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

Risk Assessment Policy and Procedures (RA-1)

Table of Contents

1.0. Purpose

The purpose of this document is to outline the Office of Information Technology's (OIT's) policy and procedures for assessing and addressing security risks. This policy corresponds to the Risk Assessment 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 (see Definitions), irrespective of location; and
- 2.1.2. Information assets from other State government branches that use the State network.

3.0. Conflict

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 and partners for externally hosted information assets (see Definitions) accountable to this policy, to the extent within the vendor or partner's span of control (see Definitions).
- 4.1.2. Develops and implements agency-level policy and procedures to meet 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 (see Definitions).

4.2. OIT Information Security

- 4.2.1. Owns, executes, and enforces this Risk Assessment Policy and Procedures.
- 4.2.2. Conducts risk assessments (see Definitions) to determine mitigation priorities and articulates dangers to State of Maine information technology systems.
- 4.2.3. Executes vulnerability (see Definitions) scans for OIT-hosted infrastructure and applications.
- 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 false-positives and false-negatives, and reports legitimate vulnerabilities.
- 4.2.6. Determines the remediation schedule for legitimate vulnerabilities as specified in the Vulnerability Scanning Procedure (RA-5).[1]

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/VulnerablityScanningProcedure.pdf

4.2.7. Distributes the scan results to all downstream partners and 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 (see Definitions), on a need-to-know basis, to help contain similar vulnerabilities in the wild. These include the Multi-State Information Sharing & Analysis Center,[2] the Maine Information Analysis[3] (which then interfaces with State, local, and Federal law-enforcement partners), and the U.S. Department of Homeland Security.
4.2.10. Ensures that all OIT personnel are aware of the penalties for noncompliance.

4.3. OIT Information Asset Owners
4.3.1. Remediate all legitimate vulnerabilities within their span of control according to the prescribed remediation schedule;
4.3.2. Collaborate with OIT Information Security in exploring compensating controls (see Definitions), should outright remediation turn out to be elusive;
4.3.3. Liaise with direct-support vendors, on a need-to-know basis, to help contain similar vulnerabilities in the wild;
4.3.4. In collaboration with the agency business partners and DAFS IT Procurement, holds all vendors and partners for externally hosted information assets accountable to this policy, to the extent within the vendor or partner's span of control; and
4.3.5. Identify false positives and report them for documentation and filtering by OIT Information Security.

4.4. DAFS IT Procurement
4.4.1. Ensures policies are in vendor contracts or IT procurement instruments, in collaboration with the agency business partners and OIT information asset owners.

5.0. Management Commitment

The State of Maine is committed to following this document.

6.0. Coordination Among Agency Entities

The 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.

[2] https://www.cisecurity.org/ms-isac/
[3] https://memiac.org/

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 violations.

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

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, OIT 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 (for example, Federal tax information, Social Security information, protected health information, credit card information, and so forth).

8.2.1.2. Vendor-supported information assets that receive, process, and store particular data types are required to demonstrate compliance with information security requirements, as outlined in System and Services Acquisition Policy and Procedures (SA-1).[4]

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 (see Definitions) impact levels are established to indicate the potential harm to the subject individuals or to the organization if the PII were 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:[5]

[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemAndServicesAcquisitionPolicy.pdf
[5] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

8.2.2.3.1. Not Applicable: Information that the organization has permission or authority to release publicly and, therefore, does not need confidentiality protection.

8.2.2.3.2. Low: The loss of confidentiality, integrity (see Definitions), or availability (see Definitions) (CIA) of the information could be expected to have a limited adverse effect (see Definitions) on organizational operations, organizational assets, or individuals.

8.2.2.3.3. Moderate/Medium: The loss of information CIA could be expected to have a serious adverse effect (see Definitions) on organizational operations, organizational assets, or individuals.

8.2.2.3.4. High: The loss of information CIA could be expected to have a severe or catastrophic adverse effect (see Definitions) 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,[6] 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 or systems? The more frequently and widely PII is accessed, the more opportunities exist 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, that are outside the direct control of the organization?

8.2.2.5. OIT subscribes to the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) Traffic Light Protocol (TLP) classification levels Traffic Light Protocol (TLP).[7] OIT's four classification levels are as follows:

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

8.2.2.5.1. Public (TLP:WHITE): Nonsensitive, suitable for public consumption. Examples include:
8.2.2.5.1.1. PII with no impact level (in other words, 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 (in other words, Not Applicable).
8.2.2.5.2.2. Employee newsletters or announcements, and so on.
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, and so on).
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 (see Definitions). 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 information, Social Security information, Affordable Care Act information, protected health information, and 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 resides on information assets and the regulatory regime to which they are subject, risk levels are routinely audited by external

partners (usually Federal regulatory agencies). See the Security Assessment Authorization Policy[8] 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 that include 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 with affected stakeholders on a need-to-know basis.

8.3.3. The sum-total of all such assessments is used to inform applicable security plans. The results of information security vulnerabilities are documented for remediation or mitigation, based on available resources, and the priorities for the remediation efforts are established. For more information, see the OIT Plan of Action and Milestones (POA&M) (CA-5).[9]

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 deployment or upgrade. If a specific threat is announced, the OIT Information Security team schedules scans to assess vulnerability risk. See the OIT Vulnerability Scanning Procedure[10] for more details.

9.0. Document Details

9.1. Initial issue Date: March 6, 2020
9.2. Latest Revision Date: June 30, 2021
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[11]
9.6. Waiver Process: Waiver Policy[12]
9.7. Distribution: Internet[13]

10.0. Review

This document is reviewed annually and when substantive changes are made to policies, procedures, or other authoritative regulations affecting this document.

---

[8] https://www.maine.gov/oit/policies/SecurityAssessmentAuthorizationPolicy.pdf
[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityAssessmentAuthorizationPolicy.pdf
[10] https://www.maine.gov/oit/policies/VulnerablityScanningProcedure.pdf
[11] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[12] https://www.maine.gov/oit/policies/waiver.pdf
[13] https://www.maine.gov/oit/policies-standards

11.0. Records Management

OIT 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 future Maine State Archives General Schedule revisions that cover these categories.

12.0. Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA), 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 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: Timely and reliable access to and use of information assets.

13.2. Compensating control: An alternative mechanism instituted to mitigate a legitimate vulnerability when the mechanism that would remediate the vulnerability properly is deemed impractical. 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 until full remediation can be undertaken.

13.3. Confidentiality: The state of being kept private or secret, including preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

13.4. Externally hosted information asset: Any information technology product consumed from the public cloud including the full spectrum of Software as a Service, Platform as a Service, and Infrastructure as a Service products.

13.5. Industry partner: An external party that apprises OIT Information Security of the cybersecurity-vulnerability landscape. These can be open-channel partners such as product vendors, trade magazines, security research organizations, and so on; or they can be closed-channel partners, such as the Multi-State Information Sharing and Analysis Center and the Maine Information and Analysis Center.

13.6. In flight: Digital information in the process of being transported between locations either within or between computer systems.

13.7. Information asset: Used interchangeably with information system. A discrete, identifiable piece of information technology, including hardware, software, and

firmware. Information assets include, for example, mainframes, workstations, servers (including database, electronic mail, authentication, web, proxy, file, and domain name), input/output devices (such as scanners, copiers, and printers), network components (such as firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, and sensors), operating systems, virtual machines, middleware, business applications, system software, development tools, and miscellaneous related utilities.

13.8. Integrity: The accuracy and consistency (validity) of data over its lifecycle. Guarding the integrity of information assets against improper modification or destruction includes ensuring information nonrepudiation and authenticity.

13.9. Legitimate vulnerability: Neither a false positive nor a false negative, but a true weakness that has been verified by a human analyst in addition to being flagged by an automated scan.

13.10. Limited adverse effect: A loss of confidentiality, integrity, or availability that might (i) cause a degradation in or loss of mission capability to an extent and duration that the organization experiences a noticeable reduction in its ability to perform its primary functions effectively; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

13.11. Risk assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact of the occurrence, and the safeguards that mitigate this impact.

13.12. Serious adverse effect: A loss of confidentiality, integrity, or availability that might (i) cause a significant degradation in or loss of mission capability to an extent and duration that the organization experiences a significant reduction in its ability to perform its primary functions effectively; (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.

13.13. Severe or catastrophic adverse effect: A loss of confidentiality, integrity, or availability that 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 life-threatening injuries.

13.14. Span of control: The area of activity and number of functions, people, or things for which an individual or organization is responsible.

13.15. Vulnerability: Weakness in an information asset that could be exploited by a threat source.

14.0. Abbreviations

14.1. CIA: confidentiality, integrity, or availability
14.2. CISO: Chief Information Security Office
14.3. FOAA: [Maine] Freedom of Access Act
14.4. NIST: National Institute of Standards and Technology
14.5. OIT: Office of Information Technology
14.6. PII: Personally Identifiable Information
14.7. POA&M: Plan of Action & Milestones
14.8. TLP: Traffic Light Protocol