Vermont Enterprise Architecture Framework (VEAF)

SOA Governance Implementation

EA APPROVALS

EA Approving Authority:

<Signature> <Date>

<Printed Name> <Position Title>

REVISION HISTORY

Version	Date	Organization/Point of Contact	Description of Changes
2	05/19/2015	Seamus Loftus	Major changes from version 1

Review History

Version	Date	Organization/Point of Contact	Description of Changes
2	9/21/2015	CTO, John P. Hunt	Draft Approval for Discussion

Table of Contents

Table of Figures

Table of Tables

1. INTRODUCTION

SOA implementation requires a formal SOA governance model. SOA Governance for the Enterprise Platform is both a human interaction process and a collection of software modules installed and configured in the SOA environment.

The State of Vermont is committed to successful implementation of SOA Governance that will foster the following:

- Reducing risk
- Maintaining business alignment
- Driving cultural change
- Adding business value to SOA investments

The SOA program must differ from traditional governance approaches. The speed at which decisions need to be made is greater, access to information in a timely manner is needed, there is a greater number of assets and relationships - all of these contribute to and require a different approach. Effective SOA Governance will require a minimum of the following capabilities.

- Asset Management
- Portfolio Management
- Asset Lifecycle Management
- Asset Version Management
- Usage Tracking
- Service Discovery
- Policy Management
- Dependency Analysis

2. SOA GOVERNANCE

The most challenging and misunderstood aspect of SOA is the effect that it has and the demand that it makes on both the enterprise and its employees. SOA Governance requires that the enterprise establishes a viable change management model.

Some stakeholders may potentially see governance as an impediment. Therefore tools must be utilized to automate as many processes and policies as possible. Examples of these tools include registries, repositories, policy management, policy compliance testing, policy enforcement, and testing/diagnostic systems. Even though automating SOA Governance processes minimizes the opportunities circumvent it, there will always be a number of human decision points.

Below is a list of tasks performed by the SoV – SOA governance organization.

- Govern the work done on and to the SOA platform by both IT and business groups
- Perform SOA governance tasks, this does not include SOA implementation tasks
- Lead the creation and implementation of SOA governance principles, policies, and procedures
- Govern SOA strategic, tactical, and operational processes
- Govern the SOA service lifecycle
- Monitor the vitality of the SOA program and lead in making adjustments, including improving skills, identifying new and changing roles, taking corrective actions, and identifying and leading change that improves the agility of the enterprise

3. SOA Governance Roles and Responsibilities

Successful SOA initiatives require active leadership and acquiring executive sponsorship. This sponsorship empowers newly formed or updated structures with not only the mandate but also the appropriate authority. Successful SOA Governance starts from the top down to drive adoption and commitment. Active leadership helps to drive the design of the SOA Governance model.

A key aspect of SOA Governance is the update and creation of new governance structures to define, monitor, and enforce SOA policies. The number and names of these structures is less important than the roles and responsibilities they are focused on. Figure 1 below illustrates the SOA governance structure.

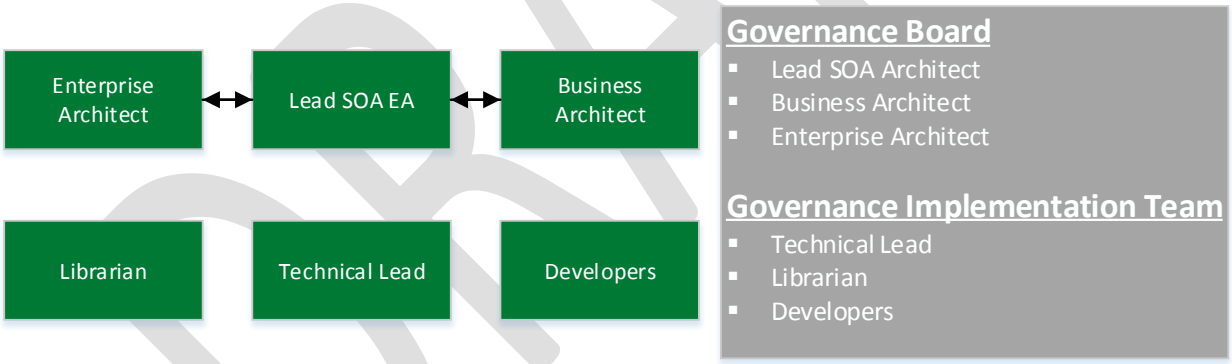

Figure 1 SOA Governance Board

3.1. SOA Governance Board

The SoV SOA Governance board constitutes the following roles and responsibilities. The primary role of the board is to oversee, approve compliance definitions, and mitigate any referrals of non-compliance based on the priority of other business factors.

3.1.1. Lead SOA Enterprise Architect

The Lead SOA Enterprise Architect (EA) is the facilitating member of the SOA governance board, creating the standards and guidelines for SOA implementation. The Lead SOA Architect also oversees the compliance of standards and guidelines put forth by the SOA Governance Board. Details on governance review will be presented by this role to the other members of SOA governance board.

The Lead SOA EA will review the comments from the SOA governance board and will actively participate in the discussions as needed. Any appeal for non-compliance will go for detailed approval with the Lead SOA Architect.

3.1.2. Enterprise Architect

The Enterprise Architect manages and delivers overall enterprise architecture, coordinates the SOA work stream with other Enterprise SOA Architects and approves directives for safeguarding SOA principles and management. They will also ensure that the SOA aligns with the EA governance model. Any compliance and compliance-based rejections will be reviewed by EA. The Enterprise Architect also validates recommendations that are put forth by the Lead SOA Enterprise Architect.

3.1.3. Business Architect

The Business Architect validates and approves service implementation in line with the business requirements and features. They report directly to their Business or Business Process Engineering (BPE) team.

3.2. SOA Governance Implementation Team (Vendor)

The SOA governance Implementation Team will present SOA artifacts to the governance board for approval. Additionally this team will structure their produced artifacts for visibility and reporting purposes to allow the Architecture Governance Board to understand implementation details.

3.2.1. Technical Lead/Solution Architect

The Technical Lead assumes responsibility for the service design and construction phase. This role is custodian of design, development, and deployment of the SOA implementation. They present all artifacts for review to the governance board and seek approval based on the established governance process.

3.2.2. Librarian

The librarian will work on all the projects and assumes responsibility for creating and updating artifacts, and artifact standardization. This role maintains the artifact repository and has the capability of the submitting artifacts into Governance Systems.

3.2.3. Developer

The developers will be responsible for development and unit testing the solutions and services.

4. SOA GOVERNANCE PROCESS

The Governance process has several views that present different aspects of the Governance process. This section delineates the various views and their respective applicable governance process as a checklist.

4.1. Business Architecture and IT Alignment

The State of Vermont is committed having the business drive technology implementation across the State. It is the business' responsibility to collect their capabilities and processes; these collected processes and capabilities allow the SOA Governance team to determine the possibility for the re-use of services across the enterprise. Services are State assets, as much as any physical object. Whenever possible, a service should be reused to actualize cost optimization.

Enterprise Architects engage the business at the project level. Each project has an exploration or requirements phase, where the business uses their capabilities and processes to determine their requirements. It is in this phase that the SOA Governance team is able to review these requirements and compare needed services to the service catalog. If there is a match between a needed and an existing service within the service catalogue, the Request for Proposal (RFP) should reflect the desire to use a pre-existing service. In turn, business processes created as the result of a project will also be reviewed for potential use throughout the enterprise.

Once a project is underway, the SOA Governance team will fall into an oversight role and the service will continue being implemented. This oversight role is detailed in section 4.2 and ensures that only services that meet the needs of the business will be built for the State of Vermont. When the business decides to not use existing services, a justification needs to be written and approved as an architectural exemption.

4.2. Service Development Lifecycle (SvDLC) Governance (Design Time)

The objective of the Service Development Lifecycle is to review and enforce prior agreed upon standards, enterprise policies and procedures.

There are risks in this area, particularly when projects and development teams take shortcuts to meet project deadlines. Although these shortcuts can provide a short-term benefit, they often have a long-term consequences that can affect the overall cost of the service and compromise the ability to achieve the lasting benefits of a well-founded SOA environment. For the governance organization, identifying these issues as soon as possible in the life cycle is essential in order to deliver on the enterprise SOA strategy and realize long term ROI.

Notes:

- Oracle Enterprise Repository (OER) is a tool that is used to provide visibility into the various stages of this lifecycle and a platform to create an automated workflow for this governance process. This is explained in the section 11 SOA Governance Tools.
- The SOA Governance Board is responsible for governance and not design artifacts.

The following is the governance activity table for the SvDLC governance.

Table 1 SvDLC Governance Activity

Responsible Party	SOA Governance Board
Principle	All projects must undergo a SvDLC controls review to determine if they are able to reuse existing services or whether they will create new services. Projects must undergo a SvDLC review and meet all the currently accepted criteria. If there are exceptions, they must be approved by the SOA Governance Board. Test plans and results must be reviewed and validated before the service may be deployed in production.
Standard	Refer to SoV SOA Guidebook for any relevant standards. (Such as SOA Development, Deployment, Security, Coding, and Versioning etc.)
Procedure	Refer SvDLC Governance process diagram below. The Governance process produces artifacts that need to be harvested in the library.
Mechanism	Reviews are scheduled and lead by the EA team working with the PMO. The EA will document the results. This artifact will then be placed in the SOA governance library for future reference by the SOA Governance Board oversight and exception processes. Automated approaches involve the use of OER for this process.
Metrics	The following metrics are very relevant and can be used as a measure of success: • Number of services reused and created in analysis • Number of changes made during design per project • Number of test cases changed per project • Number and severity of defects in integration test • Number and severity of defects in the user acceptance test

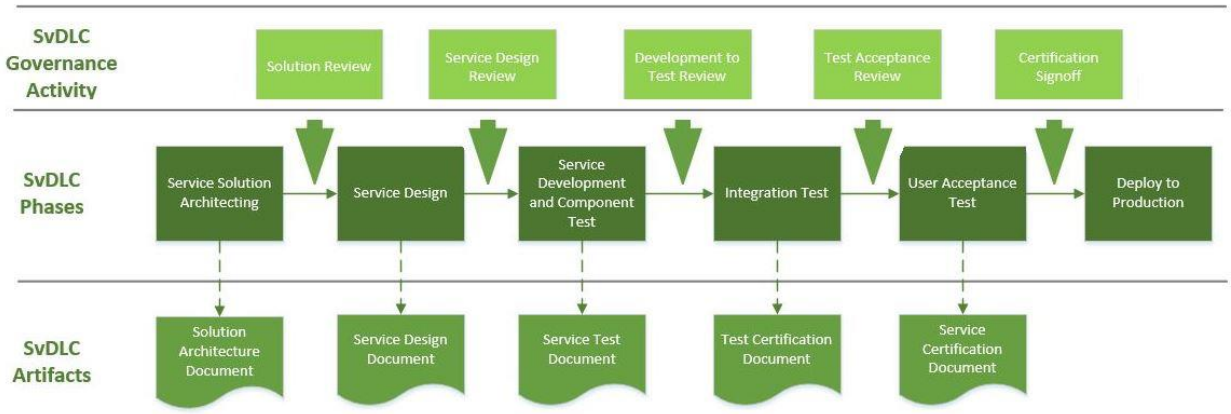

Figure 2 SvDLC Governance Process

The following are the high level phases of a Service Development Lifecycle (SvDLC) that need to be governed. It is important that the SvDLC adheres to the governance activities identified in the SvDLC Governance. Any exceptions to this process need to be reviewed by the SOA Governance Board. The executive committee must approve any deviations.

4.3. Solution Review

The SOA Governance Implementation team, in the Service Solution Architecting phase, is expected to create a solution architecture document; its purpose is to identify the solution approach and high-level design, this includes identifying services to be created or reused.

Upon its completion, the Solution Architecture Document is reviewed by the SOA Governance Board. This gate insures that the proposed solution aligns with first aligns with the State SOA Standards, and identifies areas where an Architectural Exception may have to be made.

The Solution Architecture Document will be assessed based on the following criteria:

- Anticipating and identifying any messaging interface changes to the existing services including (But not limited to)
  - Backward compatibility
  - Service versioning requirements
- Identifies new or additional services clearly delineating use of existing vs. new services

The SOA Governance Board reviews the Solution Architecture Document with the goal of optimizing the services and the project development plan.

When reviewing the Solution Architecture Document, the SOA Governance Board will:

- Identify and recommend opportunities to reuse existing services
- Ensure that the interface documents follow all information and technical standards
- Assess project risk profile and recommend options to decrease risk
- Validate that business requirements are being met
- Identify and recommend requirements for integration testing in the solution and ensure that these are adequately documented in the Solution Architecture Document
- Involve the Service Registrar to register new services or changes

Following the Solution Architecture Document Review, the SOA Governance Implementation Team will update the architecture document based on any recommendations and present again for review by the SOA Governance Board.

This process should continue until the Solution Architecture Document is complete.

4.3.1. Architectural Exemptions

Not all services are able to follow SoV SOA principles and standards; in some cases services may require human workflow, or may be unable to be placed on, or utilize, the Oracle Service Bus. Whenever solutions deviate from the accepted State SOA Standards, they will require that exemption from the SOA Governance Board.

If a service is to be built and it deviates from the State SOA principles, an Architectural Exception must be written and submitted for approval by the SOA Governance Board.

- The Architectural Exemption Document must include:
- A description of the service requiring an exception
- Principles that the service will be unable to meet
- Rationale of the exemption

In its review of an Architectural Exemption, the SOA Governance Board will consider the following:

- The impact of not granting the exception
- The technical merit of the exception
- The collateral impact to other systems and business processes
- The impact to the Enterprise Architecture
- Alternatives to granting the exception
- Precedent setting effects

Following this review the SOA Governance Board with either grant, deny, or consider revising Architectural Guiding Principles in light of the changing environment.

4.4. Service Design Review

Following the approval of the solution architecture document, the SOA Governance Implementation team creates Service Design Document / Interface Control Documents for each new service based on templates provided by the SOA Governance Board.

The Service Design Document / Interface Control Document should:

- Adhere to all policies and standards (Refer SOA Guidebook for Standards and Principles)
- Ensure that all service producer and consumer concerns are addressed, including nonfunctional requirements (NFRs)
- Ensure that the integration testing needs for the service are identified and ensure testing teams are able to perform the necessary tests
- The security design should be assessed as to whether it follows the minimum-security baseline standards (Security Standards Document)
- Review service runtime policies (Ex. WS-Policy) and ensure that service follows the necessary standards adequately

4.5. Development to Test Handoff Review

The SOA Governance Board monitors the development process, ensuring that the handoff from development to integration test occurs smoothly. This process involves:

- The SOA Governance Board facilitating conversations between the test and development teams in order to ensure satisfactory Integration test planning
- Verifying that the service test plan sufficiently tests the service's design, interfaces, and integration with other services and applications
- Ensuring that regression-testing requirements are adequate for modification of existing services
- Reviewing requirement traceability for test plan

The output of this review is recorded in appropriate template and collected in the library.

4.6. Test Acceptance Review

Following Integration Testing, the SOA Governance Board monitors the handoff to user acceptance testing. During the handoff, the SOA Governance Board performs the following:

- Reviews test results with users (if needed)
- Ensures that users have an adequate acceptance test plan
- Ensures that requirements traceability is consistent with acceptance test plan
- Records review outputs and stores it in the library

4.7. Certification Sign Off

Certification Signoff occurs after users and the SOA Governance Board have signed off on acceptance testing. Following this signoff the Registrar:

- Is notified and updates the service catalog accordingly
- Ensures that backward compatibility and versioning for existing service consumers is properly employed
- Verifies that metadata for runtime policy is correctly reflected in the service catalog

Figure 2 in section 4.2 provides a visual representation of the SvDLC governance process and refers to the governed artifact at each stage.

The outputs of all the review above are recorded in the appropriate review template which shall be found in the SvDLC Governance Template document.

5. OPERATIONAL GOVERNANCE (RUN-TIME)

SOA has an impact on the operational processes currently in use at the State of Vermont, and SOA governance must consider the impacts of these and address them with the operations group. The following are important aspects of operational processes that need governance:

5.1. Non-Functional Requirements

Operational governance is mostly concerned with services when they become operational, however, key parameters used to govern solutions need to be integrated early into the SvDLC lifecycle process. These parameters are set by non-functional requirements (NFRs) which substantially contribute to the SOA Governance Board during specification elicitation. From that point on, the SvDLC review gates must consistently ensure that design and testing addresses the NFRs that are key to operational governance.

5.2. Transaction from SvDLC

The SvDLC has a Certification Sign Off quality gate at the end of the SvDLC. This gate presents an opportunity for knowledge transfer between the Design & Development (D&D) and Maintenance & Operation (M&O) teams. The handoff between these teams needs to be governed to ensure smooth transition and success of the operations.

Knowledge Transfer (KT) – D&D team must create a schedule for and conduct formal KT sessions and shadowing sessions such that the M&O team has adequate training to take control of the SOA artifacts and manage aspects such as startup, shutdown, patching, and versioning of the SOA runtime artifacts.

Access – It has to be ensured that the M&O team has the necessary access to administer the SOA artifacts.

Tools & Techniques – The M&O team must possess the necessary tools and techniques to administer the SOA artifacts.

5.3. Service Level Agreements

Service level agreements (SLAs) must be defined to ensure that the services are available with the reliability and performance that service consumers can depend on. Necessary monitoring must be performed in order to ensure that services are meeting their defined SLAs. A properly specified SLA will describe each service offered and addresses the following:

- How a specified quality level of service will be realized
- Which metrics will be collected
- Who will collect the metrics
- How metrics will be collected
- Actions to be taken when the service is not delivered at the specified level of quality and who is responsible for doing them
- Penalties for failure to deliver the service at the specified level of quality
- How and whether the SLA will evolve as technology changes (e.g., multi-core processors improve the provider's ability to reduce end-to-end latency)

For the SoV SOA Implementation, Table 2 is a suggested list of quantitative and qualitative measures that may be used for governance. The exact qualities that are used to govern will need to be based on the objectives for the SLA as described before.

Table 2 SLA Quality Metrics

Type	Quality	Sample Metrics
Quantitative	Accuracy	• Average number of errors for a service over a given time period
	Availability	• Mean Time between failures • Probability that system will be operational when needed • The system's response when a failure occurs • The time it takes to recognize a malfunction • How long it takes to recover from a failure • Whether error handling is used to mask failures • The downtime necessary to implement upgrades (may be zero) • The percentage of time the system is available outside of planned maintenance time
	Capacity	• The number of concurrent requests that can be handled by the service in a given time period. • The maximum number of concurrent requests that can be handled by a service in a set block of time.
	Latency	• The maximum amount of time between the arrival of a request and the completion of that request.
	Provisioning-related time	• The time it takes for a new client's account to become operational
	Reliable Messaging	• How message delivery is guaranteed (e.g., exactly once, at most once) • Whether the service supports delivering messages in the proper order
	Scalability	• The ability of the service to increase the number of successful operations completed over a given time period. • The maximum number of such operations.
Qualitative	Security	This is concerned with the system's ability to resist unauthorized usage, while providing legitimate users with access to the service. Security is also characterized as a system providing non-repudiation, confidentiality, integrity, assurance, and auditing. It is possible to specify the methods for • authenticating services or users • authorizing services or users • encrypting the data

Monitoring Capability – The SLA metrics define what need to be measured. However, without appropriate monitoring capability, collecting and processing such metrics would become difficult. In section 6.2 the use of Oracle Enterprise Manager (OEM 12c) will be discussed in greater detail. It's important to monitor not just how each application is running, but also how each service (as a collection of providers) and individual provider is also running. Such monitoring can help detect and prevent problems before they occur. It can detect load imbalances and outages, provide warning before they become critical issues. They can potentially attempt to correct problems automatically. Service monitoring can measure usage over time to help predict services that are becoming more popular so that they can increase capacity.

It is expected that the vendor M&O team of the SOA platform performs the monitoring of SLAs and reports any issues to the SOA Governance Board.

6. SOA Asset Lifecycle Governance

A collection of service artifacts used to solve a specific business problem are called a SOA Asset. Reusable services are at the core of SOA. As discussed in the VEAF SOA Strategy document, the identification of services should grow from both a business strategy viewpoint and organically from project need as depicted in Figure 3.

Figure 3 Service Identification for a Reusable SOA Asset

The Governance of SOA Assets Lifecycle pertains to managing an asset from its identification through its realization until its retirement. This is an important aspect of governance for the State of Vermont especially given the strategic approach it has adopted in its move towards cloud and Software as a Service (SaaS) based architecture.

Business, information, application, and technology strategy will drive the creation of service requirements. These requirements result in the identification of services. The same can be said about projects that are initiated. The SOA asset lifecycle governance takes a comprehensive view of requirements and facilitates planning for the availability or creation of services. The lifecycle stages shown in figure 8 form control gates for governance activity. The activity is important, because tracking the service in a services catalog provides a single point of reference for available, planned, and in build services that can be referenced across the enterprise and its various projects. This ultimately promotes reuse at not just a service artifact level but conceptual level as well.

Table 3 SOA Asset Lifecycle Governance Activity Table

Responsible Party	Service Registrar
Policy	Service status is updated upon successful completion of a SvDLC control gate. Service backward compatibility needs enforced where applicable. Versioning must follow the Versioning standards document as referenced in the SOA Guidebook. (For example, from Version 1.2 to 2.0. If the service change is backward compatible, this is a "minor" version change, for example from 1.2 to 1.3.) Services Identification must result in registration with a brief description to its business purpose, interface elements and abstract use case.
Standard	SOA Guidebook provides list of standards (especially Service versioning standards). In addition, several other plans, as applicable, for Business agility and technology agility produced by individual business units of the SoV. The Technology office of SoV may form the standards and basis for this governance.
Procedure	The SOA Asset Lifecycle process shown in **Error! Reference source not found.** below must be followed. The service catalog must be kept updated as a part of the SvDLC.
Mechanism	Service catalog, with management capabilities from the service catalog.
Metrics	The following metrics can be used as a measure of the maturity. • Number of reuse of services. • Number and services by state. • Number of services by available versions (should be minimum as this would indicate they are not being retired) • Number of services in planned state that transitioned to build state. • Number of planned services as identified from projects vs. identified from agility.

Figure 4 depicts the SOA assets lifecycle Governance process. One or more of the following activity initiates the Asset Lifecycle process through Service identification.

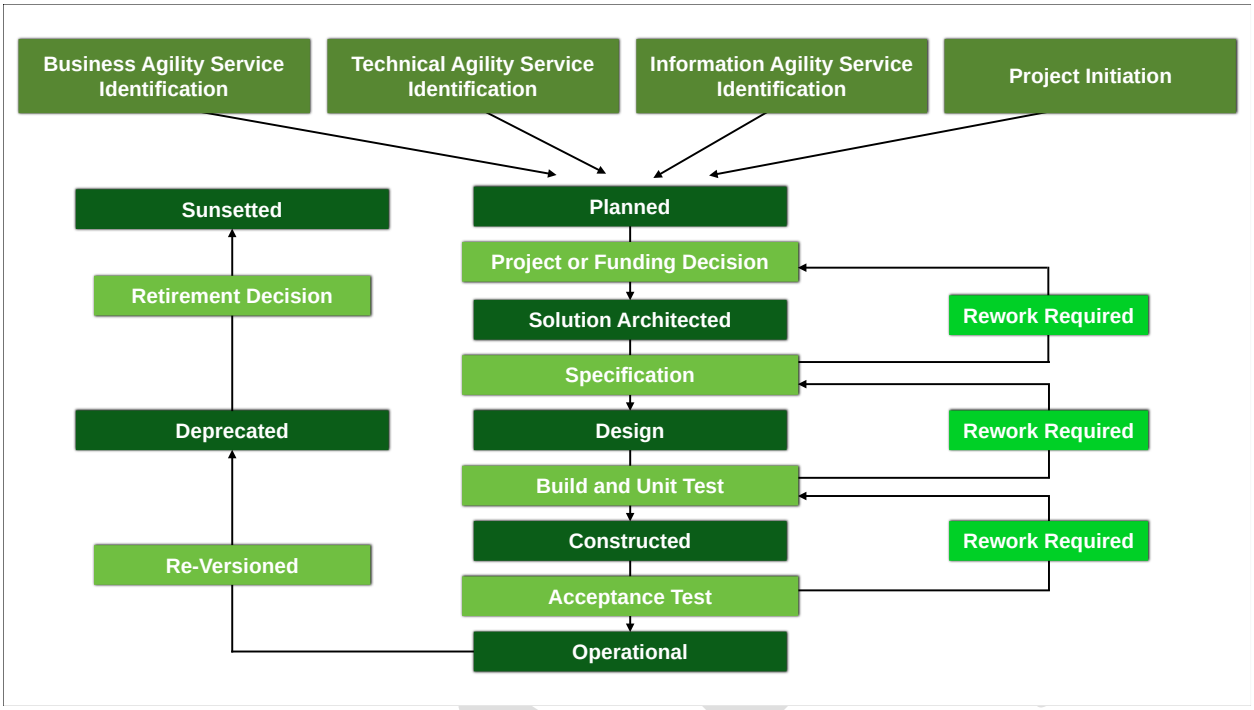

Figure 4 SOA Asset Lifecycle Governance Process

- Business Agility Service Identification – This is initiated from either the executive management or from the Business IT representatives in the SOA Governance Board. A business architecture has been evaluated and a need for a service is identified then it can initiate the SOA asset lifecycle for that service.
- Technology Agility Service Identification – SOA Architects in the SOA Governance Board may initiate this. When a technological shift is anticipated that requires the need for a service, then a SOA Asset lifecycle is initiated for that service.
- Information Agility Service Identification – A specific information need that arises from the business may be evaluated and identify a service, this would initiate the SOA Asset lifecycle for that service.
- Project Initiation – During projects initiation, business needs are evaluated, new services may be identified and are the most common use case for service identification.

The following is a list of status maintained in the services catalog by the registrar for SOA Assets.

- Planned – These are services that have been identified, but are not yet implemented. Project planners will be able to consult the catalog and find planned services that their project is in a position to fund and create. The solution architect will find the status of services that they contemplate reusing in the services catalog and the status of such services. This capability will enable them to then assess the applicability of the service to their project.
- Solution Architected - This status of the service is afforded in the service catalog as the solution architecture document is approved in the SvDLC.
- Design – Those services for which the Service Design document is approved.

- Constructed – A service that has passed through the acceptance stage of the SvDLC, this status is provided.
- Operational – Services that have been moved to production and are subject to operational governance.
- Deprecated – A service on its way to retirement. Flipping to deprecated status would mean that the service may not be freshly reused, however, any existing use of the service will need to be carefully considered for refactoring.

Service versioning enables users satisfied with an existing service to continue using it unchanged, yet allows the service to evolve to meet the needs of users with new requirements. The current service interface and behavior is preserved as one version, while the newer service is introduced as another version. Version compatibility can enable a consumer expecting one version to invoke a different but compatible version. (Refer to Service Versioning standards)

- Sunset – After a formal retirement decision based on metrics of usage and relevance to business, the services will be retired.

7. SOA SECURITY GOVERNANCE

Services, by nature, have distributed architecture as they are accessible across networks outside firewalls making security architecture vitally important. Usually, a message based security protocol such as WS-Security must be chosen as a standard and then enforced via SOA governance. This includes security for authentication, authorization, encryption, and nonrepudiation. The Security Standards document as listed in the SOA Guidebook sets these standards.

For State of Vermont, the security governance is integrated with the SvDLC governance with the standards being the SOA Security. Therefore, separate activity table and governance process for security governance is not required. Please refer to SvDLC Governance for these.

8. SOA GOVERNANCE TOOLS

In the previous sections, the various aspects of the different governance processes were described. This section discusses the various tools to facilitate governance activities. The State of Vermont utilizes the Oracle suite of governance tools which are discussed below. The SOA Governance tool provides for storage of and facilitates exchange of SOA artifacts metadata information as shown in Figure 5.

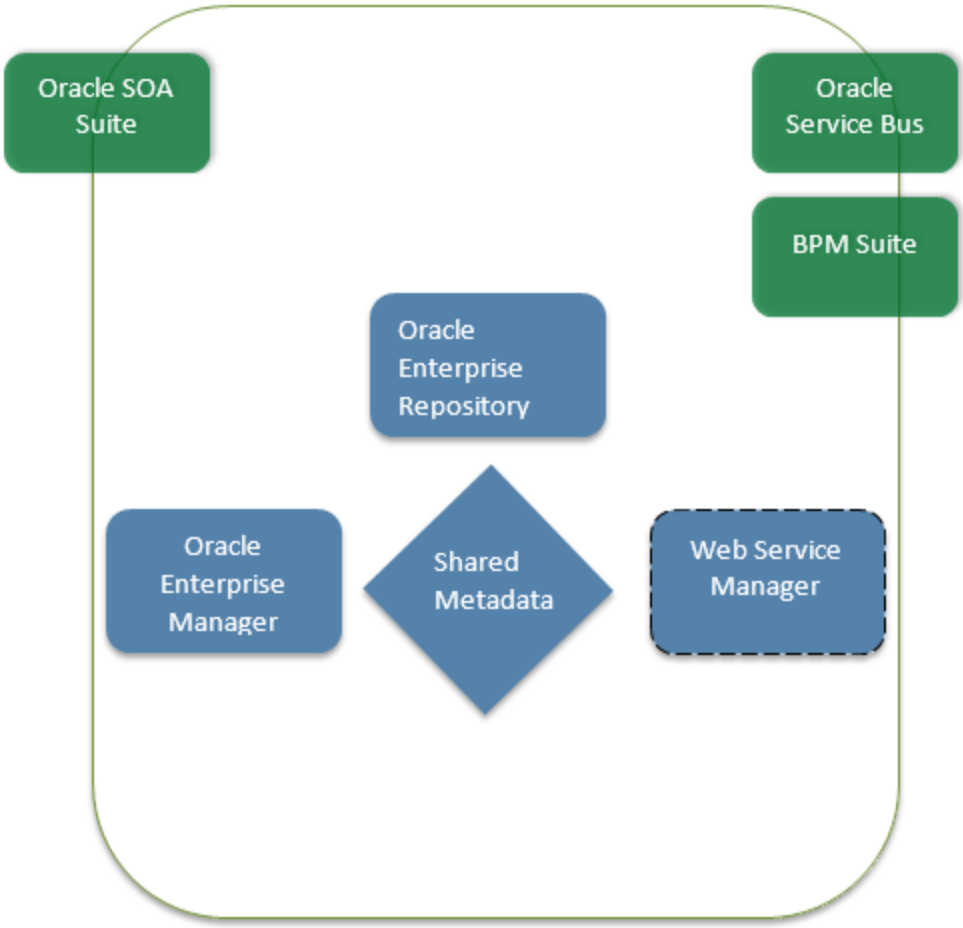

Figure 5 SOA Governance Tools

8.1. Oracle Enterprise Repository

Oracle Enterprise Repository (OER) is an industry-leading tool used in SOA Governance. A detailed list of the product features and capabilities are beyond the scope of this document. Detailed information on OER is available at the product website.

OER will be used to further the governance processes discussed earlier as discussed below. The following is a listing of key capabilities that will be utilized by the OER and apply to the various governance activities discussed earlier.

- Service Cataloging – The service catalog is the basic repository of services.
- Features – It provides role-based visibility into all SOA assets. It serves as a centralized repository for APIs, business processes, services, applications, components, models, frameworks, policies, and data services. Service Catalogs provides visibility for services in all phases of the SvDLC and also the SOA asset lifecycle.
- Utilization matrix – The following is a utilization matrix of this feature that lists the Governance activities where they will be used.

SvDLC Governance	√
SOA Asset Lifecycle Governance	√
Security Governance	
Operations Governance	
SOA Portfolio Governance	√

- Policy – The following policies are applicable
- All service artifacts at the interface definition level i.e. Service WSDL's, Adapters, BPEL and Mediator components shall be created in the catalog.
- Every project artifact will have references to the underlined XSD and also the called services.
- Artifacts will be associated to the upstream services in one of the following ways
  - Manually linking
  - Automatic Link through harvest utility
  - REX API's during registration process

8.2. Oracle Enterprise Monitoring

The Oracle Enterprise Manager is used to monitor the SOA services built onto the SOA Suite. The State is provided with regular reports from the live environment and reviews them to ensure that they meet the agreed upon SLAs. The vendor M&O team is responsible for assessing and monitoring the SLAs established for the services developed and installed in the live environment.

8.3. Oracle Web Service Manager

The State of Vermont is committed to building a secure environment, to keep data safe. This includes building secure Services on the SOA. Each service may have its own security requirements and needs to make sure they meet the necessary criteria. Security policy should be dictated in Oracle Web Service Manager.

APPENDIX A: TEMPLATES

Documentation	Link
ICD Template	https://inside.vermont.gov/sov/cto/ea/Technology%20Architecture/SOA(New)/Level%202/Templates/SOA%20ICD%20Template%20v0.2.docx