State of Maine
Department of Administrative & Financial Services
Office of Information Technology

System and Services Acquisition Policy and Procedures (SA-1)

Table of Contents

APPENDICES

1.0 Document Purpose:

1.1 The purpose of this document is to establish the Office of Information Technology's (OIT) policy and procedures for the effective implementation of security controls and control enhancements in the System and Services Acquisition family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4)[1]. This policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2.0 Scope:

2.1 This policy applies to all State of Maine (SOM) 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 the State network.

3.0 Policy Conflict:

3.1 If this policy 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 *The Chief Information Officer (CIO) is responsible for:*

4.1.1 Certifying that effective security controls are in place in the system acquisition, development, and management process for the protection of State of Maine information systems and assets;

4.1.2 Certifying that effective fiscal controls are in place for system and services acquisition, development, and management;

4.1.3 Approving the security requirement budget requests submitted by the Chief Information Security Officer (CISO); and

4.1.4 Providing the Information Security Office (ISO) with appropriate resources to secure the enterprise through the coordination, development, implementation, and maintenance of an enterprise-wide information security program.

4.2 *The Chief Information Security Officer (CISO) is responsible for:*

4.2.1 Prioritizing information security services and authorizing any security exceptions;

4.2.2 Identifying appropriate resources for allocation in information security budgeting, planning, and documentation;

4.2.3 Performing security assessments to determine information security gaps at the enterprise level and documenting those gaps in the Plan of Action and Milestones (POA&M);

[1] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

4.2.4 Defining the security and compliance requirements of services and equipment;
4.2.5 Ensuring that IT vendor-managed and contracted services and equipment are secure;
4.2.6 Co-approving the acquisition of services and equipment that affect existing technology with the Enterprise Architect; and
4.2.7 Owning, executing, and enforcing this document.

4.3 *The Information Security Office (ISO) is responsible for:*
4.3.1 Reviewing all security documentation submitted by vendors to ensure compliance with all third-party audit requirements;
4.3.2 Ensuring that information security requirements are met within the system and service acquisition process; and
4.3.3 Ensuring that the system life cycle activities meet the security requirements for the enterprise.

4.4 *The Architecture and Policy Team is responsible for:*
4.4.1 Establishing and maintaining policies for the acquisition of services and hardware, as well as documenting the necessary architectural requirements;
4.4.2 Managing the design review and new technology intake process;
4.4.3 Documenting the security and compliance requirements for services and equipment; and
4.4.4 Co-approving the acquisition of services and equipment that affect existing technology with the CISO.

4.5 *The OIT Finance Director is responsible for:*
4.5.1 Reviewing purchase requests for services and equipment above $5,000 against available resources; and
4.5.2 Managing the OIT budget process from estimation through execution.

4.6 *The Project Management Office (PMO) is responsible for:*
4.6.1 Ensuring standards, procedures and practices are being followed to ensure projects are successful and return the expected value to the organization;
4.6.2 Managing project scope changes to leverage opportunities, optimizing shared objectives across projects, resourcing projects, and managing methodologies and metrics; and
4.6.3 Facilitating the sharing of resources, methodologies, tools, and techniques.

4.7 *IT Procurement is responsible for:*
4.7.1 Managing the portfolio of IT contracts;
4.7.2 Working with vendors, SOM agencies, and the ISO to ensure that vendor contracts contain the appropriate information security requirements;
4.7.3 Working with agencies to ensure that contracts for vendor-hosted or vendor-managed agency information assets include the requisite contract language

to safeguard the data at risk in accordance with applicable federal and state regulations, and OIT policies, procedures, and standards;

4.7.4 Ensuring interconnections with vendors are properly documented using Service Level Agreements (SLAs), Memorandums of Agreement (MOAs), and contracts, to include the requisite security information (see Security Assessment and Authorization Policy and Procedures (CA-3);[2] and

4.7.5 Resolving and managing any identified problem areas with vendors in collaboration with the supported agency and the Applications Director.

4.8 *MaineIT Applications Development is responsible for:*

4.8.1 Working with agencies to ensure that:

4.8.1.1 Vendors meet the necessary security requirements; and

4.8.1.2 Any requested exceptions are submitted for evaluation and final approval by the CIO or the CISO through the waiver process.

4.9 *The Contract Administrator is responsible for:*

4.9.1 Monitoring vendor performance to ensure vendor adherence to contract provisions throughout the contract, including on-going maintenance and support;

4.9.2 Providing all vendor third party audit reports and information security documentation to the ISO for review;

4.9.3 Reviewing all services, outputs and products provided by third parties at least annually; and

4.9.4 Maintaining contract-related documentation, including security documentation.

4.10 *Agencies are responsible for:*

4.10.1 Working with the PMO to ensure projects are successful and return the expected value to the organization;

4.10.2 Proper *Traffic Light Protocol (TLP)* classification of all data used and held by the agency and their vendors in accordance with Risk Assessment Policy and Procedures;[3]

4.10.3 Ensuring that funding for the acquisition is adequate for sustaining the system/service beyond the initial purchase;

4.10.4 Ensuring compliance with Maine Department of Treasury's Credit Card Information Security Policy and Guidelines,[4] as well as taking responsibility for any fines levied as a result of Payment Card Industry Data Security Standard non-compliance;

4.10.5 Ensuring security functional requirements are part of the acquisition process for hardware, software, or firmware; and

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

[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/risk-assessment-policy-procedure.pdf

[4] https://www1.maine.gov/treasurer/private/CreditCardProcessingPolicyWithAttachments.pdf

4.10.6 Ensuring agency personnel are aware of all applicable penalties for non-compliance.

4.11 *Third party service providers/vendors are responsible for:*

4.11.1 Implementing secure information systems, system components, and services that comply with all applicable federal and state laws and regulations and ensuring compliance with all OIT contractual requirements and information security policies.

4.12 *Change Advisory Board (CAB) is responsible for:*

4.12.1 Maintaining the Change Management policies, which enables system engineers, architects, and security analysts to expediently perform their necessary business functions, yet maintain a controlled, secure, and functioning environment (see OIT Change Management Policy and Procedures).[5]

5.0 Management Commitment:

5.1 The State of Maine is committed to following this policy and the procedures that support it.

6.0 Coordination Among Agency Entities:

6.1 OIT works in close coordination with agencies to ensure alignment between the individual IT needs of the agency and the protection of SOM network infrastructure. OIT is a fee for service agency that also participates in the biennial budget process, identifying baseline funding requirements critical to safeguarding the State's information assets for inclusion within the state budget. The service expectation and business needs of OIT's customers and partner agencies relies on a collaborative partnership between State agencies and OIT. OIT fosters a collective appreciation among its partner agencies of the importance of securing the State's information technology (IT) infrastructure.

7.0 Compliance:

7.1 For SOM employees, failure to comply with the procedures identified in this policy may result in progressive discipline up to and including dismissal.

7.2 For SOM contractors and non-SOM personnel, failure to comply may result in removal of the individual's ability to access and use SOM data and systems. Employers of non-SOM personnel 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.

[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/change-management-policy.pdf

8.0 Procedures:

8.1 The following procedures are designed to satisfy the security control requirements as prescribed under relevant federal and state laws, Executive Orders, rules, regulations, policies, and guidance.

8.2 **Allocation of Resources (SA-2):**

8.2.1 OIT works with agencies to:

8.2.1.1 Identify information security requirements for information systems and services in mission/business process planning; and

8.2.1.2 Ensure security costs are integrated into the agency's costs for services within acquisition processes.

8.2.2 As part of the biennial budget process:

8.2.2.1 The CISO works in partnership with OIT *Information Asset Owners* to determine the information security requirements for protection of the State's information systems and assets.

8.2.2.2 The CISO documents information security requirements for consideration by the CIO.

8.2.2.3 The CIO consolidates the OIT budget for approval. Once budget items are approved, the CISO allocates the money required to protect the State's information systems and assets.

8.2.2.4 The CISO manages a discrete budget line for information security within OIT, which includes planning for resource allocation for initial acquisition and funding for the sustainment of the systems or services acquired.

8.2.3 OIT purchase requests for the acquisition of hardware, software, firmware, or media above $5,000 for use on the SOM network are made using the Purchase Request Form if not already specifically listed (i.e., individually by name) and approved as part of the biennial budget process. See Appendix A OIT Purchase Request Form.

8.3 **System Development Life Cycle (SDLC) (SA-3):**

8.3.1 OIT has documented System Development Life Cycle requirements in the Software Development Lifecycle (SDLC) Policy[6] and Procedures.[7]

8.3.1.1 The Software Development Lifecycle Policy and Procedures define and document security roles and responsibilities.

8.3.2 The CISO, security architects, and other members of the Information Security Office participate in development activities as required.

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

[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-procedure.pdf

8.3.3 Security concerns are taken into consideration from SDLC planning through development phases as specified in General Architecture Principles,[8] which states “security and privacy are foundational to everything else.”

8.3.4 Holding a robust, technical design review is a critical milestone in the SDLC. Design Review is conducted weekly as follows:

8.3.4.1 Technical experts from cross-functional teams within OIT meet to evaluate proposed solutions against SOM requirements. See Appendix B OIT Design Review Committee Form.

8.3.4.2 Outcomes from the Design Review session vary depending on the age, status, and where in the SDLC the solution/project current stands. Common deliverables include:

8.3.4.2.1 Areas of concern to address prior to proceed with the solution/project;

8.3.4.2.2 Security and compliance review and approval to proceed;

8.3.4.2.3 Feedback on feasibility and risk;

8.3.4.2.4 Requests for further solution diagrams and documentation; and

8.3.4.2.5 Requests for additional Design Review meetings as solution/project progresses.

8.3.4.3 A thorough security vetting is required for every solution/project. Based on a review of the documentation material provided and information obtained during the meeting, the following security measures are identified:

8.3.4.3.1 High-risk aspects of the solution/project;

8.3.4.3.2 Architectural flaws;

8.3.4.3.3 Business risk potential;

8.3.4.3.4 Vulnerability detection;

8.3.4.3.5 Security of architecture, design, and open source/third-party components; and

8.3.4.3.6 Compliance requirements and data classification.

8.3.4.4 As required, recommendations on remediation are presented to the solutioning/project team. Follow-up Design Review sessions may occur to discuss risks and steps for remediation.

8.3.5 Security is then considered through SLDC integration, testing, and implementation phases as it must pass security testing as part of the Application Deployment Certification Policy.[9] Waivers to security are approved only as a part of a formal process outlined in the Waiver Policy;[10]

[8] http://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/general-architecture-principles_1.pdf

[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf

[10] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf

this process is facilitated by the Architecture and Policy Team with approvals by either the CISO or the CIO.

8.3.6 Security is maintained through the remainder of the lifecycle process through assessments as outlined in Security Assessment and Authorization Policy and Procedures (CA-1)[11] and vulnerability management as outlined in Vulnerability Scanning Procedure (RA-5).[12] Furthermore, security of systems through changes are considered as a part of Change Management Policy and Procedures.[13]

8.4 **Acquisition Process (SA-4; CEs 1, 2 and 9):**

8.4.1 IT systems and services must meet the security requirements appropriate to the data they contain.

8.4.1.1 IT Procurement works with the agency, ISO, and the Architecture and Policy Team to document the appropriate security and compliance requirements that must be met in the request for purchase and contract documentation.

8.4.1.2 The Architecture and Policy Team facilitates a review of new technology documentation with the agencies, IT Procurement, and the ISO to determine that appropriate security and compliance requirements are met.

8.4.1.3 Project managers support agencies in the acquisition of IT systems and services that meet security requirements appropriate to the data they contain, requiring the appropriate security approvals prior to implementation through project completion in accordance with General Architecture Principles.[14]

8.4.1.4 OIT supports agencies in their efforts to ensure that all applicable security and compliance requirements for their data are maintained throughout the system's lifecycle.

8.4.2 Before the acquisition of an IT system or service is completed, in addition to meeting security and compliance requirements, the following must also be documented and understood:

8.4.2.1 Acceptance criteria;

8.4.2.2 A description of the information systems development and deployment environments;

8.4.2.3 The location of systems that receive, process, or store agency data;

8.4.2.4 The functional properties, design, and implementation of security controls to be employed; and

8.4.2.5 The functions, ports, and services intended for organizational use.

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

[12] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/vulnerablity-scanning-procedure.pdf

[13] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/change-management-policy.pdf

[14] http://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/general-architecture-principles_1.pdf

8.4.3 The minimum essential security standards that must be complied with prior to the acquisition through the deployment of IT systems and services include the following:

8.4.3.1 OIT Information Security Policy[15]
8.4.3.2 OIT Hosting and Housing Policy[16]
8.4.3.3 OIT Application Deployment Certification Policy[17]
8.4.3.4 OIT Application Deployment Certification Handbook[18]
8.4.3.5 OIT Remote Hosting Policy[19]
8.4.3.6 OIT Software Development Lifecycle Procedure[20]
8.4.3.7 OIT Software Development Lifecycle Policy[21]
8.4.3.8 OIT Change Management Policy[22]
8.4.3.9 OIT Confidentiality and Non-Disclosure Agreements for vendors with access to state and federally-protected data types (signed prior to granting access to data)

8.4.4 In addition to the minimum essential security standards considered in 8.4.3, IT systems and services that involve access to federally-protected data must document the security standards specified for that data type. Examples of documentation requirements include, but are not limited to the following:

8.4.4.1 Use of a Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreements for *Protected Health Information* (PHI);
8.4.4.2 Inclusion of contract language from Exhibit 7 of Internal Revenue Service (IRS) Publication 1075,[23] Tax Information Security Guidelines for Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information for Federal Tax Information;
8.4.4.3 Service Level Agreements containing language as specified in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (SSA); and
8.4.4.4 All SOM IT contracts of any dollar amount must be accompanied by a completed Rider B-IT Agreement to Purchase Services, which

[15] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/information-security-policy.pdf
[16] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/hosting-housing-policy.pdf
[17] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf
[18] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification-guidelines_1.pdf
[19] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/remote-hosting-policy.pdf
[20] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-procedure.pdf
[21] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-policy.pdf
[22] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/change-management-policy.pdf
[23] https://www.irs.gov/pub/irs-pdf/p1075.pdf

requires OIT's review and approval and signature of the CIO (see Division of Procurement Services).[24]

8.4.5 Only OIT-approved software may be used on the network.

8.4.5.1 All software purchases by state agencies must be pre-approved by the ISO through the change management process to mitigate risks of exploitation of covert channels.

8.4.5.2 A pre-approved list of software that has met security requirements is maintained by the Architecture and Policy Team. These software applications have been determined by the ISO to have met security functionality, assurance, and documentation requirements to receive approval.

8.4.6 Absent a waiver from the ISO, the use of Freeware and Open Source Software (OSS) by an agency is prohibited. If the use of such Freeware or OSS is discovered by OIT, the agency may be subject to fines and penalties associated with the use of such software, including the cost of remediating any security risks caused by their use to the SOM network.

8.4.7 The ISO regularly scans the network to identify unauthorized hardware and/or software and notifies appropriate agency personnel when discovered.

8.4.8 All IT hardware and software assets must be assigned to a designated business unit or individual.

8.5 **Information System Documentation (SA-5):**

8.5.1 OIT only approves information systems for which proper documentation is provided and follows the aforementioned Policies and Procedures in 8.3 or 8.4. All documents are either produced by the State or the vendor.

8.5.2 Software Development Lifecycle Procedures[25] list the artifacts required for each corresponding SDLC Discipline Test.

8.5.3 Application Deployment Certification Policy[26] requires a summary result (Passed/Failed/Not Applicable) and a short paragraph clarifying that summary result, for a host of required tests (e.g., interfaces, security, performance).

8.5.4 What matters in terms of the artifacts required in 8.5.2 and 8.5.3 is the content, not the title. The information includes administrator and user documentation for the system, component, or service. Additional

[24] https://www.maine.gov/dafs/bbm/procurementservices/forms

[25] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-procedure.pdf

[26] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf

administrator and user documentation for the system, component, or service may be required as a function of the contract or project management documentation as required by the PMO.

8.5.5 Submission of the artifacts in 8.5.2 and 8.5.3 does not preclude the necessity of submitting other project management documentation to the PMO concerning the overall management of the project. The PMO determines the scope and nature of the required project management documentation.

8.6 **Security Engineering Principles (SA-8):**

8.6.1 The following security engineering principles for new technology or technology undergoing major upgrades should be considered as part of the SLDC procedures outlined in 8.3 of this Policy:

8.6.1.1 Security is layered to create a defense in depth;

8.6.1.2 Security controls, policy, and architecture are arranged as recommended by the National Institute of Standards and Technology (NIST);

8.6.1.3 Security is foundational to everything else to include SDLC;

8.6.1.4 Clear physical and logical security boundaries should be established;

8.6.1.5 System developers are trained to develop secure software;

8.6.1.6 Security controls are established appropriate to the data and network it is engineered to protect; and

8.6.1.7 Security controls are appropriate to lower the risk a system poses to an acceptable level.

8.7 **External Information System Services (SA-9; CEs 1, 2 and 5)**

8.7.1 Plans to outsource information system services that handle select federally-provided data types require advanced notifications and approval as required by the respective federal agencies (e.g., IRS, SSA, Centers for Medicare, and Medicaid Services, etc.).

8.7.2 The use of systems other than those owned by the SOM that handle select federally-provided data types require advanced notifications and approval as required by the respective federal agencies (e.g., IRS).

8.7.3 Changes to the systems that handle select federally-provided data types require advanced notifications and approval as required by the respective federal agencies (e.g., SSA).

8.7.4 *Cloud service providers* that receive, process, store, or transmit data types categorized as TLP: Amber or TLP: Red, which include federally-protected data, must have one of the following, or combination thereof, acceptable third-party audit reports (see SA-11 for further information):

8.7.4.1 Maintain a *Federal Risk and Authorization Management Program (FedRAMP)* certification for the appropriate data impact level (e.g., Moderate, High);

8.7.4.2 Maintain an *International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001* certification; or

8.7.4.3 Provide annually a *Service Organization Control (SOC) 2 Type II* audit report with the appropriate trust principles.

8.7.5 The oversight, roles, and responsibilities with regard to *external information system services* are shared between OIT and the agencies. The delineation of these are specified in this document.

8.7.6 IT Procurement assists agencies with documenting expectations of performance with vendors using Service Level Agreements (SLAs), Memorandums of Agreement (MOAs), and contracts.

8.7.7 The ISO assists agencies who are responsible for determining the TLP classification of all data used and held by their agency and vendors. The TLP classification drives the level of information security required of an acquisition or outsourced information service to lower the risk of that data to an acceptable level. (**CE-1**)

8.7.8 External service providers identify the functions, ports, protocols, and other services required for the use of such services as a part of design review and deployment certification (**CE-2**).

8.7.9 All contracts for services that receive, process, or store data or services categorized as TLP: Red must be located in the continental United States (**CE-5**).

8.8 Developer Configuration Management (SA-10):

8.8.1 OIT's configuration management policies are to be outlined in Configuration Management Policy and Procedures (coming soon).

8.8.2 Configuration management for system, service, or component development are determined and performed:

8.8.2.1 In development, as a part of design review as determined by the agency and OIT using the OIT Design Review Committee Form (See Appendix B);

8.8.2.2 In implementation, and verified through the deployment certification process; and

8.8.2.3 In operation, as a part of required audits and vulnerability management.

8.8.3 The integrity of changes made are documented and managed in the Enterprise Ticketing System as outlined in Change Management Policy and Procedures[27] and Jira Software used by application development.

8.8.4 The OIT CAB approves changes that are then implemented using a risk-based approach. Approvals follow a documented Request for Change (RFC) process based on the RFC type (e.g., Normal, Emergency).

8.8.5 Third party vendors must configure their services in a secure manner. Developer configuration management is addressed through deployment certification, contractual obligations, and audits as appropriate.

8.8.6 Security waivers must be approved by the CISO that arise due to vulnerability scans conducted prior to deployment. Vulnerabilities must be remediated or waived as outlined in the Application Deployment Certification Policy.[28]

8.8.7 OIT security flaw resolution and reporting requirements are outlined in the OIT Vulnerability Scanning Procedures (RA-5)[29] and Incident Reporting Procedures (IR-6)[30] (available on the intranet only). Other OIT policies describe security flaw resolution during the development of information systems, the implementation of system components, or the operation of information system services.

8.9 **Developer Security Testing and Evaluation (SA-11; CE 1):**

8.9.1 OIT follows OIT deployment certification protocols, policies, and procedures.

8.9.2 OIT assists agencies in the development of security assessment plans to meet federal regulatory requirements or as otherwise required.

8.9.3 OIT performs unit, integration, system, regression, and security testing and evaluation as required.

8.9.4 Flaws are remediated as required according to the OIT Vulnerability Scanning Procedures (RA-5)[31] and the deployment certification protocols, policies, and procedures.

[27] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/change-management-policy.pdf

[28] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf

[29] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/vulnerablity-scanning-procedure.pdf

[30] https://inet.state.me.us/oit/policies/documents/IncidentReportingProcedures.pdf

[31] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/vulnerablity-scanning-procedure.pdf

8.9.5 The results of security testing and the execution of the security assessment plan are recorded in the Enterprise Ticketing System.

8.9.5.1 The execution of the security assessment plan is documented as necessary to meet federal regulatory requirements or as otherwise required.

8.9.6 OIT typically reviews static code to identify and remediate common flaws in different environments (e.g. test, development) as a part of deployment, implementation, and operations (**CE-1**).

8.9.7 Vendors are reviewed for their ability to provide the required security appropriate to their product.

8.9.8 All vendors must meet minimum security requirements to the satisfaction of the CISO and CIO. These vendors include those providing *Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS)*.

8.9.9 All CSPs that receive, process, store, or transmit data types categorized as TLP: Amber or TLP: Red must submit an approved certification or acceptable third-party audit report. See Appendix C - Cloud Service Provider Security Requirements for more details.

8.10 Unsupported System Components (SA-22)

8.10.1 OIT strives to make the best possible use of its IT dollars by eliminating waste and promoting efficiency.

8.10.2 Within available resources, OIT replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer and provides justification and documentation of the approval for the continued use of unsupported system components required to satisfy the agency's mission/business needs.

8.10.3 When necessary, if agencies or OIT require the continued use of unsupported system components, outdated applications or hardware, the entity must provide justification and documents for approval by the CISO or CIO through the waiver or budget process for the continued use of unsupported system components.

8.11 No Expectation of Privacy

8.11.1 Information assets created, purchased, leased, or licensed by the State of Maine, including, but not limited to, software (e.g. application software, application source code, systems software), physical equipment (e.g. computers, portable devices, tablets, smartphones), communications equipment (e.g. routers, switches, firewalls), electronic media (e.g. disks, tapes), services (e.g. Internet, communications, cloud), and information (e.g.

databases and data files, system documentation, network diagrams), are the property of the State of Maine. As such, the State has the absolute right to monitor the use of such property. Accordingly, users of State information assets shall not assume their actions or use of State information assets are private or protected.

9.0 Document History and Distribution:

Version	Revision Log	Date
Version 1.0	*Initial Publication*	*October 30, 2020*
Version 1.1	*Insubstantial Changes*	*November 03, 2023*

Approved by:

Legal Citation: Title 5, Chapter 163: Office of Information Technology[32].

Distribution: This document will be distributed to all appropriate State of Maine personnel and will be posted on the OIT website (https://www.maine.gov/oit/policies-standards).[33]

10.0 Document Review:

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

11.0 Records Management:

The Office of Information Technology's 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:

Under the Maine Freedom of Access Act, certain public records exceptions may limit disclosure of agency records related to IT 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.

[32] http://legislature.maine.gov/statutes/5/title5ch163sec0.html
[33] https://www.maine.gov/oit/policies-standards

13.0 Definitions:

13.1 *Cloud Service Provider* - an organization that provides cloud services. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

13.2 *External information system services* - services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. Organizations using external service providers that are processing, storing or transmitting federal information or operating information systems on behalf of the federal government must ensure that such providers meet the same security requirements that federal organizations are required to meet. (Source: NIST 800-53).

13.3 *FedRAMP* - a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

13.4 *Information Asset Owner* - Information Asset is used interchangeably with Information System and is a discrete, identifiable piece of IT, including hardware, software, and firmware. Ownership of Information Assets is listed in the OIT Information Systems Contingency Plan (CP-2).[34]

13.5 *Infrastructure as a Service (IaaS)* - the capability provided to the consumer is the provision of processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications and possibly limited control of select networking components (e.g., host firewalls).

13.6 *ISO/IEC 27001* - Internationally accepted standards and requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using these standards enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details, or information entrusted by third parties. Certification by an independent body provides the necessary written assurance (a certificate) that the product, service, or system in question meets the specific ISO/IEC 27001 requirements.

13.7 *Personally Identifiable Information (PII)* - Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying

[34] https://inet.state.me.us/oit/policies/documents/InformationSystemsContingencyPlan.pdf

information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Source: NIST CSRC Glossary.[35] Maine state law does not define PII, but rather provides a more limited definition of "personal information" within the context of the Maine Notice of Risk to Personal Data Act (see 10 M.R.S. §1347).[36]

13.8 *Platform as a Service (PaaS)* - the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

13.9 *Protected Health Information (PHI)* – individual health information held by covered entities subject to the HIPAA Privacy and Security Rules; these Rules provide federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.

13.10 *SOC 2 Type I* – A report that details the suitability of the design controls to the service organization's system. It details the system at a point in time particularly its scope, the management of the organization describing the system, and the controls in place. SOC 2 Type I report shows that a SaaS firm has best practices in place. Generation of a SOC 2 Type I report is also quick after a service entity completes a readiness assessment. This report should be used when shopping for a third-party vendor, especially since the other type of SOC 2 report, Type 2, can take up to a year to be completed.

13.11 *SOC 2 Type II* - A report that demonstrates a thorough examination by a third-party accounting and auditing firm of an organization's internal control policies and practices over a specified period of time; the report shows the firm has reviewed and examined an organization's control objectives and activities, and tested those controls to ensure that they are operating effectively. Adherence to specific Trust Service Principles must be met in order to successfully achieve certification, which include: Security, Availability, Processing Integrity, Confidentiality, or Privacy. These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

13.12 *Software as a Service (SaaS)* - the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are

[35] https://csrc.nist.gov/glossary

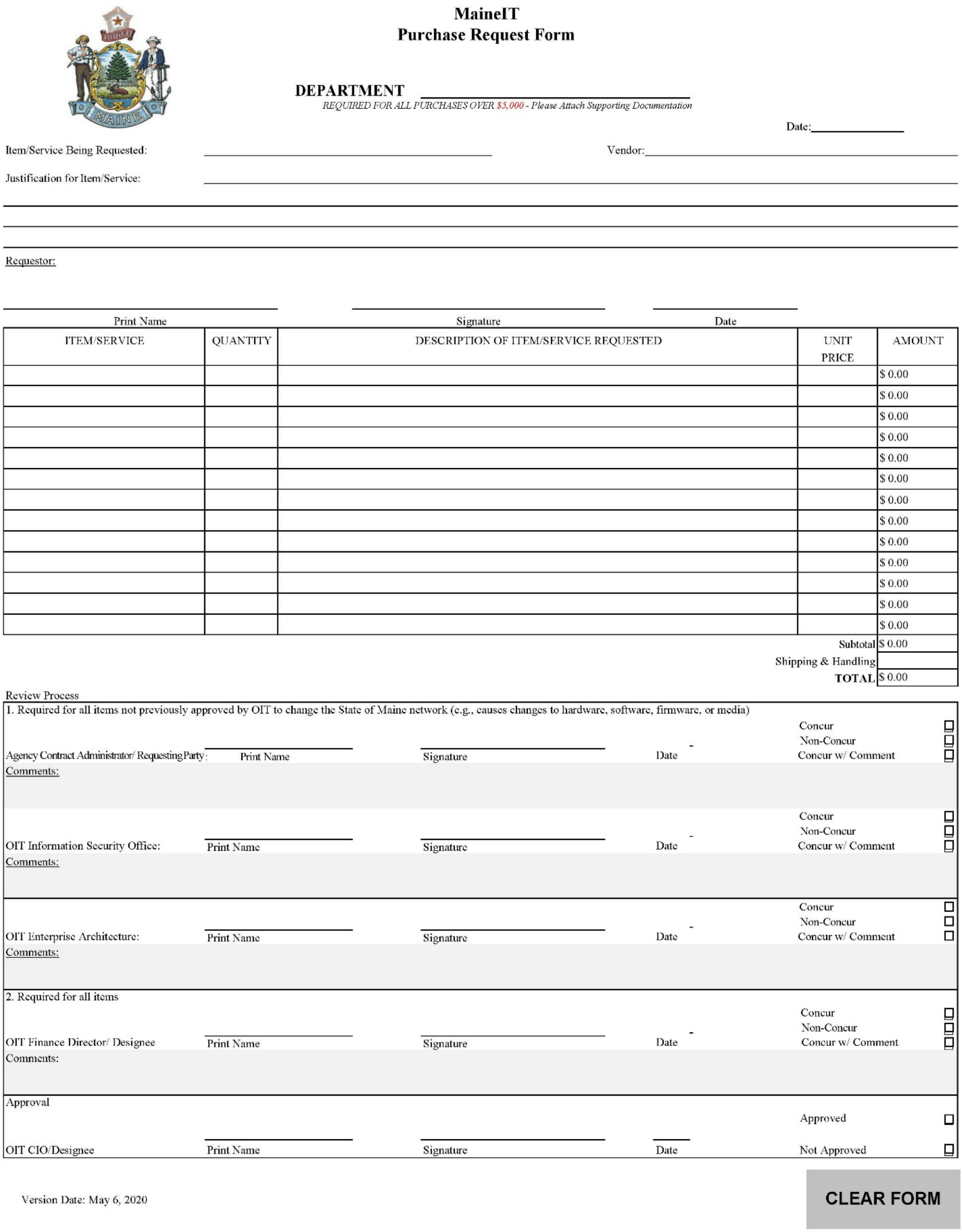
[36] http://legislature.maine.gov/legis/statutes/10/title10sec1347.html

accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

13.13 *Traffic Light Protocol (TLP)*: The Cybersecurity and Infrastructure Security Agency (CISA) Traffic Light Protocol (TLP) used by OIT for the classification of PII impact level. OIT's four data, communication, or network classification levels are Public (TLP: White), Internal (TLP: Green), Sensitive (TLP: Amber), and Restricted (TLP: Red). (See Risk Assessment Policy and Procedure (RA-1))[37]

[37] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/risk-assessment-policy-procedure.pdf

APPENDIX A: OIT PURCHASE REQUEST FORM



MaineIT
Purchase Request Form

DEPARTMENT ______________________________

REQUIRED FOR ALL PURCHASES OVER $5,000 - Please Attach Supporting Documentation

Date:______________

Item/Service Being Requested: ______________________________ Vendor:______________________________

Justification for Item/Service: ______________________________

____

____

Requestor:

______________ Print Name ______________ Signature ______________ Date

ITEM/SERVICE	QUANTITY	DESCRIPTION OF ITEM/SERVICE REQUESTED	UNIT PRICE	AMOUNT
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
				$ 0.00
			Subtotal	$ 0.00
			Shipping & Handling	
			TOTAL	$ 0.00

Review Process

1. Required for all items not previously approved by OIT to change the State of Maine network (e.g., causes changes to hardware, software, firmware, or media)

Agency Contract Administrator/ Requesting Party: ______________ Print Name ______________ Signature Date -

Concur □
Non-Concur □
Concur w/ Comment □

Comments:

OIT Information Security Office: ______________ Print Name ______________ Signature Date -

Concur □
Non-Concur □
Concur w/ Comment □

Comments:

OIT Enterprise Architecture: ______________ Print Name ______________ Signature Date -

Concur □
Non-Concur □
Concur w/ Comment □

Comments:

2. Required for all items

OIT Finance Director/ Designee ______________ Print Name ______________ Signature Date -

Concur □
Non-Concur □
Concur w/ Comment □

Comments:

Approval

OIT CIO/Designee ______________ Print Name ______________ Signature ______ Date

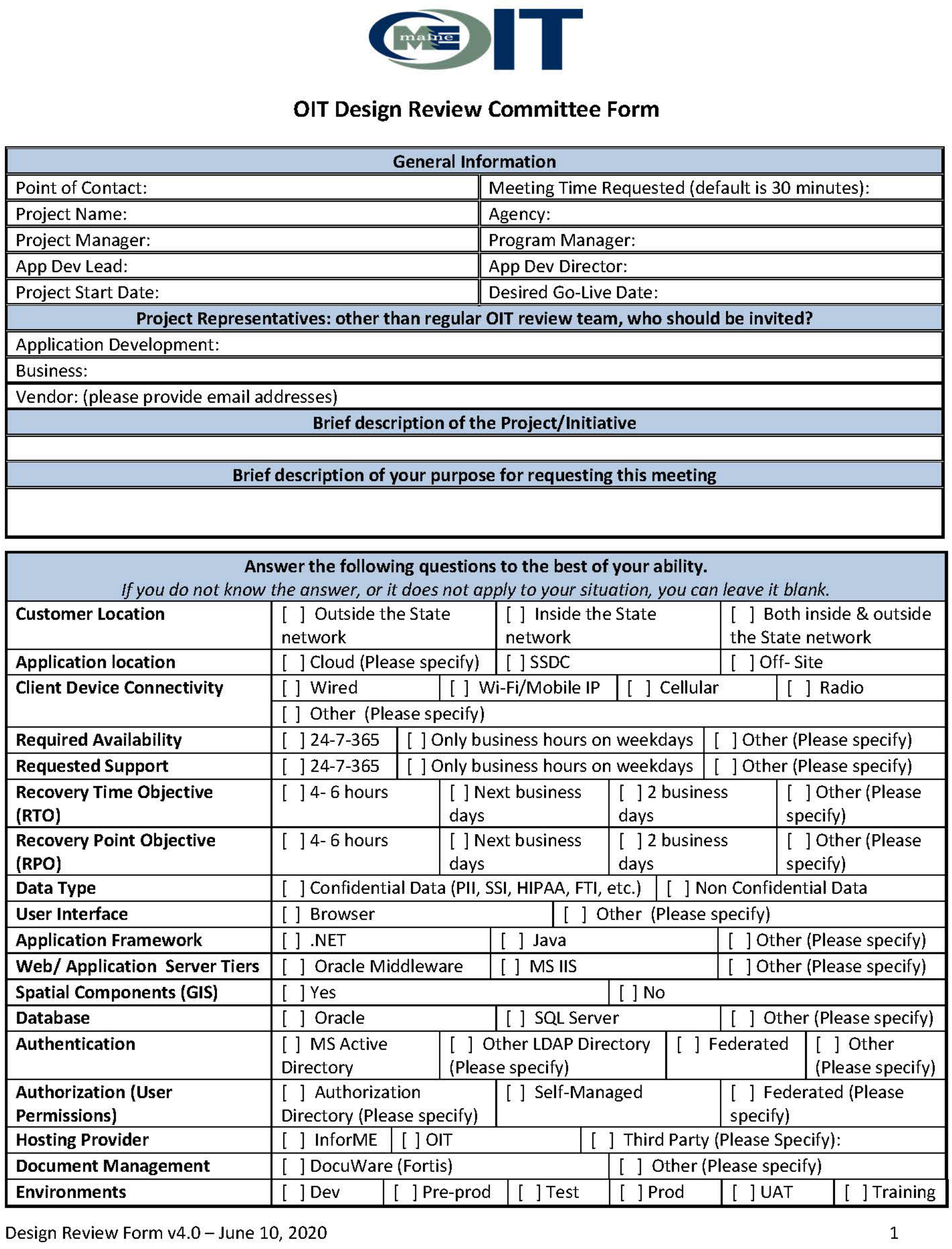
Approved □
Not Approved □

Version Date: May 6, 2020

CLEAR FORM

A fillable form is available on request from the OIT Finance Director.

APPENDIX B: OIT DESIGN REVIEW COMMITTEE FORM



OIT Design Review Committee Form

General Information	
Point of Contact:	Meeting Time Requested (default is 30 minutes):
Project Name:	Agency:
Project Manager:	Program Manager:
App Dev Lead:	App Dev Director:
Project Start Date:	Desired Go-Live Date:
Project Representatives: other than regular OIT review team, who should be invited?	
Application Development:	
Business:	
Vendor: (please provide email addresses)	
Brief description of the Project/Initiative	
Brief description of your purpose for requesting this meeting	

Answer the following questions to the best of your ability. *If you do not know the answer, or it does not apply to your situation, you can leave it blank.*						
Customer Location	[ ] Outside the State network	[ ] Inside the State network	[ ] Both inside & outside the State network			
Application location	[ ] Cloud (Please specify)	[ ] SSDC	[ ] Off- Site			
Client Device Connectivity	[ ] Wired	[ ] Wi-Fi/Mobile IP	[ ] Cellular	[ ] Radio		
	[ ] Other (Please specify)					
Required Availability	[ ] 24-7-365	[ ] Only business hours on weekdays	[ ] Other (Please specify)			
Requested Support	[ ] 24-7-365	[ ] Only business hours on weekdays	[ ] Other (Please specify)			
Recovery Time Objective (RTO)	[ ] 4- 6 hours	[ ] Next business days	[ ] 2 business days	[ ] Other (Please specify)		
Recovery Point Objective (RPO)	[ ] 4- 6 hours	[ ] Next business days	[ ] 2 business days	[ ] Other (Please specify)		
Data Type	[ ] Confidential Data (PII, SSI, HIPAA, FTI, etc.)	[ ] Non Confidential Data				
User Interface	[ ] Browser	[ ] Other (Please specify)				
Application Framework	[ ] .NET	[ ] Java	[ ] Other (Please specify)			
Web/ Application Server Tiers	[ ] Oracle Middleware	[ ] MS IIS	[ ] Other (Please specify)			
Spatial Components (GIS)	[ ] Yes	[ ] No				
Database	[ ] Oracle	[ ] SQL Server	[ ] Other (Please specify)			
Authentication	[ ] MS Active Directory	[ ] Other LDAP Directory (Please specify)	[ ] Federated	[ ] Other (Please specify)		
Authorization (User Permissions)	[ ] Authorization Directory (Please specify)	[ ] Self-Managed	[ ] Federated (Please specify)			
Hosting Provider	[ ] InforME	[ ] OIT	[ ] Third Party (Please Specify):			
Document Management	[ ] DocuWare (Fortis)	[ ] Other (Please specify)				
Environments	[ ] Dev	[ ] Pre-prod	[ ] Test	[ ] Prod	[ ] UAT	[ ] Training

APPENDIX B: OIT DESIGN REVIEW COMMITTEE FORM

Answer the following questions to the best of your ability. *If you do not know the answer, or it does not apply to your situation, you can leave it blank.*	
1. Is the application certified for virtualization? What is the preferred virtualization platform? Specify the vendor, the product, and the version of the virtualization platform.	[ ] Yes [ ] No [ ] N/A
2. What are the quantities of servers, clients and others?	
3. What is the estimate of inside LAN bandwidth use (Throughput – mb/s)? What is the estimate of outside firewall bandwidth use (Throughput – mb/s)?	
4. What is the total number of users? 5. What is the number of concurrent users?	
6. Are there any specific networking or load-balancing requirements for this application? If yes, please describe.	[ ] Yes [ ] No [ ] N/A
7. Is this application certified for external storage? Please specify the vendor, the product, and the version of the external storage.	[ ] Yes [ ] No [ ] N/A
8. Are there batch jobs transferring large amounts of data? If so, when do they run (e.g., during the production day, in the evening)?	[ ] Yes [ ] No
9. What are the acceptable maintenance windows post go-live?	
10. Are there any known business periods we need to avoid?	
11. What is the scope of impact (e.g., application changes needed, testing required)	
12. What are the drivers for the change/addition? (e.g. security, out of compliance, new functions)	
13. What are the implications to the end users/business community?	
14. Are you compliant with the State I.T. Accessibility requirements, http://maine.gov/oit/accessibility? If not, please review.	
15. Are you compliant with Deployment Certification Policy, https://www.maine.gov/oit/policies/Infrastructure-Deployment-Certification.pdf? If not, please review.	
16. Are you compliant with State Enterprise Architecture, http://maine.gov/oit/architecture? If not, please review. *If you have an architectural drawing, please share in advance of the meeting.*	

List any other technologies required for this application that were not mentioned above.	
Technology (Vendor, Product, & Version)	**Purpose**
Example: Varonis, Data advantage and DataAlert	Example: Satisfy many of the requirements prescribed by SOX, HIPAA, PCI, GLB, FERC/NERC, and more.

1.0 REQUIREMENTS

1.1 All Cloud Service Provider (CSP) vendors must meet minimum security standards and annually report and document their compliance posture. These vendors include those providing Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS). The minimum essential security standards that must be considered for the acquisition of IT systems and services include the following:

1.1.1 OIT Information Security Policy[38]
1.1.2 OIT Hosting and Housing Policy[39]
1.1.3 OIT Application Deployment Certification Policy[40]
1.1.4 OIT Application Deployment Certification Handbook[41]
1.1.5 OIT Remote Hosting Policy[42]
1.1.6 OIT Software Development Lifecycle Procedure[43]
1.1.7 OIT Software Development Lifecycle Policy[44]
1.1.8 OIT Change Management Policy[45]

1.2 All CSPs that receive, process, store, or transmit data types categorized as TLP: Amber or TLP: Red must submit one of the following, or combination thereof, acceptable third-party audit certificate of certification or reports:

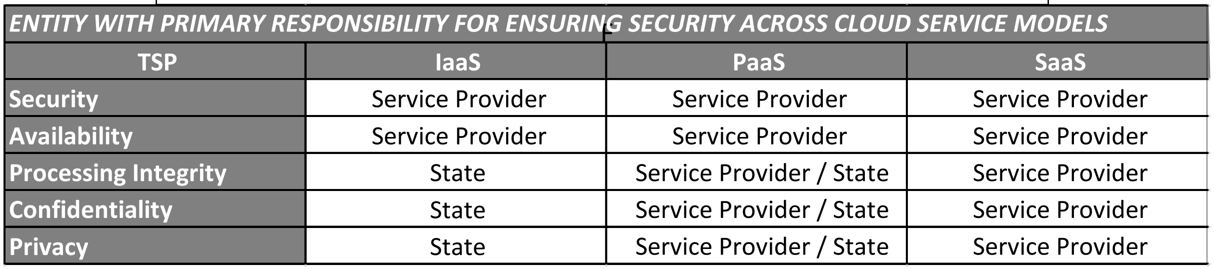
1.2.1 FedRAMP certification in accordance with the appropriate data impact level (High, Moderate, or Low) as determined by the State and Vendor;
1.2.2 ISO/IEC 27001 certification; or
1.2.3 Service Organization Control (SOC) 2 Type II audit report with the appropriate trust principles.

1.3 For SOC 2 Type II audits, OIT and the agency will determine which of the five trust principles will be required (Security, Availability, Processing Integrity, Confidentiality, and Privacy). However, general guidance of the trust principles required based on the type of cloud service provided are listed in Figure 1.

[38] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/information-security-policy.pdf
[39] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/hosting-housing-policy.pdf
[40] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf
[41] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification-guidelines_1.pdf
[42] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/remote-hosting-policy.pdf
[43] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-procedure.pdf
[44] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-policy.pdf
[45] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/change-management-policy.pdf

APPENDIX C: CLOUD SERVICE PROVIDER SECURITY

Figure 1: Responsibility for Security Across Cloud Service Models



ENTITY WITH PRIMARY RESPONSIBILITY FOR ENSURING SECURITY ACROSS CLOUD SERVICE MODELS			
TSP	IaaS	PaaS	SaaS
Security	Service Provider	Service Provider	Service Provider
Availability	Service Provider	Service Provider	Service Provider
Processing Integrity	State	Service Provider / State	Service Provider
Confidentiality	State	Service Provider / State	Service Provider
Privacy	State	Service Provider / State	Service Provider

1.4 While a vendor is not necessarily required to address all five of the Trust Services Criteria in its SOC 2 audit report; it should include the categories that are relevant to the services they are providing to State of Maine (SOM) agencies.

1.4.1 Security – In a non-privacy SOC 2 engagement, the security category must be included. Security is the common criteria that applies to all engagements and is what the other Trust Services Criteria are based off of. The security category addresses whether the system is protected (both physically and logically) against unauthorized access.

1.4.2 Confidentiality - If the services the vendor offers deal with sensitive data, such as *Personally Identifiable Information* (PII) or Protected Health Information (PHI), the confidentiality category should be present in their SOC 2 audit report. The confidentiality principle addresses the agreements that the vendor has with clients in regard to how the vendor uses SOM information, who has access to it, and how the vendor protects it. *Is the vendor following its contractual obligations by properly protecting SOM information*?

1.4.3 Availability – *Is the vendor ensuring that the system they provide SOM agencies is available for operation and used as agreed?* Availability addresses whether the services a vendor provides are operating with the type of availability that a SOM agency would expect. The availability category typically applies to companies providing colocation, data center, or hosting services to their clients.

1.4.4 Processing Integrity - If the services a vendor provides are financial services or e-commerce services and are concerned with transactional integrity, processing integrity is a category that should be included in the SOC 2 report. *Are the services the vendor provides to SOM agencies provided in a complete, accurate, authorized, and timely manner? Is the vendor ensuring that these things are happening?*

1.4.5 Privacy – Privacy is distinct from the other four and usually is in a separate report. The privacy category really stands on its own, as it specifically addresses how a vendor collects and uses consumers' personal information. It ensures that the vendor is handling client data in accordance with any commitments in the entity's privacy notice as committed or agreed, and with criteria defined in generally accepted privacy principles issued by the American Institute of Certified Public Accountants (AICPA).

1.5 CSPs are responsible for the costs associated with fulfilling the audit requirements.

1.6 OIT and the CSP will establish an agreed-upon timeline for the initial audit and report deliverables. The timing of a SOC 2 Type II audit should begin no later than 12 months after production data is utilized (i.e. if production data is used in the test environment, the SOC 2 Type II clock starts). However, an audit for a new service may take place no later than 18 months after initial purchase.

1.7 The SOC 2 Type II audit period should cover the following 12 months. The completed SOC 2 Type II report should be provided to the OIT Information Security Office within three months after the audit period.

1.8 A SOC 2 Type II audit must be completed annually thereafter and the results provided to the State.

1.9 Absent a SOC 2 Type II, a *SOC 2 Type I* will be provided. OIT and the CSP will establish an agreed-upon timeline for the initial audit and report deliverables. The timing of a SOC 2 Type I audit should begin no later than 4 months after production data is utilized (i.e. if production data is used in the test environment, the SOC 2 Type II clock starts).

1.9.1 Because a SOC 2 Type I is as of a point-in-time, if a service organization has their controls in place and documented, an examination may be performed right away, and a report generated. This report should be provided to the ISO for review.

1.9.2 If controls are not in place, a pre-assessment or readiness assessment should be completed first and then a period of remediation will generally follow. Once controls are designed and in place, then the walkthroughs/testing of those controls can take place and a report generated. This report should be provided to the ISO for review.

1.10 If a vendor is unable to meet any of the above requirements a waiver will be required by the ISO.

1.11 An ISO waiver will be required for:

1.11.1 Contracts with CSPs for a SOC 2 Type II audit that does not include all five trust principles to document the approval of the trust principles used;

1.11.2 Contracts with CSPs that do not have a SOC 2 Type II which exceed the 12 months after production data is utilized;

1.11.3 Contracts with CSPs, absent a SOC 2 Type II that do not have a SOC 2 Type I which exceed the 4 months after production data is utilized; or

1.11.4 Any determination that cloud services should be classified as TLP: White or Green (low impact level), and therefore not subject to the third-party audit requirements.

1.12 Agencies may request a third-party audit of a CSP for certain data types that are not categorized as TLP: Amber or TLP:Red, if the Agency determines that the service supports an essential business function.

1.13 SaaS vendors cannot use IaaS certification unless the application is explicitly covered as part of the IaaS assessments.

1.14 The CSP is required to plan, implement and communicate the status of corrective actions taken/planned to remediate any identified vulnerabilities.

1.15 The final third-party security review or certification requirements to be met by the vendor, and the date to meet this requirement, will be determined as a function of delivery method and date of the service provided. However, the audit or certification plan must be to the satisfaction of the ISO and be specified in the contract.

1.16 All third parties and providers of external information system services must define and document how they are compliant with statewide information security controls, including user roles and responsibilities and compliance auditing and reporting requirements.

1.17 OIT reviews and monitors all services, outputs and products provided by third parties at least on an annual basis.