State of Maine
Department of Administrative & Financial Services
Office of Information Technology (OIT)

Risk Assessment Policy and Procedure (RA-1)

Table of Contents

1.0. Purpose

1.1. The purpose of this document is to outline the Office of Information Technology's policy and procedures for assessing and addressing security risks. This corresponds to the Risk Assessment (RA) Control Family, of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

2.0. Scope

2.1. This document applies to:

- 2.1.1. All State of Maine personnel, both employees and contractors;
- 2.1.2. Executive Branch Agency information assets, irrespective of location; and
- 2.1.2. Information assets from other State government branches that use the State network.

3.0. Conflict

3.1. If this document conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0. Roles and Responsibilities

4.1. *Agency Business Partner:*

- 4.1.1. In collaboration with OIT, holds all vendors/partners for Externally-hosted Information Assets accountable to this Policy, within the vendor/partner's span-of-control.
- 4.1.2. Develops and implements agency-level policy and procedures to meet any additional federal statutory requirements pertinent to agency risk management controls.
- 4.1.3. Collaborates with OIT on User Acceptance Testing for the remediation of legitimate vulnerabilities.

4.2. *OIT Information Security:*

- 4.2.1. Owns, executes, and enforces this Policy & Procedure.
- 4.2.2. Conducts risk assessments to determine mitigation priorities and articulate dangers to State of Maine IT systems.
- 4.2.3. For OIT-hosted Infrastructure and OIT-hosted Applications, executes the vulnerability scans.
- 4.2.4. For Externally-hosted Information Assets, either executes the vulnerability scans, or collects vulnerability scans from vendors or other third-party auditors.
- 4.2.5. Interprets all vulnerability scans: filters out the false-positives and false-negatives, and reports the legitimate vulnerabilities.
- 4.2.6. Determines the remediation schedule for legitimate vulnerabilities as specified in Vulnerability Scanning Procedure (RA-5).
- 4.2.7. Distributes the scan results to all downstream partners and/or Information Asset owners, and liaises with them.
- 4.2.8. The Chief Information Security Officer (CISO) reviews and approves security categorization decisions.

4.2.9. Liaises with horizontal Industry Partners on a need-to-know basis to help contain similar vulnerabilities in the wild. Includes MS-ISAC[1], the Maine Information and Analysis Center[2] (which then interfaces with state, local, and federal law-enforcement partners), and U.S. Department of Homeland Security.

4.2.10. Ensures that all OIT personnel are aware of all applicable penalties for non-compliance.

4.3. *OIT Information Asset Owners:*

4.3.1. Remediates all legitimate vulnerabilities within its span-of-control within the prescribed remediation schedule; and

4.3.2. Collaborates with Information Security in exploring Compensating Controls, should outright remediation turn out to be elusive.

4.3.3. Liaises with direct support vendors on a need-to-know basis to help contain similar vulnerabilities in the wild.

4.3.4. Identifies false positives and reports them for documentation and filtering by OIT Information Security.

4.4. *OIT Vendor Management:*

4.4.1. In collaboration with the Agency Business Partner, holds all vendors/partners for Externally-hosted Information Assets accountable to this Policy, within the vendor/partner's span-of-control.

5.0. Management Commitment

5.1. The State of Maine is committed to following this document.

6.0. Coordination Among Agency Entities

6.1. The various Divisions within OIT, as well as the Agency Business Partners, will cooperate with OIT Information Security in executing this document. OIT coordinates with horizontal Industry Partners and vendors on a need-to-know basis to help contain similar vulnerabilities in the wild.

7.0. Compliance

7.1. For State of Maine employees, failure to comply with this document may result in progressive discipline, up to and including dismissal.

7.2. For State of Maine contractors and non-State of Maine personnel, failure to comply may result in removal of the individual's ability to access, and use, State of Maine data and systems. Employers of contractors will be notified of any violations.

7.3. Personnel are also subject to any applicable penalties for statutory requirements compliance violations. Depending on the requirement, and the nature of the violation, penalties could include fines and/or criminal charges.

[1] https://www.cisecurity.org/ms-isac/

[2] https://memiac.org/

8.0. Procedures

8.1. The following serve as the baseline procedures that are implemented to meet risk assessment requirements. For information assets under its purview, the Office of Information Technology does the following:

8.2. **Security Categorization (RA-2):**

8.2.1. Categorizes information, and the information assets, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

8.2.1.1. OIT categorizes applications and servers, based on the data it receives, processes, and stores. Information security controls are applied to systems that receive, process, and store particular data types (e.g., Federal Tax, Social Security, Affordable Care Act, Protected Health, Credit Card Information).

8.2.1.2. Vendor-supported information assets that receive, process, and store particular data types are required to demonstrate information security compliance requirements, as outlined in System and Services Acquisition Policy and Procedures (SA-1) (coming soon).

8.2.2. Documents the security categorization results (including supporting rationale) in the security plan for the information system.

8.2.2.1. OIT has adopted common classification schema for data, communications, and environments.

8.2.2.2. For purposes of this classification, Personally Identifiable Information (PII) is any data that could potentially identify a specific individual.

8.2.2.3. PII confidentiality impact levels are determined to indicate the potential harm that could result to the subject individuals and/or the organization, if PII were to be inappropriately accessed, used, or disclosed. The following confidentiality impact levels are used, as outlined in the NIST Guide to Protecting the Confidentiality of PII, NIST SP 800-122[3]:

8.2.2.3.1. Not Applicable: Does not need to have its confidentiality protected, such as information that the organization has permission or authority to release publicly.

8.2.2.3.2. Low: The loss of Confidentiality, Integrity, or Availability (CIA) could be expected to have a Limited Adverse Effect on organizational operations, organizational assets, or individuals.

8.2.2.3.3. Moderate/Medium: The loss of CIA could be expected to have a Serious Adverse Effect on organizational operations, organizational assets, or individuals.

[3] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

8.2.2.3.4. High: The loss of CIA could be expected to have a Severe or Catastrophic Adverse Effect on organizational operations, organizational assets, or individuals.

8.2.2.4. Agencies should determine the PII confidentiality impact levels of their data as outlined in NIST SP 800-122[4], based on six factors:
- 8.2.2.4.1. Identifiability - how easily PII can be used to identify specific individuals.
- 8.2.2.4.2. Quantity of PII - how many individuals are identified in the information.
- 8.2.2.4.3. Data Field Sensitivity - the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together.
- 8.2.2.4.4. Context of Use - the purpose for which PII is collected, stored, used, processed, disclosed, or disseminated.
- 8.2.2.4.5. Access to and Location of PII - the nature of authorized access to PII. Questions that help determine this include:
  - 8.2.2.4.5.1. How often will it be accessed, and by how many different persons and/or systems? When PII is accessed more frequently, and more widely, there exist more opportunities for compromise of confidentiality.
  - 8.2.2.4.5.2. Is it being stored on, or accessed from, remote workers' devices, or other systems, such as web applications, outside the direct control of the organization?

8.2.2.5. OIT subscribes to the Cybersecurity and Infrastructure Security Agency (CISA) Traffic Light Protocol (TLP)[5]. OIT's four classification levels are as follows:
- 8.2.2.5.1. Public (TLP: White): Non-sensitive, suitable for public consumption. Examples include:
  - 8.2.2.5.1.1. PII with no impact level (i.e., Not Applicable).
  - 8.2.2.5.1.2. Public announcements or other publicly suitable information.
  - 8.2.2.5.1.3. Resources exposed to the Internet.
- 8.2.2.5.2. Internal (TLP: Green): Suitable for State Employees and contractors only, but not sensitive. Examples include:
  - 8.2.2.5.2.1. PII with no impact level (i.e., Not Applicable).

[4] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf
[5] https://www.us-cert.gov/tlp

8.2.2.5.2.2. Employee newsletters or announcements, etc.
8.2.2.5.2.3. Internal memorandums not classified as "sensitive".
8.2.2.5.2.4. Subnets containing OIT Intranet servers.
8.2.2.5.3. Sensitive (TLP: Amber): Suitable for State Employees and select contractors only. Examples include:
8.2.2.5.3.1. PII of a low or moderate confidentiality impact level.
8.2.2.5.3.2. Infrastructure information (IP addresses, server names, etc.).
8.2.2.5.3.3. Information that would be embarrassing to the agency or the State if released.
8.2.2.5.3.4. OIT File-servers, File-Shares, and their associated subnets.
8.2.2.5.4. Restricted (TLP: Red): Suitable for select State Employees and contractors only, access granted only on a need-to-know basis. Data must be encrypted at rest and in flight. Examples include:
8.2.2.5.4.1. PII of a high confidentiality impact level.
8.2.2.5.4.2. Federally protected data to include Federal Tax, Social Security, Affordable Care Act, Protected Health, Credit Card Information.
8.2.2.6. As a security categorization decision, PII confidentiality impact levels and TLP determinations must reviewed and approved by the CISO.

8.3. **Risk Assessment (RA-3):**

8.3.1. Based on the data that reside on information assets, and the regulatory regime they are subjected to, risk levels are routinely audited by external partners (usually Federal regulatory agencies). See the OIT Security Assessment and Authorization Policy and Procedures (CA-1)[6] for more specific information.
8.3.2. OIT also hires third party vendors to conduct independent risk assessments. These vendors are required to produce reports including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the in-scope information system, and the information it processes, stores, or transmits. These reports are maintained by OIT Information Security. The State of Maine shares risk assessment results to affected stakeholders on a need-to-know basis.
8.3.3. The sum-total of all such assessments lead to applicable security plans. The results of information security vulnerabilities are documented for remediation or mitigation based on available resources. The priorities for

[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-assessment-authorization-policy.pdf

these remediation efforts are also established. For more information, see the OIT Plan of Action and Milestones (POA&M) (CA-5) (coming soon).

8.4 **Vulnerability Scanning (RA-5):**

8.4.1 OIT performs vulnerability scans on all information assets. Scan reports, which are provided to the responsible parties, note patches that are missing, settings that expose possible vulnerabilities, and third-party software issues. Information systems must pass the Deployment Certification which requires a scan prior to being deployed or upgraded. If a specific threat is announced at any time, the OIT Security Team schedules scans to assess vulnerability risk. See OIT Vulnerability Scanning Procedures (RA-5)[7] for more details.

9.0. Document Details

9.1. Initial Issue Date: 6 March 2020
9.2. Latest Revision Date: 6 March 2020
9.3. Point of Contact: Enterprise.Architect@Maine.Gov
9.4. Approved By: Chief Information Officer, OIT
9.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[8]
9.6. Waiver Process: Waiver Policy[9]

10.0. Review

10.1. This document will be reviewed annually, and when substantive changes are made to Policies, Procedures, or other authoritative regulations affecting this document.

11.0. Records Management

11.1. Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and Directives* records management categories. They will be retained for three (3) years, and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

12.0. Public Records Exceptions

12.1. Under the Maine Freedom of Access Act, certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures or risk assessments. Information contained in these records may be disclosed to the Legislature, or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any

[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/vulnerablity-scanning-procedure.pdf
[8] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf

aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the state.

13.0. Definitions

13.1. *Availability:* Ensuring timely and reliable access to and use of information.

13.2. *Compensating Control:* An alternative mechanism instituted to mitigate a legitimate vulnerability when the actual mechanism to properly remediate the vulnerability is deemed impractical in the present time. If utilized, Compensating Controls must provide the same, or greater level, of defense as would be attained through the proper remediation. Compensating Controls may be used as an interim solution, until the full remediation can be undertaken.

13.3. *Confidentiality:* Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

13.4. *Externally-hosted Information Assets:* Generic term for any I.T. product consumed from the Public Cloud. Includes the full spectrum of Software as a Service, Platform as a Service, and Infrastructure as a Service.

13.5. *Industry Partner:* Generic term for *all* external parties that apprise the Information Security Division of the Cybersecurity vulnerability landscape. Could be open-channel partners, such as product vendors, trade magazines, security research organizations, etc. Could be closed-channel partners, such as MS-ISAC, the Maine Information and Analysis Center, et al.

13.6. *Information Assets:* The full spectrum of all I.T. products, including business applications, system software, development tools, utilities, appliances, etc.

13.7. *Integrity:* Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

13.8. *Legitimate Vulnerability*: Neither a false positive, nor a false negative. An actual weakness, not only flagged by an automated scan, but verified by a human analyst.

13.9. *Limited Adverse Effect*: the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

13.10. *Risk Assessment*: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.

13.11. *Serious Adverse Effect*: the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

13.12. *Severe or Catastrophic Adverse Effect*: the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

13.13. *Vulnerability:* Weakness in an Information Asset that could be exploited by a threat source.