity Level | Target Maturity Level | Recommended Maturity Level |
| ⚫Sub-Baseline | ⚫Evolving | ⚫Baseline |

|  |
| --- |
| Showing Plan for Improving Maturity Level to: |
| ⚫Baseline |

## Plan of Action

#### To Improve to Baseline

1. Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards.
2. The security controls of internally developed software are periodically reviewed and tested. (\*N/A if there is no software development.)
3. All ports are monitored.
4. 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.)
5. Intellectual property and production code are held in escrow. (\*N/A if there is no production code to hold in escrow.)

# External Dependency Management

|  |  |  |
| --- | --- | --- |
| Current Maturity Level | Target Maturity Level | Recommended Maturity Level |
| ⚫Sub-Baseline | ⚫Intermediate | ⚫Baseline |

|  |
| --- |
| Showing Plan for Improving Maturity Level to: |
| ⚫Baseline |

## Plan of Action

#### To Improve to Baseline

1. A list of third-party service providers is maintained.

# Cyber Incident Management and Resilience

|  |  |  |
| --- | --- | --- |
| Current Maturity Level | Target Maturity Level | Recommended Maturity Level |
| ⚫Intermediate | ⚫Intermediate | ⚫Baseline |

|  |
| --- |
| Showing Plan for Improving Maturity Level to: |
| ⚫Baseline |

The organization has already attained a maturity level of Baseline for this domain.