State of Maine

Department of Administrative and Financial Services

Office of Information Technology

Risk Assessment Policy and Procedures (RA)

Risk Assessment Policy and Procedures (RA)

Table of Contents

1.0. Document Purpose

The purpose of this document is to define the State of Maine policy and procedures that are in place to ensure comprehensive assessment and management of security risks to State of Maine information assets (see Definitions). This part of the security program focuses on protecting the confidentiality (see Definitions), integrity (see Definitions), and availability (see Definitions) of State information assets through the identification, evaluation, and mitigation of risks. This document corresponds to the Risk Assessment (RA) Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 5).[1]

2.0. Scope

2.1. This policy applies to all State of Maine employees and contractors (collectively referred to as personnel in this document) with access to:

2.1.1. Executive Branch Agency information assets, irrespective of location; and

2.1.2. Information assets from other State government branches that use Executive Branch-managed services.

3.0. Policy Conflict

If this policy conflicts with any applicable law or union contract, the terms of the existing law or contract shall 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 the State of Maine information technology systems.

1 https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

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).[2]

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,[3] the Maine Information Analysis[4] (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.

---

[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/VulnerablityScanningProcedure.pdf
[3] https://www.cisecurity.org/ms-isac/
[4] https://memiac.org/

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 policy and the procedures that support it.

6.0. Coordination Among Agency Entities

6.1. The divisions within OIT, as well as the agency business partners, will cooperate with OIT Information Security in executing this document.

6.2. 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 the 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.

8.0. Procedures

The following standards apply to and represent the security controls established to meet an acceptable level of protection for the State of Maine contingency planning processes.

8.1. Security Categorization (RA-2)

8.1.1. OIT Categorizes information and the information assets in accordance with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance.

8.1.1.1. 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).

8.1.1.2. 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).[5]

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

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

8.1.2.2. For purposes of this classification, personally identifiable information (PII) is any data that could potentially identify a specific individual.

8.1.2.3. 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:[6]

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

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

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

8.1.2.3.4. 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.

8.1.2.4. Agencies should determine the PII confidentiality impact levels of their data as outlined in NIST SP 800-122,[7] based on six factors:

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

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

8.1.2.4.1. Identifiability — how easily PII can be used to identify specific individuals.

8.1.2.4.2. Quantity of PII — how many individuals are identified in the information.

8.1.2.4.3. Data Field Sensitivity — the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together.

8.1.2.4.4. Context of Use — the purpose for which PII is collected, stored, used, processed, disclosed, or disseminated.

8.1.2.4.5. Access to and Location of PII — the nature of authorized access to PII. Questions that help determine this include:

8.1.2.4.5.1. 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.

8.1.2.4.5.2. 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?

8.1.2.5. OIT subscribes to the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) Traffic Light Protocol (TLP)[8] classification levels. OIT's five classification levels can be found in section 7.0 of the Data Classification Policy.[9]

8.1.2.6. As a security categorization decision, PII confidentiality impact levels and TLP determinations must reviewed and approved by the CISO.

8.1.2.7. Impact-Level Prioritization (RA-2(1))

8.1.2.7.1. The State of Maine recognizes the potential value of impact-level prioritization for high-value assets.

[8] https://www.us-cert.gov/tlp
[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf

8.1.2.7.2. This approach involves partitioning systems into subcategories (e.g., low-moderate, moderate-high, high-high) to support more granular risk-based decision-making.

8.1.2.7.3. Impact-level prioritization is not currently implemented but may be considered in future iterations of the risk assessment framework.

8.2. Risk Assessment (RA-3)

8.2.1. 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[10] for more specific information.

8.2.1.1. Risk assessments are conducted to:

8.2.1.1.1. Identify potential threats to the confidentiality, integrity, and availability of an information system and the environment in which it operates.

8.2.1.1.2. Determine the likelihood that threats will materialize.

8.2.1.1.3. Identify and evaluate vulnerabilities within the system or environment.

8.2.1.1.4. Assess the potential impact if one or more vulnerabilities are exploited by a threat.

8.2.1.1.5. Evaluate the potential impact on individuals, particularly with regard to personally identifiable information (PII), arising from system breaches or vulnerabilities.

8.2.2. 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.

8.2.3. 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

[10] https://www.maine.gov/oit/policies/SecurityAssessmentAuthorizationPolicy.pdf

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).[11]

8.2.4. Risk Assessment Execution and Reporting

8.2.4.1. Enterprise risk assessments are conducted annually by OIT Information Security (GRC), utilizing the Nationwide Cybersecurity Review (NCSR) self-assessment or through engagement of a third-party for independent evaluation.

8.2.4.2. Risk assessment results are formally documented in a risk assessment report, which is submitted to the Chief Information Security Officer (CISO) for review.

8.2.4.3. Any risks identified that exceed defined risk tolerance thresholds are documented as findings requiring mitigation.

8.2.4.4. Risk assessment results are disseminated to relevant stakeholders to inform decision-making.

8.2.4.5. Initial and subsequent risk assessments are conducted at the discretion of the CISO, in response to regulatory compliance requirements, or when significant changes to a system, its operational environment, or other factors may impact the system's security posture.

8.2.5. Supply Chain Risk Assessment (RA-3(1))

8.2.5.1. The State of Maine recognizes the importance of assessing supply chain risks associated with organizational systems, components, and services. These risks may include disruption, insertion of counterfeits, theft, malicious development practices, improper delivery, and the introduction of malicious code. Supply chain risk assessments help identify systems or components requiring additional mitigation measures.

8.2.5.2. Implementation guidance for RA-3(1) is currently under review and will be finalized following the completion of Supply Chain Risk (SR) Policy and Procedures.

8.2.6. All-Source Intelligence Integration (RA-3(2))

8.2.6.1. The State of Maine recognizes the value of incorporating all-source intelligence into the risk assessment process to improve its ability to identify, assess, and respond to risk.

[11] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityAssessmentAuthorizationPolicy.pdf

8.2.6.2. All-source intelligence includes threat intelligence from internal sources (e.g., system logs, incident reports) and external sources (e.g., Information Sharing and Analysis Centers [ISACs], federal agencies, commercial threat feeds).

8.2.6.3. All-source intelligence helps identify adversarial tactics, techniques, and procedures (TTPs) that may target organizational systems, vendors, or supply chains.

8.2.6.4. Incorporating all-source intelligence enhances the prioritization of risk response activities and supports more accurate threat modeling.

8.2.6.5. Intelligence sources will be cataloged and reviewed annually to ensure relevance, accuracy, and alignment with enterprise risk priorities.

8.3. Risk Response (RA-7)

8.3.1. The State of Maine responds to findings from assessments, monitoring, and audits in accordance with its defined risk tolerance.

8.3.2. Risk response strategies are selected based on the nature of the risk and its potential impact on enterprise operations.

8.3.3. Salient risks are documented in the Enterprise Risk Register, with an approved response strategy selected by the Chief Information Security Officer (CISO).

8.3.4. Risk response decisions are made prior to generating a plan of action and milestones (POA&M) entry. If mitigation cannot be completed immediately, a POA&M entry is created to track remediation.

8.4. Privacy Impact Assessments (RA-8)

8.4.1. As owners of their data, agencies are required to conduct Privacy Impact Assessments (PIAs) to evaluate the privacy risks associated with the collection, processing, storage, and dissemination of personally identifiable information (PII).

8.4.2. PIAs must be performed prior to developing or procuring information technology that processes PII, and before initiating new collections of PII that meet applicable thresholds.

8.4.3. PIAs are updated as needed in response to significant changes to the system, environment, or organizational practices, and to meet federal regulatory compliance requirements.

8.4.4. As owners of their data, agencies are responsible for ensuring compliance with applicable privacy regulations and for mitigating privacy risks related to PII. The Office of Information Technology (OIT) may support the security portions of these assessments on an as-needed basis.

8.5. Criticality Analysis (RA-9)

8.5.1. OIT fulfills criticality analysis requirements by developing and maintaining data flow diagrams that identify essential system components, data, and functions supporting regulated data exchanges in compliance with applicable federal and partner requirements.

9.0. Document Details

9.1. Initial Issue Date: March 6, 2020

9.2. Latest Revision Date: October 31, 2025

9.3. Point of Contact: PolicyTeam.OIT@Maine.Gov

9.4. Approved By: Chief Information Officer, OIT

9.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[12]

9.6. Waiver Process: Waiver Policy[13]

9.7. Distribution: Internet[14]

10.0. Review

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

11.0. Records Management

OIT security policies, plans, and procedures fall under the *Major Administrative Policies and Procedures* and *Internal Control Policies and Directives* records management categories. They will be retained for a minimum of six years after withdrawal or replacement and then destroyed in accordance with guidance[15] 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

Under the Maine Freedom of Access Act (FOAA),[16] 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 Maine State 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.

---

[12] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[13] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[14] https://www.maine.gov/oit/policies-standards
[15] https://www.maine.gov/sos/arc/records/state/GS1Administrative.pdf
[16] https://legislature.maine.gov/statutes/1/title1sec402.html

13.0. Definitions

13.1. All-Source Intelligence: Threat intelligence derived from both internal sources (e.g., system logs, incident reports) and external sources (e.g., ISACs, federal agencies, commercial threat feeds).

13.2. Availability: Timely and reliable access to and use of information assets.

13.3. Bug Bounty Program: A financial incentive program that rewards external researchers for responsibly reporting discovered vulnerabilities.

13.4. 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.

13.5. 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.

13.6. Criticality Analysis: The process of identifying system components and functions that are essential to mission execution and assessing their potential impact if compromised.

13.7. 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.

13.8. Impact-Level Prioritization: A method of partitioning systems into subcategories (e.g., low-moderate, moderate-high, high-high) to support more granular risk-based decision-making.

13.9. 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, or they can be closed-channel partners, such as the Multi-State Information Sharing and Analysis Center and the Maine Information and Analysis Center.

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

13.11. Information Asset: Used interchangeably with Information System. A discrete, identifiable piece of information technology, including hardware, software, firmware, systems, services, and related technology assets used to execute work on behalf of OIT or another State agency. (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30).

13.12. Instrumentation-Based Tools: Tools that analyze system components continuously using embedded instrumentation, without relying on active scanning.

13.13. 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.

13.14. 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.

13.15. 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.

13.16. Remediation Window: A defined timeframe within which identified vulnerabilities must be remediated to meet compliance or operational requirements.

13.17. 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.

13.18. 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.

13.19. 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.

13.20. Security Operations Center: A centralized team responsible for monitoring, analyzing, and responding to cybersecurity incidents, alerts, and public disclosures.

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

13.22. Threat Modeling: The process of identifying potential threats, vulnerabilities, and attack vectors to inform risk prioritization and mitigation strategies.

13.23. Unmediated Access: Direct access to critical system components or functions without appropriate controls or safeguards, increasing vulnerability risk.

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

13.25. Vulnerability Disclosure Program: A formal process for receiving and responding to reports of security vulnerabilities from external researchers or the public.

14.0. Abbreviations

14.1. CIA: Confidentiality, Integrity, and Availability

14.2. CISO: Chief Information Security Officer

14.3. CVE: Common Vulnerabilities and Exposures

14.4. CVSS: Common Vulnerability Scoring System

14.5. CWE: Common Weakness Enumeration

14.6. DAFS: Department of Administrative and Financial Services

14.7. FOAA: [Maine] Freedom of Access Act

14.8. GRC: Governance, Risk, and Compliance

14.9. ISAC: Information Sharing and Analysis Center

14.10. NCSR: Nationwide Cybersecurity Review

14.11. NIST: National Institute of Standards and Technology

14.12. NVD: National Vulnerability Database

14.13. OIT: Office of Information Technology

14.14.

14.15. OVAL Open Vulnerability and Assessment Language

14.16. PIA Privacy Impact Assessment

14.17. PII: Personally Identifiable Information

14.18. POA&M: Plan of Action and Milestones

14.19. SCAP Security Content Automation Protocol

14.20. SOC Security Operations Center

14.21. TLP: Traffic Light Protocol

14.22. TTPs Tactics, Techniques, and Procedures