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

Application Deployment Guidelines and Procedures

1.0   Purpose

1.1   This document is designed to act as guidelines for the implementation of the State of Maine Application Deployment Certification policy.[1]

1.2   See Appendix A for a Deployment Communication Guide/Plan for teams to assure stakeholders are informed.

2.0   Definitions

2.1   *State of Maine (SOM) Application:* A computer program, either specifically created or configured, to assist State of Maine users to perform a useful business function.

2.2   *Commodity Application:* Commercial-off-the-shelf (COTS) computer program, either consumed from the cloud or installed on a client device, that was not created or configured for any State of Maine-specific utility.

2.3   *Application Owners*: With respect to the application considered for deployment, the Executive Sponsor, Product Manager, and Product Owner are jointly and collectively identified as the Application Owners. If any of the roles is vacant, the same person fulfils more than one role, or there is a difference-in-opinion with respect to this Procedure among the three roles, for this Procedure, the decision of the Executive Director, Enterprise Shared Services, will be final and binding.

    2.3.1   *Executive Sponsor* is the Agency Partner representative that has the accountability for the strategic direction and budget of the program within the Agency that the application supports.

    2.3.2   *Product Manager* is the OIT representative who works with the Agency Partner whose responsibilities include that the business objectives of an application are met.

    2.3.3   *Product Owner* is the Agency Partner representative with the authority to determine the business objectives of an application and the priority of the product features that are developed.

2.4   *Product Tester:* is one or more designee of the Product Manager and the Product Owner whose responsibilities include testing and validation of the performance, security, accessibility, and functionality of the application.

---

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

2.5   *Project Manager (PM):* is the DAFS representative whose responsibilities do not include certification of the deployment of the application. Their responsibilities are coordination and completion of application releases (including managing budget, scope, and schedule targets) when the Application Owners have mutually agreed upon the deliverables.

2.6   *Vendor Product Manager:* is the vendor representative for a purchased application, responsible for the product roadmap, release plan and application features. This may include Commercial off the Shelf (COTS), Software as a Service (SaaS), subscriptions, and other vendor managed and maintained technology solutions.

2.7   *Chief Information Security Officer (CISO):* is the State of Maine Chief Information Security Officer or designee.

2.8   *Recovery Point Objective (RPO):* The capability to restore data completely to its status at the time of the last valid backup, measured in hours. RPO limits how far to roll back in time and defines the maximum allowable data loss for the Application in the event of a catastrophic failure. It is determined collaboratively with the Product Owner.

2.9   *Recovery Time Objective (RTO):* The time it takes to recover the application, measured in hours. It defines the maximum downtime before there is significant business impact. RTO represents how long it takes to restore from the incident until normal operations are available. It is determined by the Product Owner.

2.10   *Support Model:* A collection of documented methods and resources used by the Application Owners to provide and manage end-to-end service and product delivery following deployment.

3.0   Applicability
3.1   This process applies to all State of Maine applications as described in the [Application Deployment Certification Policy](#).[2]

4.0   Roles and Responsibilities
4.1   IT Directors: Enforce this Policy and determine applicability.

4.2   Application Owners: The Application Owners are responsible for ensuring appropriate tests are conducted, determining who should perform each test, and defining and documenting the support model. This certification consists of:
    4.2.1   The names and signatures of the Product Manager, Product Owners, and the Executive Sponsor.
    4.2.2   A summary result (Passed/Failed/Not Applicable) and a short paragraph clarifying that summary result, for each of the tests specifiedbelow, and the location of the test results.
    4.2.3   An outline of the defined support model for the application.

---

[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ApplicationDeploymentCertification.pdf

4.3   Product Managers: The Product Managers are required to document applications into the Enterprise Application Inventory.

4.4   Testing
    4.4.1   Any part of the testing required by this policy may be outsourced to a third-party without affecting the responsibility or the prerogative of the Application Owners. Irrespective of who executes a test, the Application Owners remain in charge of its execution. The Application Owners are not answerable to the third-party regarding the nature or the result of any outsourced test. Further, the third-party exclusively conveys the test results directly back to the Application Owners.
    4.4.2   For OIT–Hosted applications, Application Owners will designate State personnel who will perform assigned applicable application tests.
    4.4.3   For Remote-Hosted applications, it is a generally a combination of vetting vendor provided test results and State personnel performing applicable tests. If that vendor provided results for a specific application test are deemed acceptable by the Applications Director and subject matter experts (Chief Information Security Officer for Security, etc.), no further State personnel testing is required for that item. Should there be deficiencies, then additional testing must be conducted by either the vendor or by State personnel, until acceptable results are achieved.

4.5   Executive Director, Enterprise Shared Services: Owns and interprets this Procedure.

4.6   Chief Information Officer (CIO): The CIO may delegate authority to certify or approve applications for deployment. Regardless of approving authority, certification of applications will be based on advice from any Director, and/or other subject matter experts.

4.7   MaineIT Accessibility Team: performs accessibility testing, assesses vendor-provided accessibility testing results (Accessibility Conformance Reports (ACRs) or equivalent reports), determines pass/fail results.

5.0   Guidelines
5.1   For any net-new application deployment certifications and retention of documentation, Atlassian/Confluence will be the de-facto proxy for retaining ALL deployment certification documentation. If a different proxy is being requested, the business case burden to justify the use of a non-standard product (Atlassian/Confluence) involves a decision through communication with the Executive Director of Enterprise Shared Services.

5.2   Details & Considerations prior to testing:
    ➢   Defining how many users? (internal, external, 1 or more user groups?)
    ➢   What is the classification[3] of the data being transacted?
    ➢   Is the app, or are components of the app public facing?
    ➢   What is the mission criticality of the app?
    ➢   If a test or scan reveals that a Waiver[4] is needed, plan a minimum of 3 weeks lead time after waiver submission.

---

[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/Waiver.pdf

> ➢ Does any of the data contain or move/push PII outside of the application (data staging[5]) and how will this be handled to ensure confidentiality, integrity and availability?
> ➢ Detail out a Responsible, Accountable, Consulted, Informed (RACI) Matrix: This is designed as a tool to help inform stakeholders of their direct or indirect involvement in deployment certification. It is important that only one Role is identified as the Accountable party for each deliverable.

	Roles					
	Role A	Role B	Role C	Role D	Role E	Role F
Tasks						
Determine need and/or scope for testing						
Schedule test activities						
Define the test						
Review validity of tests						
Execute tests and document results						
Verify test results						
Approve test results as acceptable for production release						
Communication Plan						
Support Model						

Legend:
  I.   R = Party responsible for performing the work activity.
  II.   A = Party held accountable for validating the work is completed as defined.
  III.   C = Party consulted on the work activity, providing input and/or information.
  IV.   I = Party informed of the results or outcomes of the work activity.

---

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

Example RACI Matrix for UAT (User Acceptance Testing)

Example Tasks:	Example Roles					
	Project Manager	Product Manager	Business SME(s)	Business Executive Sponsor	IT Team	IT Director
Determine need and/or scope for UAT	I	R	C	A	C	I
Schedule UAT activities	R	A	I	I	C	I
Define UAT	C	A	R	I	C	I
Review validity of tests						
Execute tests and document results	I	I	R	I	C	A
Verify test results				A	R	
Approve test results as acceptable for production release	I	R	C	A	I	I
Communication Plan	R	C	C	C	I	A
*Support Model	N/A	N/A	N/A	N/A	N/A	N/A

*NOTE: You may identify that not every task listed is needed for every test guideline. The goal here is each task is intentionally thought about and communicated within the team.

5.3   **Testing guidelines**

    5.3.1   **User Acceptance Test (UAT):** Ensures functioning of all application features are fit for use.
   - ➢ Factors to consider determining when/if UAT is required:
      1. Were any significant capabilities or functions added and/or changed? (ex. Bug fixes)
      2. Were any significant ancillary functions or commodity applications added and/or changed? (ex. Word, Adobe, Outlook, etc.)
   - ➢ What is the support model for User Acceptance testing and capturing the results?

    5.3.2   **Accessibility Test:** Ensures compliance with the OIT accessibility policies and standards.
   - ➢ As early in the process as possible, review the Digital Accessibility Policy[6] with the team and determine if an accessibility assessment is required.

---

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

1. If an assessment is needed, engage with the MaineIT Accessibility Team through a [ticket on the Enterprise Ticketing System](#).[7]
2. An assessment typically is not needed if the application has no user interface (UI) or if the deployment does not modify the UI.

➢ Determine whether a vendor Accessibility Conformance Report (ACR) (also known as a completed VPAT) or equivalent report is available.
1. If so, submit a request for the ACR or equivalent report to be assessed.
2. If not, submit a request for an accessibility test. For test requests:
    o   Securely provide the MaineIT Accessibility Team with logon credentials and provide appropriate permissions for testing.

➢ Provide as much lead time as possible when making a request. The amount of time required to perform a test may be impacted by the number of requests in the testing queue.

➢ If findings are unable to be remediated prior to deployment, a [Waiver](#)[8] will be needed, plan a minimum of 3 weeks lead time after waiver submission.

➢ What is the support model for Digital Accessibility testing and capturing the results? (This can be as simple as the vendor has agreed to uphold the requirements of the [Digital Accessibility Policy](#)[9])

5.3.3   **Data Conversion and Migration Test:** Ensures the accurate migration of appropriate data.
➢ Definitions:
1. Data Conversion: The process of changing data from one format to another so that it can be used with a different system, application, or storage method.
2. Data Migration: The process of moving digital information from one location, file format, environment, storage system, database, datacenter, or application to another.

➢ Is the data source of truth and actual data moving to a different host/platform/tech (e.g. Footprints to Assyst, Subversion to GitHub)?

➢ Are any components (e.g. application, hosting platforms, or backend databases across the same platform) whole or in part migrating to a new host? If true, data conversion and migration testing is required.

➢ Is the application code repository migrating to a new host/platform?

➢ If Data Conversion and/or Migration is occurring, has a plan/strategy been drafted, reviewed and approved with all involved? Some items to consider when planning include:
1. How will validation be accomplished; manually, scripted, tool based?
2. Will the conversion and /or migration be incremental, iterative, all at once, etc.?
3. Will it require active monitoring or only validation when complete?
4. How will the final validation occur, manual compares (e.g. pre/post), scripts, tool based or other?

---

[7] https://maineitservices.maine.gov/assystnet/application.jsp#serviceOfferings/800

[8] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/Waiver.pdf

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

5. Is there a freeze (code, data, etc.) in place to allow migration to complete without impacts? If not, will additional validation steps be required?
6. Please refer to 5.3.6 for guidance on additional potential testing needs.

➢ What is the support model for Data Conversion/Migration testing and capturing the results?

5.3.4 **Interfaces Test:** Few applications exist in isolation, and many business processes depend on the data that flows into and out of an application just as much as the functionality of the application itself. Therefore, interface testing is just as important as other types of testing, and with the additional involvement of a third party, it also comes with additional challenges.

➢ Have interface requirements/criteria been defined and communicated through a RACI matrix/table? Ensure third party application owners are included in the RACI and the requirements are in line with any data sharing agreement.

➢ Factors that determine whether an interface needs to be tested for deployment:
1. Was an interface directly modified in any way?
2. Was functionality in the application modified that could affect the data in the interface?
3. If so, how high is the confidence level that the third-party system can accept the new data?

➢ Items to discuss and agree upon with third party application owners before conducting interface tests:
1. Project timelines, especially deadlines and dependencies that affect interfaces.
2. Turnaround time expectations.
3. How test data is kept separate from production data.
4. Test scenarios that must be included in test data.
5. Ensure that interfaces meet performance expectations.
6. How sign-off on successful test completion will be obtained and documented.

5.3.5 **Security Test:** Ensures the confidentiality, integrity, and availability of the application.

➢ Have Security requirements/criteria been defined through collaboration with the Security Operations Center (SOC) Vulnerability Management team, if applicable, the IT Director responsible for the Infrastructure Deployment, and communicated with the larger team? These requirements may include any form of operationalization, communications, and support models.

➢ Review/complete RACI table for Security Test.

➢ Has the vendor agreed to the Data Classification Policy[10] and Vulnerability Scanning Procedure?[11]

---

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

➤ If vendor hosted, ideally the Vendor will provide their own authorized security scan (SOC 2 Type II or other security document) for the SOC team to review. Submit through this workflow [Third Party Vulnerability Scan Reviews ticket](#).[12]
   1. If this isn't possible, the scan engine IP address needs to be whitelisted at <u>all security controls</u> and the SOC Vulnerability Management team member running the scan needs admin access to the application.
➤ All security scans follow this [Application Scans ticket workflow](#).[13] You will need to fill in several data points when requesting this scan. Commonly confused areas include:
   • "Scan Type"
      o Initial: This is the 1st scan for a specific implementation of application or web service.
      o Follow-up: This is for a scan that has already been performed and requires follow-up.
   • "This is for:"
      o Audit: For audits.
      o Baseline: For new applications or applications that have never been deployed in the State environment. This allows vendors/staff to make changes needed to get ready for deployment(s).
      o Deployment Certification: This is for deployment certifications ensuring all items are ready to move to production.
➤ Make sure to give 2-3 weeks lead time for scans to be performed by the SOC Team.
➤ After a scan is completed, the ticket will be updated with results by the SOC Team. App Dev then needs to evaluate the results and come up with a remediation plan, if needed. If the App is owned by a Vendor, the App Dev team should work with the Vendor to create this remediation plan.
   1. Validate findings. Any questions related to the findings, reach out through the ticket to SOC. If there are no questions, close out the ticket.
   2. Remediate the findings, or apply for a waiver. This may include meetings will all relevant stakeholders.
   3. If a follow up scan is needed, submit a new ticket.
➤ If findings are unable to be remediated, a [waiver](#)[14] will be needed. Plan a minimum of 3 weeks lead time after a complete submission and acknowledgement.
➤ What is the support model for future Security testing on/with the App and capturing the results?

5.3.6 **Performance Test:** Ensures responsiveness under projected average and peak processing loads.
   ➤ Have performance requirements/criteria been defined and communicated through a RACI matrix/table.

---

[12] https://maineitservices.maine.gov/assystnet/application.jsp#services/516
[13] https://maineitservices.maine.gov/assystnet/application.jsp#services/519
[14] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/Waiver.pdf

- ➢ Will the state or a vendor do the testing?
    1. If vendor, review the vendor's test results for quality. If the vendor test is deemed insufficient, the State may need to perform its own test.
    2. If state, factor in time and potential cost for doing load tests. If engaging the load testing team, has the Product Owner agreed to any associated expenses and timeline(s).
- ➢ Factors for testing:
    1. Test script development
    2. Enhancements
    3. Test data validation
    4. Test executions
    5. Analysis
- ➢ Business is required to supply testing information/criteria for the Performance Team to verify and use.
- ➢ While the testing schedule is ultimately determined by the Application Director, it is good practice to perform these tests any time a change is made (see 5.3.8 Regression Test) that could affect performance.
- ➢ What is the support model for Performance testing and capturing the results?

5.3.7 **Restoration Test:** Ensures full functioning of the application following an infrastructure rollback/restoration.
- ➢ Have the Restoration testing requirements been defined and communicated through a RACI matrix? Is this on-prem, in the cloud, or hybrid? What are the RTOs and RPOs?
- ➢ Application Owners are responsible for ensuring that restoration testing has been completed but not necessarily doing the testing.
- ➢ Often times this is through 3rd party or Vendor artifacts (Disaster Recovery Plans, etc.)

5.3.8 **Regression Test:** Applies exclusively to modifications of existing applications. Ensures that the new version does not compromise existing functionality.
- ➢ Have the Regression testing requirements been defined and communicated through a RACI Matrix?
    1. Ensure alignment between Application Owner, Vendor (if applicable), and State App Dev Team in advance of test execution.
- ➢ Create test cases which build a test suite that minimally confirms core functionality of application, but the more robust the better. State App Dev Team or the Vendor execute these tests.
    1. Added test results should be included to the test suite as the developing process continues for enhancements or bug fixes.
- ➢ Document and review results with artifacts to prepare for leadership signoff getting ready for production.
- ➢ Regression testing can be fully automated, manual or a mix of both.

5.3.9 **End-to-End Test:** Ensures proper functioning of the application across all combinations of relevant hardware and software components. This may be inclusive of a Platform Test, as applicable.

- ➢ Have End-to-End testing requirements been defined and communicated through a RACI Matrix?
- ➢ Factor in user involvement to get their perspective for simulating typical operations the application can perform.
- ➢ Testing lifecycle:
    1. Test planning
    2. Test design
    3. Test execution
    4. Results analysis
- ➢ End-to-end testing can be fully automated, manual or a mix of both.
- ➢ It is left to the IT Director's (or designee's) discretion to determine exactly what constitutes an 'End-to-End' test.
- ➢ What type of test environment is required for this (production-like, test, etc.)?

6.0   Document Information
6.1   Initial Issue Date: March 14, 2011
6.2   Latest Revision Date: February 5, 2025
6.3   Point of Contact: Enterprise.Architect@Maine.Gov
6.4.   Distribution: Internet[15]

---

[15] https://www.maine.gov/oit/policies-standards

Appendix A. Communication Plan

The process should include establishing "who" needs to be notified, "what" will be communicated, "how" we will communicate it (e.g. RFC's, emails, etc.), "who" is responsible for the communication, and "when" those changes will be communicated.

Who needs to be notified	What is being communicated	How will this be communicated	Who is responsible for communication	When (Frequency)
IT Leadership	• Communication Plan (RACI/Appendix A)			
Application Teams/ Agency	• High Level Timeline • Communication Plan			
Application Teams/ Agency	• Granular communications: • Impact of Deployment • RFC's • Schedule Details • Support Model • Point of Integrations			
Key Stakeholders/ Vendors/Staff	• Cadance Briefings • High Level Timeline			
Agency/ Organization	• Cadance Updates			

*Retain a copy of these communications for historical purposes in the chosen deployment certification documentation repository. See 5.1 above for more information on documentation repositories.