Salesforce Governance: Details

1.0. Purpose

This document specifies the governance for Salesforce within the State of Maine (SOM) Executive Branch, including the roles and responsibilities of the various parties. There are also two additional documents, one containing background information, and the other containing the executive summary. The background document constitutes essential pre-requisite for this document. It is strongly suggested that the background document be read prior to this detailed governance document. The executive summary document showcases the essential highlights from this document.

2.0. Salesforce Governance Committee

2.1. The SOM Executive Branch maintains a standing *Salesforce Governance Committee* to oversee all aspects of Salesforce within the Executive Branch, under the authority of the State of Maine CIO. The following persons/roles/designates are members of the Salesforce Governance Committee:

- OIT Enterprise Architect (Committee Chair)
- OIT Executive Director, Enterprise Shared Services
- Any OIT Application Director with investment in Salesforce
- Agency business representatives from each Salesforce application (either already live, or in development, or under serious consideration).

3.0. Governance Directives

3.1. The only way in which a net-new Salesforce application comes into the SOM Executive Branch is as turnkey SaaS product from a vendor. However, OIT may choose to develop some internal bandwidth to perform post-go-live routine maintenance and Configuration ("Declarative" in Salesforce terminology) changes.

3.2. All net-new Salesforce applications will be developed using the latest Lightning Experience interface only. The legacy Classic interface will not be accepted.

3.3. Org Strategy: When deciding on an Org structure (Single versus Multi versus Shared), a cost-benefit analysis must be performed. The decision criteria is summarized below. A green checkmark (✅) indicates significant advantage. *The Salesforce Governance Committee will make the final recommendation re: whether a Program/App deserves its own Org, or shares an Org with another Program/App.* Under appropriate conditions, the Governance Committee may recommend a shared Executive Branch-wide Org. Any shared Org must have additional architecture oversight from a competent party not affiliated by any of the product vendors sharing that Org. Finally, each Org must have a single Executive Sponsor, chosen from the Agency Business Partners' agency/department.

Criterion	Single Org	Multi Org
Licensing Cost	✅	
Optimization of Security Settings (Record Sharing, Org Wide Settings, Data Model, Data Classification, etc.)	✅	

Salesforce Governance: Details

Criterion	Single Org	Multi Org
Running multiple Projects at the same time		✓
Customizations that may result in running into Org Limits		✓
Greater Management Visibility, such as Roll-Up Reporting, Global drill-down into pipeline & activities, Shared Information/Datasets, etc.	✓	
Maintenance & Backup	✓	
Shared Processes, leading to better Re-use	✓	
Maintenance	✓	
Standardized Processes	✓	
Global Standardization and Economies of Scale, including User Training, Application Release Management, Application Integration, Data Management, etc.	✓	
Re-Use of automated Test Scripts	✓	
Standardization of Change Management Processes and Policies	✓	
Business Units with different regulatory, compliance, security, or privacy requirements		✓

3.4. Org Naming Convention:

- Production: "SOM" followed by a two (2) digit number starting with 01. The following Orgs have been defined so far:
  - SOM01: DHHS-OCFS Child Welfare
  - SOM02: DHHS-OFI to implement Eligibility & Enrollment
- Lower than Production: Production names, suffixed with the appropriate environment type. Examples: SOM01Test1, SOM01Test2, SOM01Staging, SOM01Dev, etc. The number of non-Production environments will depend upon the application/project budget, size, complexity, etc.

3.5. All Orgs must be integrated with the State of Maine Active Directory. Further, Single Sign-on with the Active Directory must be enabled for internal users.

3.6. Each Org may host one or more Programs/Apps serving the same Active Directory group. An Org *never* hosts Programs/Apps that serve disparate/unconnected Active Directory groups.

3.7. Out-of-the-box, Salesforce provides a robust auditing capabilities, including Change

Data Capture[1] and Platform Events[2]. Any data classified as Sensitive (TLP: Amber) or Restricted (TLP: Red) must have its Production Instance audited using the native Salesforce auditing capability. Field history tracking can be established by field, by object, by Org, for up to 20 fields per object, and retention for 18 months. Business use cases that are subject to extra regulatory burden may consider an add-on product, Field Audit Trail[3], which increases the default limits to 60 fields per object, and retention up to 10 years. (See 3.22 below for Salesforce Shield.)

3.8. All lookup lists (Dimensions, in Data Warehousing terminology) must be owned by the entire State of Maine enterprise. Transactional data (Facts, in Data Warehousing terminology) may be owned by individual agencies. Enterprise ownership better facilitates sharing and re-use. Therefore, any data element that is likely to be shared across the enterprise must be owned by the enterprise right from the beginning. *Until an enterprise Master Data Management strategy, this provision will remain aspirational. However, implementing this provision will setup the State of Maine for better data alignment.*

3.9. AppExchange vs. Homegrown Solution: An app from the AppExchange must be considered prior to any Customization ("Programmatic in Salesforce terminology). Only if an AppExchange app does not come close to the use case at hand, or is, for some reason, unsuitable for the Org, should Customization ("Programmatic in Salesforce terminology) be considered. The AppExchange has both free resources and paid resources. *In all instances, adoption of any AppExchange app is subject to approval by the Salesforce Governance Committee.* The following considerations must be weighed in instance:

- Will it, or could it, impact Configuration ("Declarative" in Salesforce terminology) and/or Customization ("Programmatic in Salesforce terminology) in the Org?
- Does the app fit the core business need?
- How many other Orgs are using the app, and the length of time they have been using it?
- How do other Orgs meet the same need?
- What is the app's roadmap?
- What support is available, including documentation and training?
- What is the licensing model of the app?
- Is it a managed, or an unmanaged, package? A managed app is more likely to have a lower lifetime total cost of ownership.

3.10. An essential component of Governance is the perpetual vigilance for deprecated code with third-party Apps. At least once per annum, every Org must undertake a review, and clean-up[4] of legacy customizations.

---

[1] https://developer.salesforce.com/docs/atlas.en-us.change_data_capture.meta/change_data_capture/cdc_intro.htm
[2] https://developer.salesforce.com/docs/atlas.en-us.platform_events.meta/platform_events/platform_events_intro.htm
[3] https://help.salesforce.com/articleView?id=field_audit_trail.htm&type=5
[4] https://developer.salesforce.com/blogs/developer-relations/2017/01/time-clean-unneeded-salesforce-customizations.html

3.11. An essential component of Governance is to minimize complexity.
- The Governance Committee must exercise vigilance re: how complex a Solution is, and whether it includes Custom Coding.
- For instance, are there "lots" of custom objects? A "modest" number of custom objects and derived fields may be acceptable, but "too many" must be identified as a risk. Unfortunately, this is a matter of judgement call that the Governance Committee must exercise through deliberation. Further, the Salesforce Governance Committee will provide a risk mitigation strategy to the Project Sponsor.

3.12. Configuration ("Declarative" in Salesforce terminology) should always be considered first. However, there are situations where the business has a specific requirement that cannot be easily Configured, and Customization ("Programmatic in Salesforce terminology) must be considered. Sometimes, avoiding Customization may lead to excessive complexity. Therefore, instead of a dogmatic stance re: Configuration versus Customization, a better goal is to reduce the overall complexity. In most instances, where Configuration yields lower complexity than Customization, Configuration is the better option. Whereas, in instances where Customization yields lower complexity than Configuration, Customization is the better option. In the end, the goal is to lower Complexity. It *usually* translates to favoring Configuration over Customization. *All Customization ("Programmatic" in Salesforce terminology) requests will be submitted by the Project Sponsor to the Salesforce Governance Committee for approval.*

3.13. Limitations on field counts, document counts, objects, etc. are by the Org[5], and determined by Salesforce during the sale. All such counts can be increased (subject to certain ceilings), but at extra cost.

3.14. Irrespective of Configuration ("Declarative" in Salesforce terminology) versus Customization ("Programmatic" in Salesforce terminology), there may be instances where the only means of implementing a desired workflow is through breaking the standard model of Data Normalization. *Strict scrutiny must be exercised by the Salesforce Governance Committee re: the tradeoffs involved.*

3.15. Irrespective of Configuration ("Declarative" in Salesforce terminology) versus Customization ("Programmatic" in Salesforce terminology), it is mandatory to comply with the Salesforce Naming Conventions.[6]

3.16. Salesforce allows two kinds of relationship between objects: Master-Detail and Lookup.[7] This is a consequential design decision, which ends up affecting complexity, Org limits, and reporting. However, done right, this is one of the most potent tools to extend Salesforce with pure configuration, as opposed to custom coding.

3.17. If Customization ("Programmatic" in Salesforce terminology) cannot be avoided, it is mandatory to comply with the following:

---

[5] https://help.salesforce.com/articleView?id=overview_storage.htm&type=5

[6] https://quip.com/MW5cAPVwat8k#JCIACA8Q963

[7] https://help.salesforce.com/articleView?id=overview_of_custom_object_relationships.htm&type=5

- Apex Design Best Practices[8]
- Execution Governor Limits[9]

3.18. The Optimizer[10] and the Health Check[11] are built-in tools that interrogate an Org for limits and Customizations ("Programmatic" in Salesforce terminology). *Each Org must be subjected to the Optimizer and the Health Check, at commencement, and subsequently, after every customization sprint.*

- Health Check:

Results	Status	Action	Governance Review
90% +	Excellent	Celebrate	Not Necessary
80%–89%	Very Good	Document, and Mitigate, Critical and Warning items	Quarterly
70%–79%	Good		Monthly
55%–69%	Poor		Weekly
<= 54%	Very Poor		Immediately

- Optimizer: The app owner/vendor must either mitigate, or reasonably explain, the items under Immediate Action Required, Action Required, and Review Required. The Optimizer evaluates only the Org metadata, *not* the records, or any other content. Further, the Optimizer does *not* evaluate items installed from managed packages.
- If the application is built with Experience Cloud,[12] then the term "Optimizer" above is also understood to include the Community Builder Page Optimizer.[13]

3.19. Even though the Optimizer provides the most comprehensive report re: customizations, other companion tools provide additional context: Field Trip,[14] Config Workbook,[15] Profile and Permission sets reports, etc.

3.20. Salesforce does *not* allow Site-to-Site Virtual Private Network between Salesforce and the state. However, Salesforce and OIT have jointly agreed upon the narrowest possible range of Internet Protocol addresses on both sides.

3.21. OIT has already created a playbook for email relay between Salesforce and the Maine State Azure Office 365 email. Which means, Salesforce can send and receive email as the Maine.Gov email identity. As of this writing, OIT is also in the process of executing a limited-time pilot for bi-directional calendar synch between Salesforce and the SOM Exchange (email server).

3.22. Security Configurations: Salesforce provides detailed guidance re: data protection and privacy.[16] Here are the highlights:

---

[8] https://developer.salesforce.com/wiki/apex_code_best_practices
[9] https://developer.salesforce.com/docs/atlas.en-us.apexcode.meta/apexcode/apex_gov_limits.htm
[10] https://help.salesforce.com/articleView?id=optimizer_introduction.htm&type=5
[11] https://trailhead.salesforce.com/en/content/learn/modules/security_basics/security_basics_healthcheck
[12] https://www.salesforce.com/products/experience-cloud/overview/
[13] https://developer.salesforce.com/docs/atlas.en-us.communities_dev.meta/communities_dev/community_builder_page_optimizer.htm
[14] https://appexchange.salesforce.com/listingDetail?listingId=a0N30000003HSXEEA4
[15] https://appexchange.salesforce.com/appxListingDetail?listingId=a0N30000000q4evEAA
[16] https://help.salesforce.com/articleView?id=data_protection_and_privacy.htm&type=5

- Salesforce offers a number of profiles[17] that may be used in a particular Org/App. *Each Org shall have at most three System Administrators, one from the staff of the product vendor, one from the staff of the agency/department, and one from OIT.*
- Salesforce Shield[18] is a must if the app transacts in TLP: Red data. The Shield includes three components:
  - Encryption: All TLP: Red data fields must be subjected to Encryption. And, all Encryption will be "Deterministic, Case Insensitive".
  - Field Audit Trail: Any field that is subject to Encryption is also subject to Audit. Unless the number reaches 60, in which case, the Executive Sponsor and the Governance Committee will advise further.
  - Event Monitoring: Must be enabled.
- Org-wide sharing rules must be as restrictive as possible. *More specifically, the Org-wide Sharing Default for any object that contains TLP: Red data must be set to Private.*
- Users must be granted the least privilege in order to accomplish their duties.
- Aggressively leverage role hierarchies.[19] Define hierarchies based upon the actual business needs for users to access the records, and *not* based upon the users' positions in the organization chart (i.e., command chain).
- No user with a role should own more than 10,000 records in an object. Users who need to see that level of information should either not have a role, or be at the top of the role hierarchy.
- No two users should ever share a license.
- Session timeout must be set at 15 minutes of inactivity.
- Generate a new tenant secret at least once per month. This will generate a new encryption key.
- When destroying encryption keys, make sure all data encrypted with that key are decrypted first
- Enable Clickjack Protection[20] for all pages at the level of "Allow framing by the same origin only".
- For any public portal transaction involving TLP: Red data, the public portal user must be subjected to MFA via a time-sensitive, random code emailed to the registered email address.
- All devices accessing Salesforce should have the latest stable operating system, browser version, and an approved anti-malware. Admittedly, this provision cannot be enforced for a public portal application.

3.23. All applications must follow an Agile Software Development Life Cycle (SDLC), as interpreted by the Governance Committee, in consultation with the OIT PMO. Salesforce updates the platform three times a year: Spring, Summer and Winter. The Agile SDLC cadence (whether it is Continuous Integration, or any other kind of

[17] https://help.salesforce.com/articleView?id=standard_profiles.htm&type=5
[18] https://help.salesforce.com/articleView?id=salesforce_shield.htm&type=5
[19] https://help.salesforce.com/articleView?id=admin_roles.htm&type=5
[20] https://help.salesforce.com/articleView?id=siteforce_clickjacking_enable.htm&type=5

defined release strategy) must explicitly accommodate this release schedule, and pre-provision the appropriate number of environments/sandboxes. Special attention must be paid on external interfaces, where the other party (such as the Federal Government) may not provide a non-Production environment.

3.24. The Executive Sponsor of each Org must make a conscious decision whether or not to utilize the native Salesforce social network, Chatter.[21] This is especially critical for programs subject to a Federal compliance mandate, and/or TLP: Red data.

3.25. All interface of the Salesforce app/Org with its partner ecosystem must place the Maine Service Bus as the first position for this service option before considering alternatives.

3.26. All applications must complete the Application Deployment Certification[22] prior to going live into production.

3.27. Salesforce recommends a routine data backup strategy[23] for both the data and metadata. There are multiple solutions available. While every Org/program will make independent judgements, based upon their Recovery Time Objective and Recovery Point Objective, at a minimum, the Steering Committee strongly recommends a point-in-time cloud-to-cloud backup at all major project milestones.

3.28. All major project milestone code versions must be copied to the OIT enterprise source configuration management system.

3.29. All major project milestones, and all production changes, must adhere to the OIT Change Management Policy.[24] Production changes in shared Orgs require explicit buy-in from the Executive Sponsors of both apps/projects, or their designees. All changes must be explicitly signed off by an Org System Administrator. At their discretion, the Org System Administrator may delegate some minor changes to an empowered Superuser or Business Analyst. However, even in those instances, the Org System Administrator is still held accountable for any and all executed changes. Further, all changes, without exception, must be logged as required in the OIT Change Management Policy.

3.30. All Orgs/Projects/Programs must explicitly provision the responsibility of a support plan for post-go-live support, be it through a vendor, or OIT.

3.31. Org Migration: Under rare circumstances, it may be necessary to migrate from one Org to another. This is one of the most difficult tasks under the rubric of Salesforce, and must not be taken lightly. Salesforce provides detailed instructions, including the Overview,[25] and the details of Data Migration.[26] It is strongly recommended that dedicated professional services are provisioned and will be identified to be responsible for this exercise.

3.32. Pre-approved Tools: Here is a listing of Salesforce tools already pre-approved by the Salesforce Governance Committee:

---

[21] https://www.salesforce.com/products/chatter/overview/
[22] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf
[23] https://help.salesforce.com/articleView?id=000334121&language=en_US&type=1&mode=1
[24] https://www.maine.gov/oit/policies/ChangeManagementPolicy.pdf
[25] https://help.salesforce.com/articleView?id=000320503&type=1&language=en_US&mode=1
[26] https://help.salesforce.com/articleView?id=000322219&type=1&language=en_US&mode=1

DevOps	Gearset[27]
Release Management (Continuous Integration)	Flosum[28]
Additional User Interface Features	Vlocity[29]
Agile	Agile Accelerator[30]
Integrated Development Environment	Visual Studio Salesforce Extension[31]
Bulk Upload	Data Loader[32]
Extract-Transform-Load from legacy sources	Talend[33]
Documentation	DocGen[34]
Analytics, Artificial Intelligence	Einstein[35]

3.33. In the long run, there must be a SOM Executive Branch *Salesforce User Group*. This group will share knowledge, FAQs, and actively participate in Ideas[36] (online Salesforce user forum). This SOM Salesforce User Group must also actively monitor usage, including Adoption Key Performance Indicators, Salesforce Features Usage Popularity, etc. The Enterprise Architect will be responsible to facilitate this *Salesforce User Group.*

3.34. Vendor Monitoring: All Salesforce vendors under contract with the SOM Executive Branch must be monitored, and evaluated, based upon the following broad criteria. This is primarily the responsibility of the Executive Sponsor, but in consultation with the Executive Committee. Vendors will be responsible for reporting:

- Scorecard (Key Performance Indicators):
  - Service Level Agreements
  - Return on Investment
  - Compliance with the standards detailed in this document
  - License Consumption Check
  - Org Limits Check
- Quality of Service:
  - Adoption and Utilization
- Technical Documentation:
  - Security and Privacy Configurations
  - Data Dictionary of Custom Fields
  - Entity Relationship Diagrams of Custom Objects
  - Change Log of Configurable Features

[27] https://gearset.com/
[28] https://flosum.com/
[29] https://vlocity.com/
[30] https://appexchange.salesforce.com/listingDetail?listingId=a0N30000000ps3jEAA
[31] https://developer.salesforce.com/tools/vscode/
[32] https://help.salesforce.com/articleView?id=data_loader.htm&type=5
[33] https://www.talend.com/
[34] https://appexchange.salesforce.com/appxListingDetail?listingId=a0N300000016Zn3EAE
[35] https://www.salesforce.com/products/einstein/overview/
[36] https://help.salesforce.com/articleView?id=ideas_about.htm&type=5

- Architectural Diagrams (or equivalents)
  - High-Level System Diagram
  - Unified Modeling Language Class Diagrams
  - Unified Modeling Language Use Case Diagrams
  - Unified Modeling Language Activity Diagrams
  - Unified Modeling Language Sequence Diagrams

Initial Issue: 22 September 2021
Latest Revision: 22 September 2021
Point-of-Contact: Enterprise.Architect@Maine.Gov