State of California
Franchise Tax Board

Service Oriented Architecture (SOA) Governance Model

Version No. 1.4

May 2010

Author:
SOA CoE Core Team 2008/2009

Document Information

Revision History

Version No.	Date	Author	Change Description
1.0	9/3/2009	SOA CoE Core Team 2008/2009	Initial Release
1.1	12/4/2009	Cheryl Deagon	Incorporated review comments from EAC and SOA CoE members: • Grammar and spelling changes • Reference to SOA Governor Role changed to SOA Governor Team for consistency • Removed references to SOA Entry points in the Service Discovery section
1.2	12/23/2009	Cheryl Deagon	Incorporated review comments from TAC: • Clarification of service consumer role in the SOA Roles and Responsibilities section • Added definition for SOA Watch List to the SOA Glossary (Appendix A) • Changed reference to SOA Criteria to Service Criteria for consistency (Appendix C). • Replaced logo on front page with the most current one.
1.3	01/21/2010	Cheryl Deagon	Incorporated Policy Review changes: • Add SOA Governor Team definition to the Glossary. • Removed IBM reference from SOA definition in Policy & Glossary • Removed 1st row of text in the RACI under roles • Clarified what projects come in through the SOA intake process.
1.4	05/19/2010	SOA Governor Team	• Updated Section 1.3 Assumptions to clarify that enterprise services can also be developed and maintained by vendors (per EDR review comments). • Updated the Glossary (Appendix A). Some references were modified during the SOA Policy approval process. • Included link to SOA Policy (Appendix G) that was approved on 5/7/2010. • Included the latest Enterprise Services Sign-off Procedures (Appendix I).

Contents

1. Introduction

1.1. Background

The Franchise Tax Board (FTB) and the State of California have a long-term vision of transitioning to a Service Oriented Architecture (SOA) enterprise environment. SOA is defined as a framework for integrating business processes and supporting IT infrastructure as secure, standardized components (services) that can be reused and combined. SOA services provide better utilization of functionality and reduce the development of redundant systems across the enterprise, thus maximizing the cost-effectiveness of developing and implementing services. A strong and well-defined governance process ensures that these services become assets, or building blocks, that can be leveraged to develop new systems more efficiently and effectively to meet FTB's business needs.

One of the challenges that SOA services bring to an organization is the need for clearly defined governance processes. Once identified, and clearly defined, the governance process will help to manage the lifecycle of the SOA services from initiation, through maintenance, and ultimately until the service is retired.

To help implement and mature SOA at FTB, Enterprise Architecture commissioned the SOA Center of Excellence (CoE). The SOA CoE is a cohesive and collaborative team of FTB staff from around the department lead by the Enterprise Architect Council's (EAC) Service Solutions Architect. The SOA CoE primary tasks include planning and governance activities that support the implementation and maturation of service-oriented architecture at FTB. The key initiative for 2008/2009 was to develop a practical and comprehensive service-oriented architecture governance strategy. The governance strategy includes governance for SOA service planning, development, operations and reuse. The SOA Governance Model is a result of the SOA CoE 2008/2009 efforts.

1.2. Purpose

The purpose of SOA governance is to establish a set of enforceable policies, procedures, processes, tools, standards and organizational structure that allows for the effective creation, reuse and retirement of services. FTB SOA goals are to:

- Align business and IT
- Establish service re-use
- Establish an agile service environment

FTB's SOA governance defines the interrelationships of different groups, participants and service providers describing how they will work as a cohesive unit within the larger SOA architecture. In order for FTB to develop a mature SOA enterprise architecture, it is necessary to align business and IT to a methodology and process that connects business and enterprise architecture. To achieve service reuse, FTB will ensure the existence of standards and put into place an effective governance model. Agility will be achieved as new projects come along and processes can be quickly assembled for the business using existing (reusable) services. In addition, many of the SOA governance processes will be automated as FTB matures in SOA practices.

This documentation describes FTB's SOA Governance Model which will be used by staff to manage our Enterprise Services. It describes the activities in the SOA Lifecycle and the roles that are needed to support them, the policies that surround SOA services, metrics that will be captured to measure the effectiveness of the SOA governance process and the key checkpoints throughout the SOA Lifecycle. To assist in this effort, a set of Templates and Procedures are provided within the appendices.

1.3. Assumptions

The SOA Governance Model is based on the following assumptions:

- Enterprise services will continue to be developed and maintained either by the Enterprise Integration Services Section or a vendor.
- Only approved projects/efforts, with assigned resources (funding and people) and the potential to create, modify or consume (reuse) a SOA or enterprise service are governed by the SOA Governance Model.
- A Project Manager must be identified for SOA service development (i.e. a responsible party must be identified to carry out the project management duties for SOA service development). One of the responsibilities of the SOA Project Manager is to ensure that the SOA Governance Model is followed.

1.4. Scope

The scope of SOA Governance is for enterprise services developed and maintained at FTB (either by FTB staff or vendors). It does not govern the following (although it could be expanded in the future to include them):

- Purchased products.
- Local and rogue services (see SOA Glossary – Appendix A for definitions)

2. Governance Decisions

2.1. SOA Governance Policy

The governance policy for SOA services outlines the policy statement, purpose and applicability of Enterprise Services. Having a policy to back the governance model allows specific standards, procedures and templates to be set. The policy statement and the standards, procedures and template documents are detailed in the Appendices of this document.

2.2. Service Ownership

SOA introduces several challenges to traditional IT ownership for two primary reasons: 1) services are built to address enterprise concerns, and 2) services are made up of several parts that are generally distributed in nature.

The following types of ownership are related to operating in the SOA environment at FTB (see SOA Roles and Responsibilities - Appendix E for more information):

- **Business Owner** –defines service requirements and judges the business impact of any changes or enhancements to the service
- **Technical and Infrastructure Owner** – responsible for the design, development, and provisioning of the service
- **Operational Owner** – responsible during the operational or maintenance life cycle of the service

- **SOA Governor Team** –ongoing governance body with membership coming from the following areas: Lead: SOA Solution Architect; Member 1: SOA Development representative; Member 2: Transition representative; Member 3: Operations representative, Member 4: Business Stakeholder. These members represent the major SOA SDLC checkpoints ("hand offs") as shown on the RACI. This team will meet on an as-needed basis and will be empowered with the authority and responsibilities described in the SOA Roles and Responsibilities document (Appendix E).

2.3. Service Criteria, Service Prioritization, and SOA Portfolio Management

Service Criteria is the pre-determined set of factors used to evaluate the merits of developing an enterprise SOA service. Examples would include such factors as strategic relevance, technical feasibility, return-on-investment (such as the expected amount of reuse), and business value (such as consistency of functionality). The task of deciding the service criteria will be performed by the SOA Governor Team.

Service Prioritization is a dynamic decision process whereby SOA service requests (new work and changes) are considered, evaluated, and prioritized against other service requests using some pre-defined criteria. Prioritization is creating the list/the roadmap (in other words, the order of development and/or change); it is not the balancing of workload and people. If development, infrastructure, and/or operational areas require more staff that is the responsibility of the appropriate manager (in other words, the pace of development and/or change). The task of deciding the service prioritization will be performed by the SOA Governor Team.

SOA Portfolio Management is the management of that collection of SOA services in which an organization invests (develops, maintains, operates, and retires) to implement its SOA strategy. Sources of ideas for new services may be brought forward by the following:

1. New Projects
2. New ideas from any area
3. Legacy system review/deconstruction/extraction
4. Analysis of Business Process Maps

The task of deciding which services to create, modify, extend, combine or retire will be performed by the SOA Governor Team. FTB's SOA Portfolio is made up of ideas that are being considered for new services (SOA Watch List) and the existing services that are listed in the Enterprise Services Registry.

2.4. SOA Service Discovery

Service Discovery refers to the ways that services are discovered and is essential to facilitate the reuse of existing services. The service registry and repository are governance tools associated with service discovery.

At FTB, services may be discovered in one of two ways:

1. Through the EA Assurance Process where an initial review of the project is done to see if there is an existing service that will meet the project's needs.
2. By a technical developer who is searching the Enterprise Services Registry for a service that may be reused to meet their needs.

There is an online document that serves as FTB's registry/repository. It lists the enterprise services that are available for reuse. Each service listed links to documentation that includes a data sheet with high level service information.

2.5. SOA Operational Agreements (OA)

Operational Agreements are an agreement between the provider of a service and the consumers that describes performance expectations and defines ownership responsibilities for the SOA service (in the absence of an SLA/OLA).

The goal of the OA is to define, document and agree to the level of service that is to be provided. They are necessary to establish confidence and trust in SOA services. By meeting these predefined service levels others will be agreeable to reuse a service as well.

FTB will ensure the terms of the OA are being met by following the SOA Governance Model when developing, modifying, or consuming SOA services. Monitoring criteria will be defined along with whom and how SOA services will be monitored. Tools like "What's Up Gold" and Introscope will be used to monitor SOA services. When problems are encountered, they will be managed by the incident management and problem management processes (including lessons learned and continuous improvement).

When adding new consumers to a SOA Service, we will guarantee existing Operational Agreements by performing an impact analysis (this is part of the SOA Lifecycle) to validate that the existing OAs with prior customers will continue to be met. (See Operational Agreement Template – Appendix J for more information.)

2.6. SOA Service Certification

Service Certification is the governance process that verifies a service meets the functional and non-functional requirements. An Enterprise SOA service, whose development has followed the SOA Lifecycle (Appendix B) and has obtained the required signoffs (see SOA Sign Off Template - Appendix J), will be certified once it has been deployed into the production environment and published to the registry/repository. A special process is not necessary for certification for SOA services that follow the SOA governance process.

If an existing enterprise service or a local service wants to become certified, it must come through the SOA Intake step of the SOA Lifecycle ("New/Modify" - Appendix B) and meet the requirements of each step of the lifecycle in order to qualify for certification.

The registry list will specify whether a service is certified or not. It is recognized that certification is an important aspect to "building trust" in SOA services and fostering their reuse within the organization.

2.7. SOA Governance Metrics

SOA governance metrics measure compliance and verify policy enforcement regarding service use. They will measure trends, including the level of reuse, and the number of violations and requests for waivers. The success of SOA governance and policies in relation to directing service consumption will be determined by these metrics.

Establishing metrics and a baseline for SOA governance will help FTB to determine how well the SOA governance model is working. See SOA Governance Metrics Service Use – Appendix F for specific governance metrics that will be captured, as well as an example of the process.

The objectives of the SOA Governance Metrics are to ensure:

1. SOA Governance process is streamlined and predictable (faster).
    - Capture the time required for the SOA governance process per project/request, including the appeal process time for project exceptions to EAC recommendations
2. SOA Governance Process is recognized and supported by CIO and TAC.
    - Capture the number of exceptions to EAC recommendations that are supported or are overturned by TAC.
3. SOA Governance Process results in quality enterprise SOA services providing development and maintenance cost savings to FTB (better, cheaper).
4. Capture the number of services recommended by EAC, denied or rejected by TAC, implemented by the Project, and continued use in production.

Note: The SOA Performance Metrics are addressed in the Operational Agreement section of this document.

3. Components of SOA Governance

3.1. SOA Glossary

The SOA Glossary (SOA Glossary – Appendix A) includes common definitions used between the Information Technology Infrastructure Library (ITIL) and SOA. Everywhere ITIL is cited in the SOA Glossary, the definition is taken directly from ITIL's v3 Glossary of Terms and Acronyms. In order to reach common understanding of services a distinction in terms is crucial. The SOA Glossary is a "living" document and definitions may be added and/or modified as needed.

3.2. SOA Lifecycle

The SOA Lifecycle diagrams (SOA Lifecycles – Appendix B) represent the activities that take place from service initiation through the retirement of a SOA service.

All projects are subject to the EA Assurance Process. During the EA Assurance Process, if it is determined that the project has the potential to create, modify, consume (reuse) or retire a SOA service it will enter the SOA Lifecycle at the SOA Intake Process after all of the necessary project approvals have been obtained.

The "New/Modify" lifecycle diagram describes the processes required to define, design, build, test, performance verify, accept, execute, operate, and maintain SOA services. The "New/Modify" SOA Lifecycle used for creating a new enterprise service or for modifying an existing service. The lifecycle ensures that enterprise requirements are met including business functionality and performance expectations.

The "Consume/Deconsume" lifecycle diagram describes the processes required to access and reuse existing SOA services.

The SOA Lifecycle is a combination of SDLC and ITIL processes. SOA Services, because of their widespread use, require more structure than stand alone applications during the planning and operations phases of the lifecycle. In addition to the SDLC, ITIL provides the structure and processes that enterprise SOA requires to be successful.

Each step of the lifecycle is described in detail in the SOA Lifecycle Activity Definitions - Appendix C. For each activity a short description is given. It also describes the inputs, outputs, and signoff responsibility for each lifecycle activity.

3.3. SOA RACI Diagram

The SOA RACI diagram (SOA RACI – Appendix D) represents the roles and responsibilities in relation to the SOA Lifecycle.

The following description is taken from Wikipedia.
The RACI diagram splits tasks into four participatory responsibility types, which are then assigned to different roles in the project or process. These responsibility types make up the acronym RACI.

- **R**esponsible – Those who do work to achieve the task. There can be multiple resources responsible.
- **A**ccountable – (Also **A**pprover) The resource ultimately answerable for the correct and thorough completions of a task. There must be only one **A** specified for each task.
- **C**onsulted – Those whose opinions are sought. Two-way communication.
- **I**nformed - Those who are kept up-to-date on progress. One-way communication.

3.4. SOA Roles and Responsibilities

The roles that relate directly to operating in a SOA enterprise environment and depicted on the SOA RACI diagram, are described in detail in the SOA Roles and Responsibilities – Appendix E.

Note: The consumer of the service participates in multiple roles, which are described in the following references:

1. SOA Roles and Responsibilities (Appendix E) – documents the consumer's role when a SOA Service is created, modified or consumed:
    - Business Owner
    - Application Expert

2. Calling Application Area's SDLC (outside the scope of SOA Governance) - documents the consumer's roles when the existing application code is changed to consume the service and to test the application's connection to the service. The consumer would be represented in the application area's SDLC by the following roles:
    - Developer
    - Tester

4. Appendices

4.1. **Appendix A: SOA Glossary**

4.2. **Appendix B: SOA Lifecycles**

- SOA Lifecycle – New/Modify
- SOA Lifecycle – Consume/Deconsume

4.3. **Appendix C: SOA Lifecycle Activity Definitions**

4.4. **Appendix D: SOA RACI**

4.5. **Appendix E: SOA Roles and Responsibilities**

4.6. **Appendix F: SOA Governance Metrics**

4.7. **Appendix G: SOA Governance Policy**

4.8. **Appendix H: Standards**

- SOA Version Standard

4.9. **Appendix I: Procedures**

- Enterprise Services Sign-Off Procedure

4.10. **Appendix J: Templates**

- Enterprise Services Sign-Off Template
- Enterprise Service Request to Consume/Deconsume Template
- Operational Agreement (OA) between Consumer and Service Provider

Architecture Framework – A tool which can be used for developing a broad range of different architectures. It should describe a method for designing an information system in terms of a set of building blocks, and for showing how the building blocks fit together. It should contain a set of tools and provide a common vocabulary. It should also include a list of recommended standards and compliant products that can be used to implement the building blocks.

Access Management – The Process responsible for allowing Users to make use of IT Services, data, or other Assets. Access Management helps to protect the Confidentiality, Integrity and Availability of Assets by ensuring that only authorized Users are able to access or modify the Assets. Access Management is sometimes referred to as Rights Management or Identity Management (ITIL).

Backward Compatible – a product or a technology is said to be backward compatible when it is able to fully take the place of an older product, by interoperating with products that were designed for the older product.

BPEL (Business Process Execution Language) – The XML business process modeling language that is executable and universally supported. BPEL supports both public (protocol) and private (execution) languages (BPM CoE).

BPM (Business Process Management) – A strategy for managing and improving the performance of a business through continuous optimization of business processes in a closed-loop cycle of modeling, execution, and measurement. The methods, techniques, and tools used to design, enact, control, and analyze operational business processes involving people, systems, applications, data, and organizations (BPM CoE).

Business Service – The logical encapsulation of a business function. The following are examples of a business service: a tax calculation of penalties and interest, an estimated payment calculation for a taxpayer (SOA EAD).

Change Management – The Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services (ITIL).

Composite Service – A collection of services that are assembled to form a business process built on SOA and have no manual elements.

Configuration Management – The process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the lifecycle of a CI. Configuration Management is part of the overall Service Asset and Configuration Management Process (ITIL).

Configuration Item – Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs (ITIL).

Consumers – Software applications that call an existing enterprise service rather than re-creating like functionality.

Customer – Someone who buys goods or Services. The Customer of an IT Service Provider is the person or group who defines and agrees the Service Level Targets. The term Customers is also sometimes informally used to mean Users, for example "this is a Customer focused Organization" (ITIL).

Data Service – A type of service that delivers data from an information store. (i.e. Franchise Tax Board ID) (SOA EAD).

Deploy Service – Making the service available so that it can be called on in the operational environment.

Design Package – The body of design documents that includes the architectural diagram, high-level design, and detailed design.

Enterprise Service – A certified SOA service that is reusable across FTB, has enterprise-level requirements and is centrally managed.

Enterprise Service Bus (ESB) – A collection of components that comprise the foundational services for more complex architectures via an event-driven and standards-based messaging engine “the bus” (SOA EAD).

Evaluation – The Process responsible for assessing a new or Changed IT Service to ensure that Risks have been managed and to help determine whether to proceed with the Change. Evaluation is also used to mean comparing an actual Outcome with the intended Outcome, or comparing one alternative with another (ITIL).

Event – A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged (ITIL).

Event-Driven Architecture (EDA) – A software architecture pattern promoting the production, detection, consumption of, and reaction to events. Event-driven architecture complements service oriented architecture (SOA) because triggers such as events can start services.

Event Management – The Process responsible for managing Events throughout their Lifecycle. Event Management is one of the main Activities of IT Operations (ITIL).

Functional Requirement – A requirement that defines the specific behavior of a software system or its components with a prescribed set of inputs, the prescribed activities, and expected outputs.

Impact Analysis – The analysis of a proposed change (e.g. service request or project) and its net positive or negative impact (risk) on the environment in which it would be implemented (including business programs, applications, and related business areas). Said another way, an impact analysis is the process of assessing the merits of pursuing and implementing a project or service request.

Incident Management – The Process responsible for managing the Lifecycle of all Incidents. The primary Objective of Incident Management is to return the IT Service to Users as quickly as possible (ITIL).

Infrastructure Services – The “plumbing” services that are leveraged to increase the sophistication with which ESB is able to carry out messaging, routing, and SOA related functions. Security and business policies will need to incorporate or introduce rules. Some of the infrastructure services may be applied together with policy services and security centralization (SOA EAD).

IT Service – A function performed using information technology to support a process. An IT service is made up of a combination of people, processes and technology and should be defined in a SLA and/or an OLA.

Knowledge Management – The Process responsible for gathering, analyzing, storing and sharing knowledge and information within an Organization. The primary purpose of Knowledge Management is to improve Efficiency by reducing the need to rediscover knowledge. See Data-to-Information-to-Knowledge-to-Wisdom, Service Knowledge Management System (ITIL).

Local Service – An IT service that is reusable but was not designed to be used as an enterprise service.

Major Incident – The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business (ITIL).

Monitoring – Repeated observation of a Configuration Item, IT Service or Process to detect Events and to ensure that the current status is known (ITIL).

Non-Functional Requirement – A requirement that specifies criteria that can be used to judge the operation of a system (i.e. response times, accessibility, reliability), not specific behaviors of a system or process.

Operations – Day-to-day management of an IT Service, System, or other Configuration Item. Operation is also used to mean any pre-defined Activity or Transaction. For example loading a magnetic tape, accepting money at a point of sale, or reading data from a disk drive (ITIL).

Operational Agreement – In the absence of an OLA/SLA, an agreement between the provider(s) of a service and a consumer that describes performance expectations and defines ownership responsibilities for the SOA Service.

Operations Management – Synonym for IT Operations Management (ITIL).

Operating Level Agreement (OLA) – An Agreement between an IT Service Provider and another part of the same Organization. An OLA supports the IT Service Provider's delivery of IT Services to the Customers (ITIL).

Orchestration – A process based approach to combine services with workflow, typically using BPEL (BPM CoE).

Problem – A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation (ITIL).

Problem Management – The Process responsible for managing the Lifecycle of all Problems. The primary Objectives of Problem Management are to prevent Incidents from happening, and to minimize the Impact of Incidents that cannot be prevented (ITIL).

Publish Service – Making known the service definition and state so that the service can be found and used by consumers.

Process – A set of business tasks designed to deliver value to an internal or external client. A process may be comprised of any combination of sub-processes and activities.

Quality – The ability of a product, Service, or Process to provide the intended value. For example, a hardware Component can be considered to be of high Quality if it performs as expected and delivers the required Reliability. Process Quality also requires an ability to monitor Effectiveness and Efficiency, and to improve them if necessary (ITIL).

Quality Management – (Continual Service Improvement) The set of Processes responsible for ensuring that all work carried out by an Organization is of a suitable Quality to reliably meet Business Objectives or Service Levels (ITIL).

Registry & Repository – A central reference for all the software components within the SOA environment (SOA EAD).

Release Management – The process responsible for planning, scheduling and controlling the movement of Releases to Test and Live Environments (ITIL).

Request for Change – A formal proposal for a Change to be made. An RFC includes details of the proposed Change, and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record, or the Change itself (ITIL).

Request Fulfillment – The Process responsible for managing the Lifecycle of all Service Requests (ITIL).

Requirements Package – The body of requirements documentation that includes the functional, non-functional, and security requirements.

Retire - (Service Transition) Permanent removal of an IT Service, or other Configuration Item, from the Live Environment. Retired is a stage in the Lifecycle of many Configuration Items. **(**ITIL)

Risk Management – The Process responsible for identifying, assessing and controlling Risks. See Risk Assessment (ITIL).

Rogue Service – An uncertified IT service, which may or may not be used across the enterprise.

Service – A means to delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.

Service Asset and Configuration Management (SACM) – The process responsible for both Configuration Management and Asset Management. (ITIL)

Service Catalog – A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalog is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes (ITIL).

Service Certification – The governance process that verifies that a service meets the functional and non-functional requirements.

Service Component Architecture (SCA) – A set of standards (a relatively new initiative advocated by major software vendors) related to the delivery of applications that conform with the principles of SOA.

Service Consumer – An application or another service that uses a SOA service.

Service Criteria – The pre-determined set of factors used to evaluate the merits of developing an enterprise SOA service. Examples would include such factors as strategic relevance, technical feasibility, return-on-investment (such as the expected amount of reuse), and business value (such as consistency of functionality).

Service Deployment – Making the service available so that it can be called on in the operational environment.

Service Desk – The Single Point of Contact between the Service Provider and the Users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users (ITIL).

Service Discovery – Refers to the ways that services are discovered or made known to the public or an organization. Service discovery is essential to facilitate the reuse of existing services. The service registry and repository are governance tools associated with service discovery.

Service Level Agreement (SLA) – An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer (ITIL).

Service Level Management – The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews (ITIL).

Service Oriented Architecture (SOA) – A framework for integrating business processes and supporting IT infrastructure as secure, standardized components — services — that can be reused and combined to address changing business priorities and is based on the following design principles:

Design Principles of SOA

- *Technology Neutral* – Uses industry agreed upon standards to create interfaces, which make it possible for consumers on any platform to invoke services provided on any platform.
- *Modular* – Self-contained components that can communicate with each other through a well-defined interface.
- *Sharable* – Can be reused by more than one functional area.
- *Loosely Coupled* (agility) – Ability to make changes to one part of the system without changing the other – each component offers a small range of simple services to other components.
- *Encapsulation* – Focus is on the interface rather than the underlying implementation details - hides any data or behavior that is specific only to the internal working or the service and irrelevant to the service consumer.

Service Portfolio – The complete set of Services that are managed by a Service Provider. The Service Portfolio is used to manage the entire Lifecycle of all Services, and includes three Categories: Service Pipeline (proposed or in Development); Service Catalogue (Live or available for Deployment); and Retired Services (ITIL).

Service Portfolio Management – The Process responsible for managing the Service Portfolio. Service Portfolio Management considers Services in terms of the Business value that they provide (ITIL).

Service Prioritization - A dynamic decision process whereby SOA service requests (new work and changes) are considered, evaluated, and prioritized against other service requests using some pre-defined criteria.

Service Registry Administrator (SRA) – person who manages the consistency of the registry and enforces guidelines that protect against redundancy, proliferation and unauthorized modifications of the service registry.

Service Tool – Tools that support the governance, implementation and deployment of SOA Services. Service tools include the run time environment, testing tools, orchestration tools and registry and repository tools. COTS products that supply services are not considered service tools.

Service Use – The governance and policy directing service consumption.

Service Validation and Testing – The Process responsible for Validation and Testing of a new or Changed IT Service. Service Validation and Testing ensures that the IT Service matches its Design Specification and will meet the needs of the Business (ITIL).

Simple Object Access Protocol (SOAP) – A protocol for exchanging XML-based messages over computer networks, normally using HTTP/HTTPS. SOAP forms the foundation layer of the web services protocol stack providing a basic messaging framework upon which abstract layers can be built.

SOA Governance – The set of enforceable processes, tools, standards and organizational structure that allows for the effective creation, reuse and retirement of services.

SOA Governor Team – Centralized organizational body assigned to protect the interests of the enterprise.

SOA Metrics – SOA Metrics measure outcomes that characterize the performance and value of our services and actions.

SOA Service – An enterprise service that is based on the principles of service oriented architecture.

SOA Watch List – ideas that are being considered for new enterprise services.

System Development Life Cycle (SDLC) – A model that describes the stages involved in an information system development project from an initial feasibility study through maintenance of the completed application.

SOA Lifecycle – a model that describes the stages involved in a SOA service from initiation through operations and retirement.

SOA Ownership – The owners of service assets that ensure that these assets serve in the best interests of the consumer and the enterprise. Owners are held accountable for the part they own.

SOA Portfolio Management - The management of that collection of SOA services in which an organization invests (develops, maintains, operates, and retires) to implement its SOA strategy.

SOA Version Management - refers to the policies and procedures around the management of multiple revisions of a single SOA service.

The Open Group Architectural Framework (TOGAF) – A framework for Enterprise Architecture which provides a comprehensive approach to the design, planning, implementation, and governance of an enterprise information architecture. The architecture is typically modeled at four levels or domains; Business, Application, Data, Technology.

Transition Planning and Support – The Process responsible for planning all Service Transition Processes and co-coordinating the resources that they require. These Service Transition Processes are Change Management, Service Asset and Configuration Management, Release and Deployment Management, Service Validation and Testing, Evaluation, and Knowledge Management (ITIL).

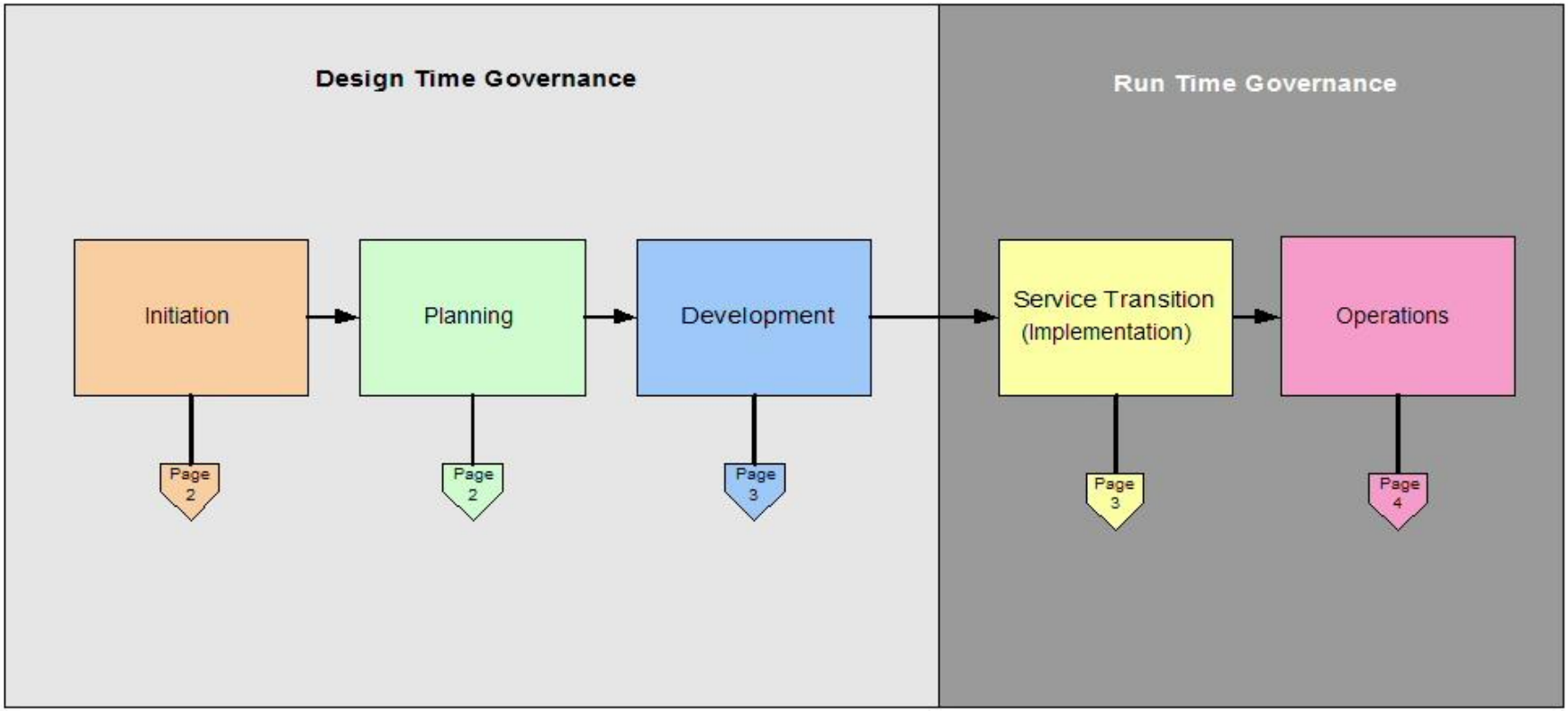
User – A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly (ITIL).

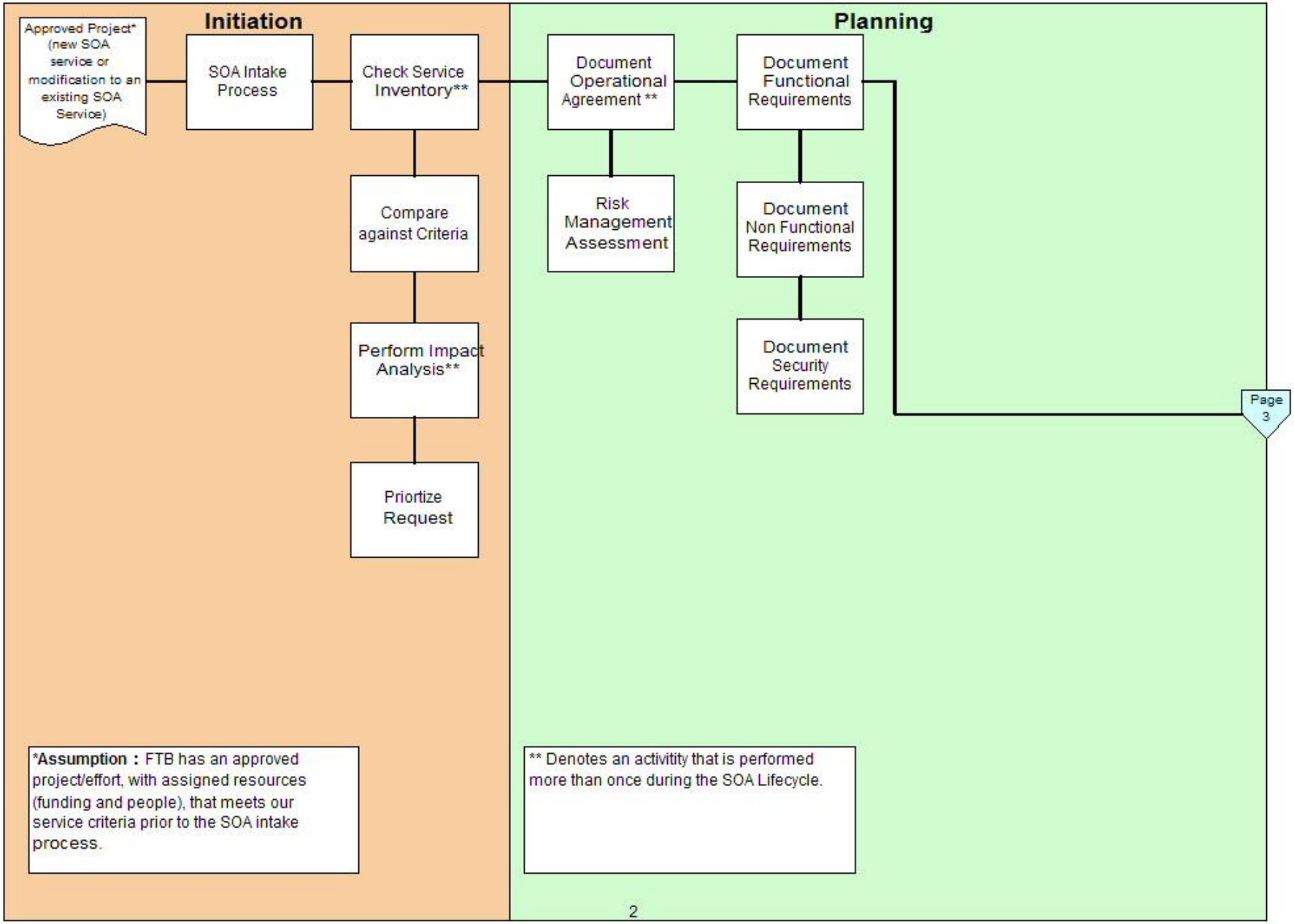
Version - Software versioning is the process of assigning either unique version names or unique version numbers to unique states of computer software.

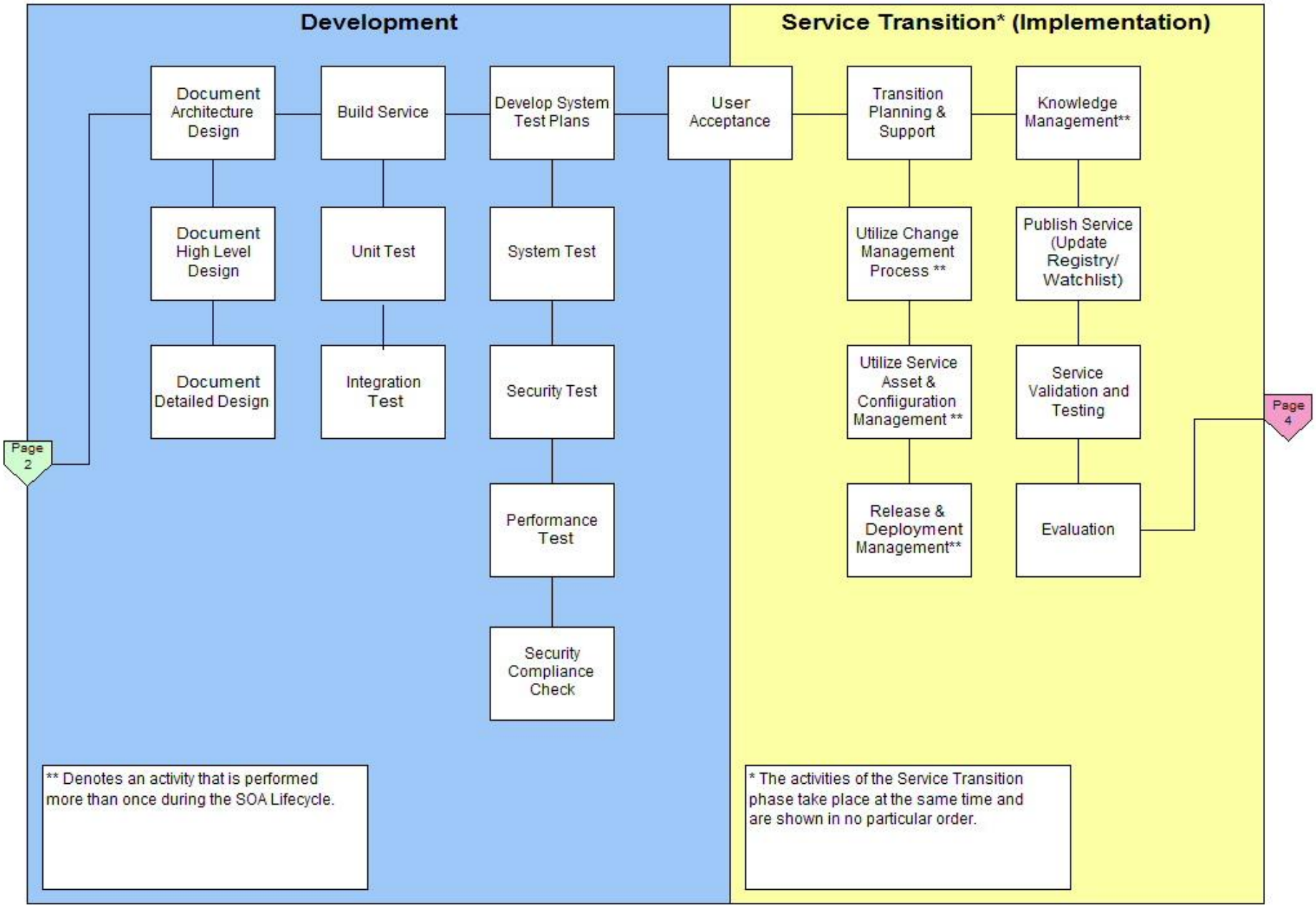
Glossary

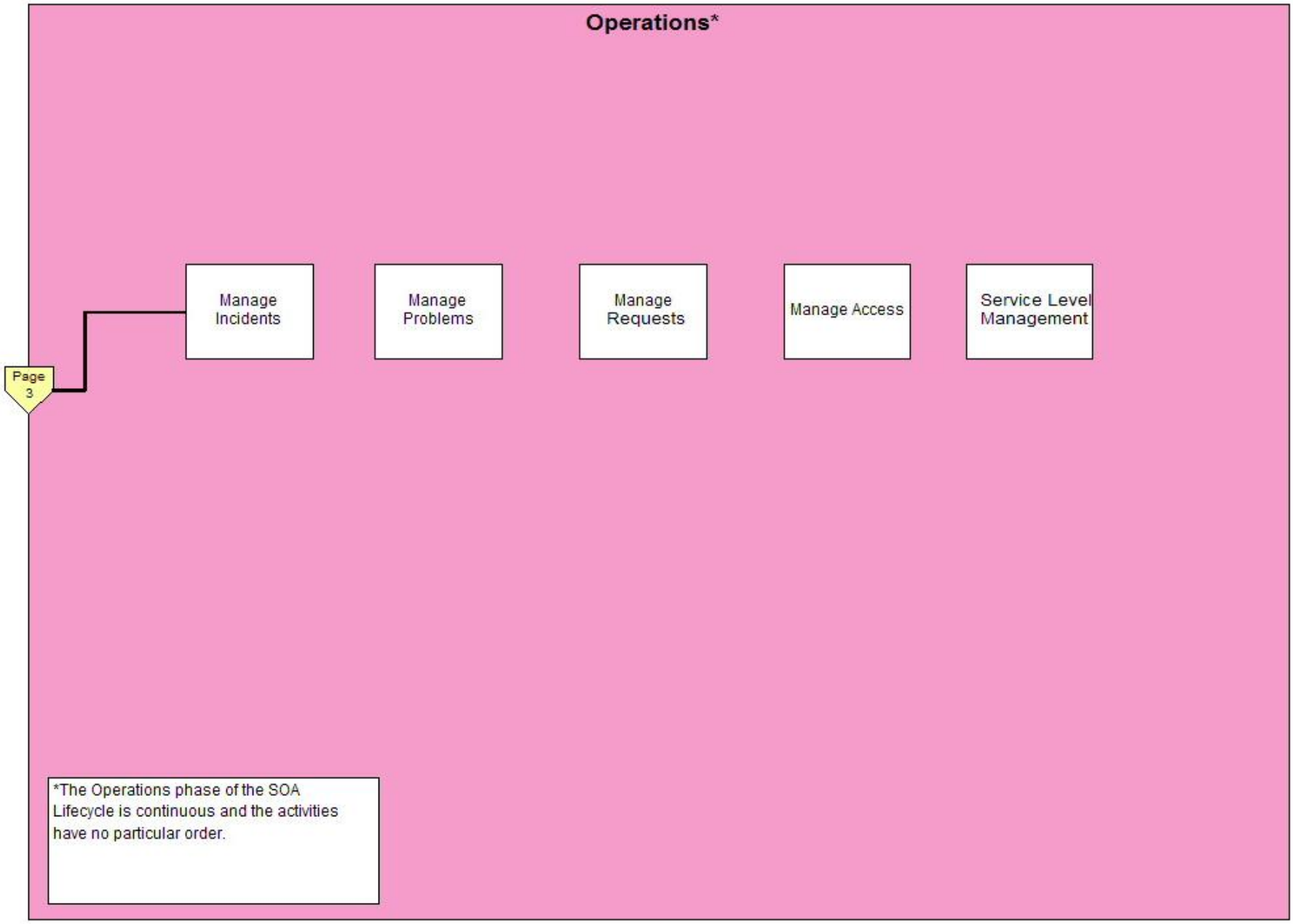
Web Service – A service with encapsulated logic used for transforming and/or transferring structured data to disparate systems regardless of platform or programming language. It is capable of being accessed via standard network protocols such as but not limited to SOAP over HTTP.

WSDL (Web Service Description Language) – An XML-based service description that describes how client applications can communicate with the web service endpoints or ports as they are called (SOA EAD).

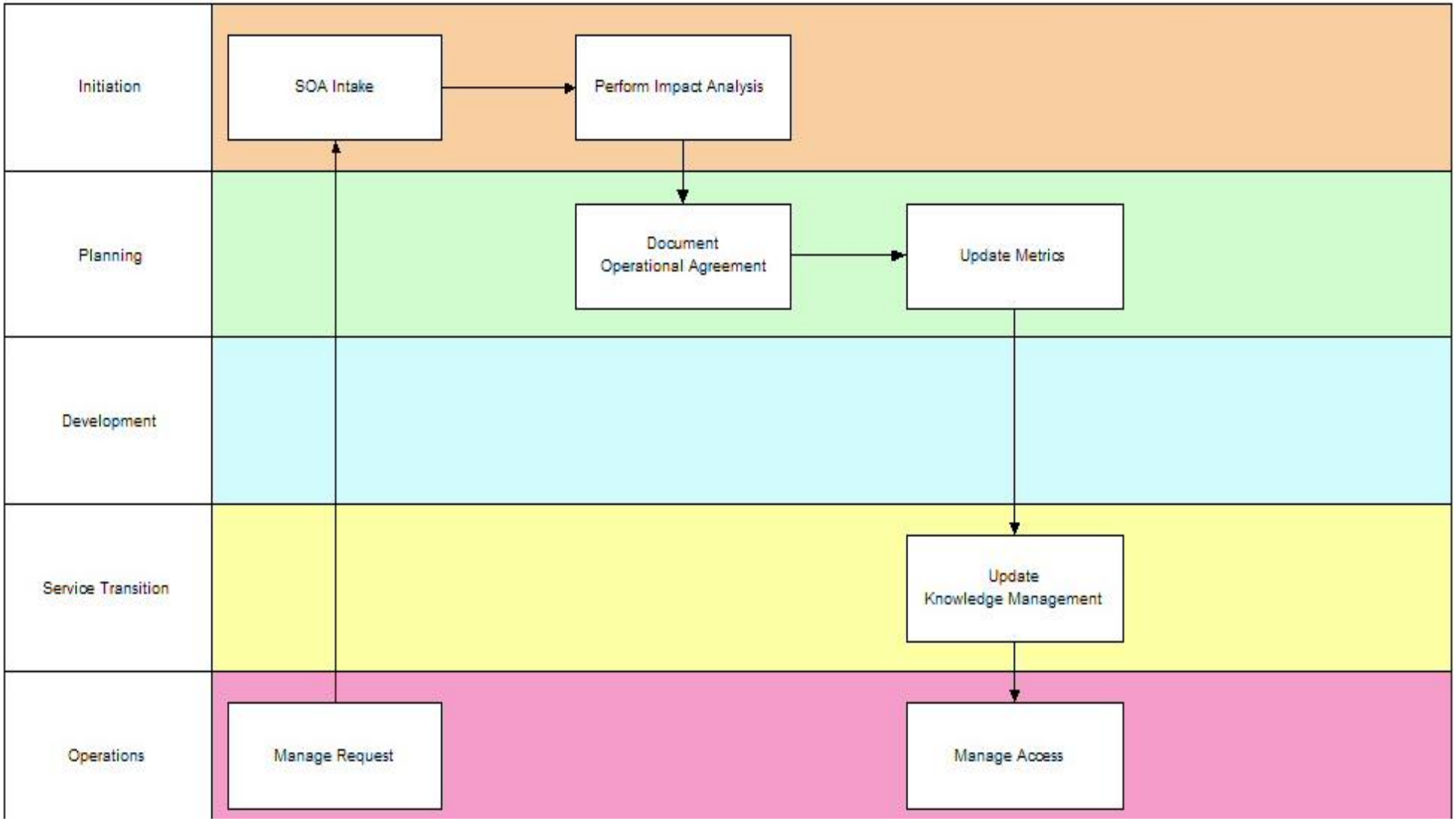

Design Time Governance
Run Time Governance
Initiation
Planning
Development
Service Transition
(Implementation)
Operations
Page 2
Page 2
Page 3
Page 3
Page 4


Initiation
Planning
Approved Project* (new SOA service or modification to an existing SOA Service)
SOA Intake Process
Check Service Inventory**
Compare against Criteria
Perform Impact Analysis**
Priortize Request
Document Operational Agreement **
Risk Management Assessment
Document Functional Requirements
Document Non Functional Requirements
Document Security Requirements
Page 3
*Assumption : FTB has an approved project/effort, with assigned resources (funding and people), that meets our service criteria prior to the SOA intake process.
** Denotes an activitity that is performed more than once during the SOA Lifecycle.


Development
Service Transition* (Implementation)
Document Architecture Design
Build Service
Develop System Test Plans
User Acceptance
Transition Planning & Support
Knowledge Management**
Document High Level Design
Unit Test
System Test
Utilize Change Management Process **
Publish Service (Update Registry/ Watchlist)
Document Detailed Design
Integration Test
Security Test
Utilize Service Asset & Confiiguration Management **
Service Validation and Testing
Page 2
Performance Test
Release & Deployment Management**
Evaluation
Page 4
Security Compliance Check
** Denotes an activity that is performed more than once during the SOA Lifecycle.
* The activities of the Service Transition phase take place at the same time and are shown in no particular order.


Operations*
Manage Incidents
Manage Problems
Manage Requests
Manage Access
Service Level Management
Page 3
*The Operations phase of the SOA Lifecycle is continuous and the activities have no particular order.

Consume(Deconsume) a Service



SOA Lifecycle Activity Definitions

	Activity	Description	Major Input	Major Outputs	Signoff Resp*
Initiation	SOA Intake Process	A project came in through the EA Assurance process and it was determined that there is potential to create, modify, consume (reuse) or retire a SOA service.	Initial Project Documentation (Annual Changes, Scheduled Releases, ITPC's, FSR's, Project Notices)	Initial Project Documentation (Annual Changes, Scheduled Releases, ITPC's, FSR's, Project Notices)	
	Check Service Inventory**	Check the registry for an existing service	Initial Project Documentation Enterprise Services Registry	EA Findings Report	
	Compare Against Criteria	The SOA Governor Team compares the project description against the service criteria to determine a service candidate.	Initial Project Documentation, SOA Watch List, Service Criteria	Criteria Analysis (EA Findings Report)	
	Perform Impact Analysis**	Analysis of a proposed change (e.g. service request or project) and its net positive or negative impact (risk) on the environment in which it would be implemented (including business programs, applications, and related business areas). Said another way, an impact analysis is the process of assessing the merits of pursuing and implementing a project or service request.	Initial Project Documentation	Level of Impact (EA Findings Report)	
	Prioritize Request in SOA Portfolio	Assessment of criticality is performed and the SOA Watch List is updated.	Initial Project Documentation, SOA Watch List	Recommendation & Timing (EA Findings Report) Updated SOA Watch List	
	Milestone	Initiation complete			Service Solution Architect*

	Activity	Description	Major Input	Major Outputs	Signoff Resp*
Planning	Define and Document Operational Agreement**	An agreement between the provider(s) of a service and the consumers that describes performance expectations and defines ownership responsibilities for the SOA Service (in the absence of a SLA/OLA).	Initial Project Documentation, EA Findings Report	Draft Operational Agreement	
	Risk Management Assessment	Assessment of implementation risk - such areas include resources, hardware, software, project schedule.	EA Findings Report, Project Schedule	Draft Risk Management Plan	
	Document Functional Requirements	Identify enterprise business requirements for the SOA service	EA Findings Report, Draft Risk Management Plan	Functional requirements document, Revised Operational Agreement, Revised Risk Management Plan	Business Owner
	Document Non-Functional Requirements	Identify enterprise non functional requirements for SOA	EA Findings Report, Operational agreement, Draft Risk Management Plan	Non-functional requirement document, Revised Operational Agreement, Revised Risk Management Plan	Business Owner
	Document Security Requirements	Identify Security Requirements for the SOA service	EA Findings Report, Operational agreement, Draft Risk Management Plan	Security requirements document, Revised Operational Agreement, Revised Risk Management Plan	Business Owner, Security
	Milestone	Requirements and planning complete			

	Activity	Description	Major Input	Major Outputs	Signoff Resp*
Development	Document Architecture Design	A description and diagram showing the interfaces and infrastructure components.	Completed Requirements Package	Architecture Diagram	EA Service Solution Architect
	Document High Level Design	Process flow(s) with inputs and outputs	Architecture Diagram, Completed Requirements Package	High-level Design (functional flow)	EA Service Solution Architect
	Document Detailed Design	A detailed description of the service, inputs, outputs, the process, data, and interfaces.	Architecture diagram, Enterprise Requirements, High-level Design	Design Package	Technical Development Owner (TDO)
	Milestone	Design Complete			
	Build Service	Develop all necessary business logic and connectors to enable service operation.	Design Package	Compiled Service Ready for Testing (code)	
	Unit Test	Create unit test plan and test application logic within the service.	Design Package	Unit Test Plan, Unit Tested Service ready for system testing	TDO
	Integration Test	Test service from end to end to detect any inconsistencies between the software units that are integrated together.	Unit Tested Service	Integration Tested Service	TDO
	Develop Test Plans	Test plan including documented scenarios based upon functional and non-functional requirements.	Enterprise Requirements	Test Plans (System, Security, Performance, etc)	TDO
	System Test	The process to evaluate that the service meets the functional and non-functional requirements.	System Test Plan, Integration Tested Service	Defect and Change Control System Tested Service	TDO, TIO
	Security Test	The process to evaluate that the service's functionality meets security requirements.	Security Requirements, System Tested Service	Defect and Change Control	Security
	Performance Test	The process to ensure that the service meets performance requirements.	Non-Functional Requirements System Tested Service	Defect and Change Control	TDO, TIO
	Security Compliance Check	The process to ensure that the service complies with security policies and standards (e.g., Penetration testing, scanning, etc).	Security Policy and Standards, System Tested Service	Defect and Change Control	Security
	User Acceptance	The process to ensure that the service meets customer requirements.	Fully Tested Service	Customer Approval	Business Owner
	Milestone	Service Development complete			

	Activity	Description	Major Input	Major Outputs	Signoff Resp*
Service Transition	Transition Planning and Support	The Process responsible for planning all Service Transition Processes and co-coordinating the resources that they require.	All Major Outputs	Transition Strategy, Service Transition Plan	Operations
	Utilize Change Management Process**	The Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services (ITIL). This process takes place prior to go live.	IT Change Request	Approved or Rejected IT Change Request	Change Advisory Board (CAB)
	Utilize Service Asset & Configuration Management**	The process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships (ITIL).	Approved IT Change Request, Design Package	Updates to asset CIs in the system of record (Unicenter).	Asset Mgr, Config Mgr
	Release & Deployment Management**	The process responsible for planning, scheduling and controlling the movement of Releases to Test and Live Environments (Including retirement).	Release and Deployment checklist	Completed release and deployment checklist, Implementation Test Plan	As described in the RDM Process
	Knowledge Management**	The Process responsible for gathering, analyzing, storing and sharing knowledge and information within an Organization.	Operational Agreement, Design Package	All are posted in the system of record (Unicenter Knowledge Management System).	Knowledge Manager
	Publish Service	Making known the service definition and state so that the service can be found and used by consumers.	Completed release and deployment checklist, SOA Watchlist, SOA Registry	Published service, updated SOA Watchlist, updated SOA Registry	Operational Owner
	Service Validation & Testing	The process to ensure that a new or changed service and its associated release process will meet the needs of the business (utility and warranty) at the agreed cost (ITIL).	Requirements Package, Operational Agreement, Implementation Test Plan	Test Results, Defect and Change Control, updated Knowledge Management System (KMS).	Service Transition Manager
	Evaluation	A process that considers whether the performance of something is acceptable, value for money, fit for purpose, and whether implementation can proceed based on defined and agreed criteria (ITIL).	Approved IT Change Request, Design Package, Implementation Test Plan and Results	Evaluation report	Service Transition Manager
	Milestone	Service Certified			

Operations

Activity	Description	Major Input	Major Outputs	Signoff Resp*
Manage Incidents	The Process responsible for managing the Lifecycle of all Incidents. (ITIL). The primary Objective of Incident Management is to return the IT Service to Users as quickly as possible (ITIL).	State of Configuration Item, User contact	Incident Report, Incident Ticket, IT Change Request, workarounds, Problem Ticket, updated System Status Page	
Manage Problems	The Process responsible for managing the Lifecycle of all Problems. (ITIL).	Problem Ticket, Incident Details, configuration details from the KMS and OAs. Details about the infrastructure and the way it behaves, such as capacity records, performance measurements, and service level reports, etc.	Problem Ticket, updated Known Error Database, IT Change Request, problem resolution, workaround, updated System Status page	
Manage Requests	The Process responsible for managing the Lifecycle of all Service Requests (ITIL).	Request to consume	Request disposition (approved (including security), denied, sent for funding, etc.)	
Manage Access	The Process responsible for allowing Users to make use of IT Services, data, or other Assets. ITIL).	Approved request to consume	Access granted	
Service Level Management	The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews (ITIL).	Metrics, OA (SLA, OLA), ITIL Processes.	Updated OAs, Service Level Report	

* Sign-off responsibility is met by following the Enterprise Service Sign-off Template. Operations phase - normal operations; no sign-off required

** Activity that is performed more than once during the SOA Lifecycle

SOA RACI Diagram

R- Responsible
A- Accountable
C- Consulted
I- Informed

		Business Owner	Technical Development Owner	Technical Infrastructure Owner	Operational Owner	SOA Governor Team	SOA Project Manager	Security	EA Project Solution Architect	EA Service Solution Architect	Service Registry Administrator	Application Experts	Service Level Administrator	Business Analyst	Developer	System Tester	Infrastructure Technician	Service Transition Manager	Service Transition Technician	Service Desk Analyst	SOA Monitor	Problem Manager
Initiation	SOA Intake Process								A													
	Check Service Inventory					R			C	A												
	Compare against Criteria					R	C		C	A												
	Perform Impact Analysis	C	C	C	I	R	C		C	A		C	C									
	Prioritize Request	C	C			R	C		C	A	C						C					
Planning	Define/Document Operational Agrmt.	C	C	C	C	I	A	I	I	I			R									
	Risk Management	A	C	C	C		R		C	C		C										
	Doc Functional Requirements	A	C	I	I	I	I	I	I	I				R	C	I						
	Doc Non-Functional Requirements	A	C	C	I	I	I	I	I	I				R	C	I	I					
	Doc Security Requirements	A	C	C	I	I	I	R	I	I				I	I	I						
Development	Document Architecture Design			C			I		C	A					R	I	C					
	Document High Level Design		C	C			I			A					R	I	C					
	Document Detailed Service Design		A	C			I			I					R	I	C					
	Build Service		A				I							C	R	I	I					
	Develop Test Plans		A				I	C						C	C	R	I	C			C	
	Unit Test		A				I							I	R	C	I					
	Integration Test		A				I							I	R	I	I					
	System Test		A	C			I							I	C	R	I					
	Security Test						I	A						I	C	R	C					
	Performance Test		A	C			I							I	C	R	I					
	Security Compliance Check		I	I			A	R							C		C					
	User Acceptance	A	R				I							C	C	I		I				
Service Transition	Transition Planning & Support	I					C	C						C	C	C	C	A	R	C	C	
	Utilize Change Mgmt Process	I													R		R	A	C			
	Utilize Service Asset & Configuration Mgmt			C											C		C	A	R		C	
	Release & Deployment Mgmt	I	I	I	I		I	C							C		C	A	R			
	Knowledge Management				I										C		C	A	R	I	I	I
	Publish Service		R	R	A	I				I	C				C		C	R				
	Service Validation & Testing														C		C	A	R		C	C
	Evaluation	I	C	C	I	C	C	C	C	C					C		C	A	R			
Operations	Manage Incidents from Events/Users	C	C	R	A										C		C			R	R	I
	Manage Problems	C	R	R	A										C	C	C			I	C	R
	Manage Requests		I	I	A	C				C										R	I	
	Manage Access		I	I	A	C				C							C			R	I	
	Service Level Management	C			A								I					R		R	R	

SOA Roles and Responsibilities

(Roles are in the order as they appear on the SOA Governance RACI)

Business Owner

- Conceiver or user of the service
- Judges the business impact of any changes or enhancements to the service
- Defines service requirements – functional and non functional
- Acceptance Testing

Technical Development Owner

- Design Service
- Service interface definitions
- Schema definitions
- Document service architecture
- Technical documentation
- Build Service
- Test Service
- Ensures service follows enterprise standards and best practices

They work with the business owners to understand the service requirements and implement the service. In some cases, they may need to work with a different group to implement all or part of the business or access logic.

Technical Infrastructure Owner

- Responsible for the hardware and software used by SOA Services.
- Responsible for ensuring non functional requirements are met
- Respond to incidents as prescribed in the OLAs
- Ensures service follows enterprise standards and best practices
- Technical documentation

Operational Owner

- Responsible for maintaining the service in the operational life cycle of the service.
- Owns the "runtime instances" of the services
- Makes changes to the runtime instances and configuration in order to meet SLAs and OLAs for SOA services
- Gathers operational metrics and provides back to the Service Level Administrator for continuously improving service capabilities
- Coordinator among the various owners and stakeholders for run time incidents (responsible for these activities – may leverage groups within the enterprise to execute them)

SOA Roles and Responsibilities

SOA Governor Team
Centralized organizational body assigned to protect the interests of the enterprise.

- Performs impact analysis
- Prioritizes SOA Service requests
- Manages portfolio of SOA Services
- Controls the adoption of service definitions into the shared registry, and is responsible for controlling consistency and quality of the design of services
- Promote reuse and mediate between parties to accelerate the adoption of the services
- Mediates requests between consumers and other parties for access, changes and enhancements
- Understands the value of the services
- Manages SOA Lifecycle
- Recommends policy changes to TAC
- Recommends performance and governance metrics
- Responsible for the continuous improvement of the SOA Governance Model
- Updates SOA Roadmap and provides feedback to the SOA Enterprise Architecture Definition (EAD)

SOA Project Manager

- Create and monitors the project schedule
- Ensures the SOA governance process is followed
- Synchronizes the development and release of the service with the development and release schedules of the consumer(s)
- Coordinates among the various owners and stakeholders during “design time” of the SOA service

Security

- Defines and documents SOA security requirements according to security policy
- Ensures security requirements are met

EA Project Solution Architect

- Works with the Project Manager to ensure all EA processes are understood and followed

EA Service Solution Architect

- Compare potential service to the service criteria
- Check the service catalog – does it already exist?
- Make recommendations regarding service development, consumption and modifications
- Updates the SOA Enterprise Architecture Definition (EAD)
- Leads the SOA Governor Team

Service Registry Administrator

- Manages the consistency of the service registry
- Enforces guidelines that protect against redundancy, proliferation and unauthorized modifications of the service registry
- Updates the registry

SOA Roles and Responsibilities

Application Experts

- Point of contact to determine the impact of a SOA service to an application area. For example, a new service could replace something they already have, or a service change could be an impact to their area, or an existing service could be reused to meet their needs.

Service Level Administrator

- Create the SLA based on functional requirements
- Creates OLAs based on nonfunctional requirements
- Establish metrics for SOA service
- Defines ownership of SOA service
- Signoff of SLAs/OLAs
- Annual review of SLA/OLA for SOA services
- Ensures that the services are supported by the appropriate owners until they are retired.

Business Analyst

- Defines and documents functional requirements
- Defines and documents non functional requirements

Developer

- Designs the service
- Code service to enterprise standards and best practices
- Unit tests the service
- Integration tests the service
- Assists with performance and security testing

System Tester

- Develop test cases based on functional and nonfunctional requirements
- Performs System Testing based on test cases developed
- Performs Performance Testing
- Performs Security Testing
- Facilitates Acceptance Testing

Infrastructure Technician

- Hardware planning and support for SOA services
- Systems software (Websphere, registry repository, ESB) planning and support for SOA services

Service Transition Manager

- Coordinates the release and retirement of service versions among the owners and consumers
- Accountable for user acceptance testing

Service Transition Technician

- Performs service transition tasks

Service Desk Analyst

- Supplies help desk services

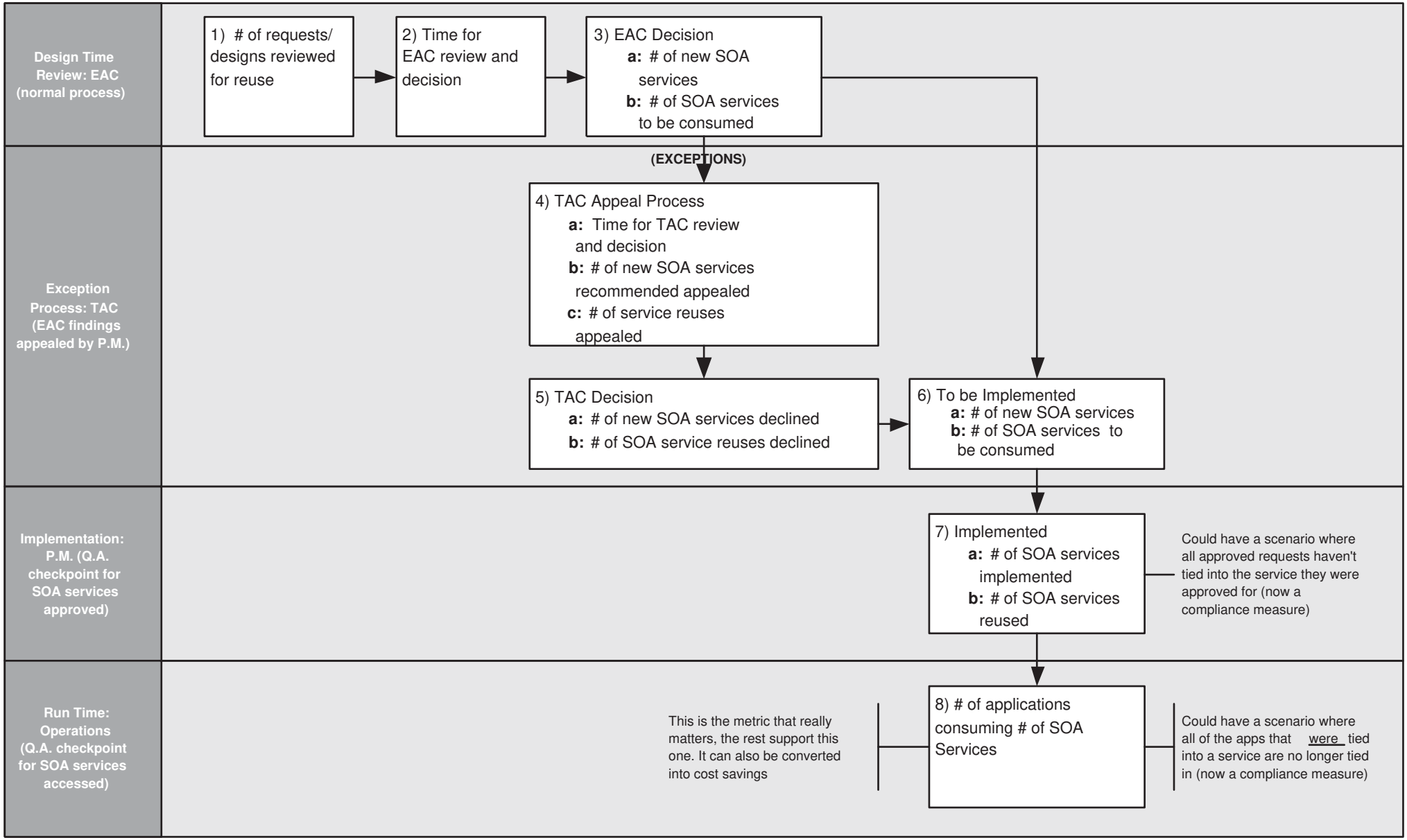
SOA Monitor

- Measure the performance of SOA services

Problem Manager

- Problem resolution coordinator (ongoing problems with SOA services)

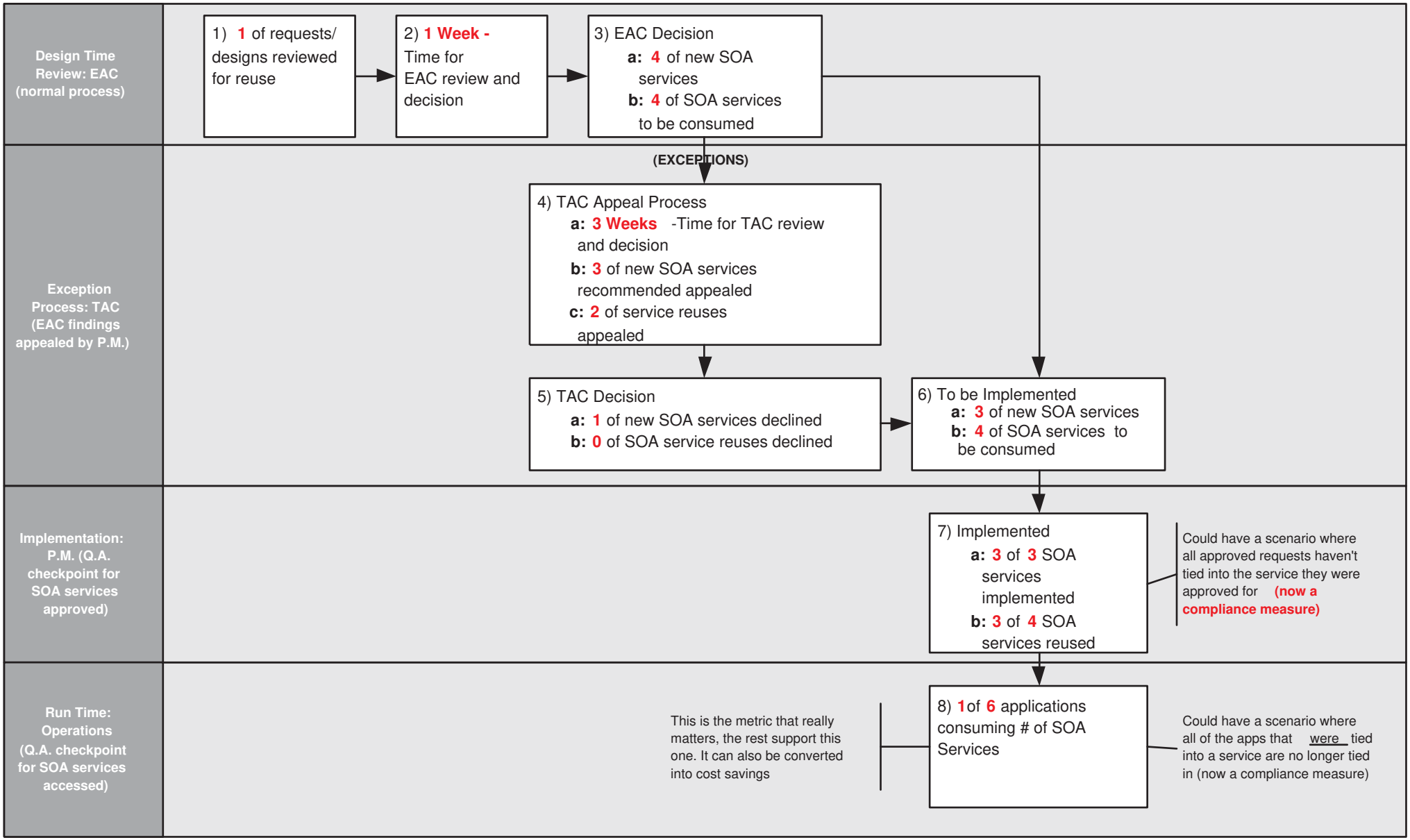
SOA Governance Value Measure: Reuse of SOA Services



NOTES:

1) Request = project (FSR or PN), annual change release, major release.
2) Over time this would be an average per request metric.
3a) Future cost savings for other projects. 3b. Current savings to the project.
4a) Over time this would be an average per exception metric.

SOA Governance Value Measure: Reuse of SOA Services (Example)



NOTES:

1) Request = project (FSR or PN), annual change release, major release.
2) Over time this would be an average per request metric.
3a) Future cost savings for other projects. 3b. Current savings to the project.
4a) Over time this would be an average per exception metric.
4b) 3 of the 4 new SOA services were not agreeable to the project team.
4c) 2 0f the 4 SOA service reuses were not agreeable to the project team.
7a) All services were implemented.
7b) 1 service reuse missing at implementation.

State of California
Franchise Tax Board

IT Policy

SUBJECT: Service-Oriented Architecture (SOA) Governance	**NUMBER:** ITP 09-XX
	DATE ISSUED: | DATE LAST REVIEWED/REVISED [Insert date] | [Insert date]
	EXPIRES: Until rescinded
REFERENCES: SOA Governance Final Report SOA Lifecycle (Flow Chart/Activity Definition) ; SOA RACI SOA Glossary SOA Standards	**POLICY TOPIC: | POLICY OWNER** Enterprise Architecture | TSD Planning & Support Bureau Director, Carlos Quant

POLICY

Enterprise services are created, modified, used, and retired via the Service-Oriented Architecture (SOA) governance model as described in the SOA Governance Final Report.

PURPOSE

The purpose of the SOA Governance policy is to ensure that:

- Certified SOA services meet the business needs of FTB; change is driven by enterprise-wide need.
- Operational and support risk is minimized by having controlled and registered services. Standards are set for documentation; versions are controlled; performance is considered at the enterprise level; appropriate diagnostic data is available.
- Standardized methods and procedures are used for efficient and prompt handling of changes.

DEFINITIONS

Version: Software versioning is the process of assigning either unique version names or unique version numbers to unique states of computer software.

Service Oriented Architecture (SOA) – A framework for integrating business processes and supporting IT infrastructure as secure, standardized components — services — that can be

reused and combined to address changing business priorities and is based on the following design principles:

Design Principles of SOA

- *Technology Neutral* – Uses industry agreed upon standards to create interfaces, which make it possible for consumers on any platform to invoke services provided on any platform.
- *Modular* – Self-contained components that can communicate with each other through a well-defined interface.
- *Sharable* – Can be reused by more than one functional area.
- *Loose Coupling* (agility) – Ability to make changes to one part of the system without changing the other – each component offers a small range of simple services to other components.
- *Encapsulation* – Focus is on the interface rather than the underlying implementation details - hides any data or behavior that is specific only to the internal working or the service and irrelevant to the service consumer.

Enterprise Service – A certified SOA service that is reusable across FTB has enterprise-level requirements and is centrally managed.

APPLICABILITY

This policy applies to all Enterprise Services. It does not apply to Local Services. SOA standards covered by this policy are referenced in the SOA Governance Final Report. .

CONTACT

Cheryl Deagon

SOA Solution Architect
Enterprise Architecture Council (EAC)
California Franchise Tax Board
Phone: (916) 845-6170

Carl Engel

Chief Architect
Enterprise Architecture Council (EAC)
California Franchise Tax Board
Phone: (916) 845-4954

SIGNATURE

Carlos Quant
Bureau Director, TSD Planning & Support Bureau
Franchise Tax Board

SOA Version Standard --- draft 10/29/09, adapted from Eclipse Wiki:

http://wiki.eclipse.org/index.php/Version_Numbering#When_to_change_the_major_segment

This document contains the FTB SOA standard for expressing how to evolve enterprise service version numbers in a way that captures the nature of the changes that have been made.

Standard Statement:

Only two versions (v and v-1) of an Enterprise Service will be in production at any given time. Upon publication of a new version (v), Consumers of v-1 will be given one year to transition to the new version.

Version Number Assignments:

Version numbers are composed of four (4) segments: 3 integers and a string respectively named major.minor.service.qualifier.

Each segment captures a different intent:

- the major segment indicates breakage in the service (version number is part of the service name)
- the minor segment indicates "externally visible" changes
- the service segment indicates bug fixes and the change of development stream
- the qualifier segment indicates a particular build (used only for development iterations)

When to change the major segment

The major segment number must be increased when a service makes breaking changes. When the major segment is changed the minor and service segments are reset to 0. A breaking change is created when new functionality or new interface parameters cause an existing version to be inoperable.

Example: From the version 2.2.7, an incompatible change would lead to 3.0.0. By definition, such changes should not be made when working in a maintenance stream.

When to change the minor segment

The minor segment number must be incremented when a service changes in an "externally visible" way. Examples of externally visible changes include significant performance changes, major code rework, etc. Another way to know when this version number should be changed is by exclusion: it should indicate change that is a neither bug fix (indicated by the service segment) or a breaking change (indicated by the major segment). When the minor segment is changed, the service segment is reset to 0.

Example: From the version 2.2.7, a minor change would lead to 2.3.0.

When to change the service segment

The service segment number must be incremented whenever there have been changes to a service between releases that are not visible. For example, a bug has been fixed in the code, the service manifest has changed, documentation has changed, compiler settings have changed, etc. In addition, incrementing the version number by one hundred (100) indicates a change of development stream. This increment must be done when the first change is made in a new development stream.

Example: At the end of the development stream N, the version of the service S is 2.4.8. When S makes its first change in the development stream N+1, then the version should be changed to 2.4.108. If S version 2.4.8 needs to receive a bug fix in the maintenance stream started from N, then its version number will be 2.4.9.

Overall example

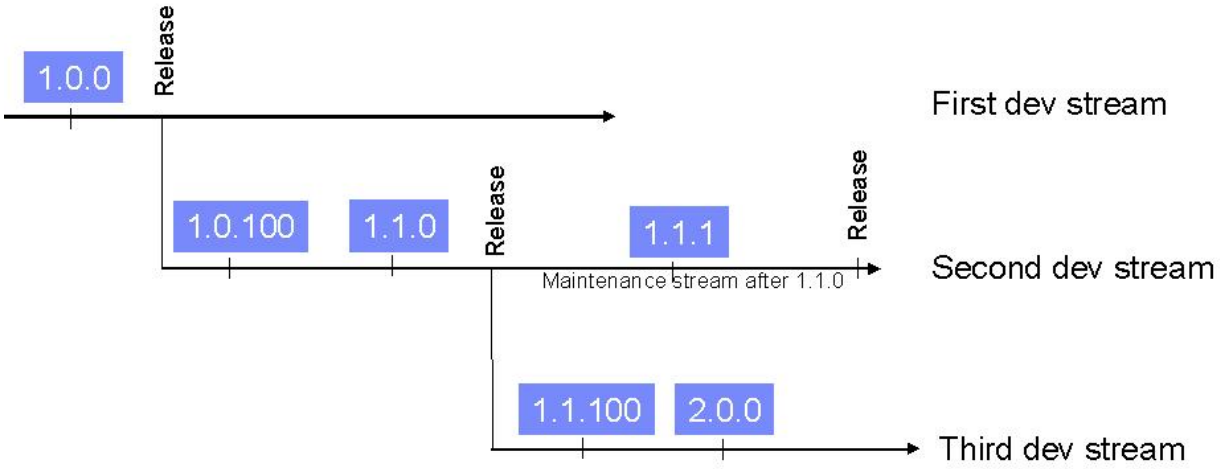
This example shows how the version of a service reacts to changes (indicated in parenthesis) in the context of different development stream. Both the text and the diagram illustrate the same example.

```
First development stream
 - 1.0.0

Second development stream
 - 1.0.100 (indicates a bug fix)
 - 1.1.0 (a new release has been introduced)
 The service goes into production as 1.1.0

Third development stream
 - 1.1.100 (indicates a bug fix)
 - 2.0.0 (indicates a breaking change)
 The service goes into production as 2.0.0

Maintenance stream after 1.1.0
 - 1.1.1
 The service goes into production as 1.1.1
```


1.0.0
Release
First dev stream
1.0.100
1.1.0
Release
1.1.1
Release
Second dev stream
Maintenance stream after 1.1.0
1.1.100
2.0.0
Third dev stream

Service Oriented Architecture

Enterprise Service Sign-Off Procedure

Overview

The SOA Project Manager (PM) is responsible to obtain all sign-offs required by the Enterprise Service Sign-off Template before the service is allowed to proceed into a fully operational state. In order to get final sign-off, the SOA PM ensures that the SOA Governance Model is followed and milestones defined in the SOA Lifecycle are met.

References

- Enterprise Service Sign-off Template <link>
- SOA Governance Model <link>
- SOA Lifecycle <link>

Process

SOA PM:

1. Obtains the template
2. Ensures that the template is routed to the key signatories
3. Provides a copy of the signed template to the Business Owner, Operational Owner, SOA Monitor
4. Maintains a record of the sign-offs on the SOA system of record

Enterprise Service Sign-off Template

(use for a new or modified service)

Enterprise Service Name: _____

Project Name: _____

Project Manager: _____

SOA Project Manager:_____(*if different than Project Manager*)_____

Brief description of service:

Milestone	Deliverable	Date	Signature(s)	Description
Initiation	EA Findings Report; Updated SOA Watch List	MM/DD/YYYY	Service Solution Architect	I have reviewed and approved the Findings Report for the service named above. The SOA Watch List has been updated. **I hereby approve proceeding to the Planning and Requirements activity within the SOA Lifecycle.**
Requirements (package includes functional, non-functional, and security requirements; **all requirements must be verifiable through testing**)				
Functional	Functional requirements document	MM/DD/YYYY	Business Owner	I have reviewed and approved the service functional and non-functional requirements. These requirements represent the enterprise and cover all identified potential consumers' needs.
Non-Functional	Non-functional requirements document			
Security	Security requirements document	MM/DD/YYYY	Business Owner; Security	I have reviewed and approved the security requirements. **I hereby approve proceeding to the Design activity within the SOA Lifecycle**.

Design				
Architecture/ High Level	Architecture diagram; High-level design (functional flow) (first section of the Design Package)	MM/DD/YYYY	Service Solution Architect	I have reviewed and approved the architecture diagram, including the service interfaces and infrastructure components. I have reviewed and approved the High Level Design, including process flow, inputs, and outputs. **I hereby approve proceeding to the Detailed Design Activity within the SOA Lifecycle.**
Detail Design	Detailed Design Doc; Technical Specs Doc (second section of the Design Package)	MM/DD/YYYY	Technical Development Owner	I have reviewed and approved the detailed design and technical specification documents. **I hereby approve proceeding to the Build Activity within the SOA Lifecycle.**
Develop				
Build; Unit/ Integration Tests	Unit tested compiled service; Unit Test Plan	MM/DD/YYYY	Technical Development Owner	I have reviewed and approved the Unit Test Plan. End-to-end test results (request/response model) are satisfactory. **I hereby approve proceeding to the System Test activity within the SOA Lifecycle**
Test				
System (functional) System (non-functional) Performance	Defect & Chg. Control **Note:** Defect=ClearQuest Chg. Cntl=Unicenter (production)	MM/DD/YYYY	Technical Development Owner	I have reviewed the test plans. Test results are satisfactory. The service meets the functional and non-functional requirements, including performance requirements. Critical defects have been fixed; Change Control requests have been added to code or deferred. Service design documentation has been updated. **I hereby approve test results for these tests.** **Note: Proceeding to the Transition Activity requires System Testing, Security Testing, and User Acceptance Testing sign-offs.**

Security	Defect & Chg. Control	MM/DD/YYYY	Security	Test results are satisfactory. The service functionality meets the security requirements. Critical defects have been fixed; Change Control requests have been added to code or deferred.
Security compliance	Defect & Chg. Control			The service complies with security policies and standards. **I hereby approve proceeding to the Transition activity within the SOA Lifecycle.** **Note: Proceeding to the Transition Activity requires System Testing, Security Testing, and User Acceptance Testing sign-offs.**
User Acceptance	Defect & Chg. Control	MM/DD/YYYY	Business Owner	The UAT is complete. Requirement defects have been fixed; Change Control requests have been added to code or deferred. **I hereby accept that the service meets the business requirements. I hereby approved proceeding to the Transition Activity within the SOA Lifecycle.** **Note: Proceeding to the Transition Activity requires System Testing, Security Testing, and User Acceptance Testing sign-offs.**
Transition				
Release & Deployment	Completed Release & Deployment (RDM) Checklist	MM/DD/YYYY	Service Transition Mgr.	I have reviewed the Service Design Package and the Release & Deployment Checklist. All plans are in place; communication ready for this service to be deployed to the production environment. **I hereby authorize approve proceeding to the Operations activities within the SOA Lifecycle. (Release to Production Environment requires approval of the following: Transition plan, Operational Agreement, and Risk Mgt Plan)**

Operational Agreement	Operational Agreement	MM/DD/YYYY	Operational Owner; Business Owner	I have reviewed and approved the OA for the service named above. Service Owners have been assigned; current consumers have been identified. **I hereby approve proceeding to the Operations activities within the SOA Lifecycle. (Release to Production Environment requires approval of the following: Transition plan, Operational Agreement, and Risk Mgt Plan)**
Risk Mgt.	Risk Management Plan	MM/DD/YYYY	Business Owner	The Project's Risk Management Plan has been updated with risks and mitigation strategies as necessary. **I hereby approve proceeding to the Operations activities within the SOA Lifecycle. (Release to Production Environment requires approval of the following: Transition plan, Operational Agreement, and Risk Mgt Plan)**
Transition - Evaluation	Evaluation Report	MM/DD/YYYY	Business Owner	Service acceptance criteria have been met. I hereby acknowledge that the Service is operating as expected in the production environment.
When all signatures are complete, SERVICE IS CERTIFIED.				
Operation			N/A	Normal operations; no sign-off required

Enterprise Service
Request to Consume/Deconsume Template

(use for an existing service)

Enterprise Service Name: _____
Version Number: _____

Requestor Name: _____
Phone: _____

Approving Manager's Name: _____

Application Area: _____
PUC: _____

DECONSUMER INFORMATION

This is the only section you need to complete if you are no longer going to be consuming this service.

Application Name: _____

Reason: _____

De-consume Date: _____

CONSUMER INFORMATION

Please complete this section if you are requesting to consume an existing service.

Project Manager: _____ Phone: _____

How did this request originate (from a project, EA, enhancement, or other, please describe):

_____
_____
_____
_____

Date Needed: _____

Have you read the existing Operational Agreement and agree with its terms? Yes / No
If yes, do those terms of service meet your requirements? Yes / No
If not, please contact _____

APPLICATION INFORMATION

Please complete this section if you are requesting to consume an existing service.

Application Name that will consume this service: _____

Please provide brief description of application:

_____
_____
_____

What are the hours of operation for the application? _____

Will you be calling this service Real-time or Batch: _____

Indicate the peak and/or critical time of year and/or day of the week, if any, for this Business Process.

_____January	_____Monday	_____End of Week
_____February	_____Tuesday	_____End of Month
_____March	_____Wednesd ay	_____End of Quarter
_____April	_____Thursday	_____End of Fiscal Year
_____May	_____Friday	_____End of Calendar Year
_____June	_____Saturday	_____Other (please specify)
_____July	_____Sunday	
_____August		
_____September		
_____October		
_____November		
_____December		

Please explain why:

_____
_____
_____
_____
_____

Indicate the relative impact of the loss of this Business Process for each of the time frame slots below. Assume the outage is continuous and occurs during a time of peak business activity.

- CATASTROPHIC – Major financial impact to FTB
- SIGNIFICANT- Major impact to the business processes
- MODERATE –Some business areas can continue operations – minor financial impact
- MINOR – minor impact to application – business areas can continue operations with workarounds. No financial impact.

30 Minutes_____
1 Hour _____
8 Hours _____
16 Hours _____

Comments:
_____
_____
_____

SECURITY

Please complete this section if you are requesting to consume an existing service.

Have you already received Security approval to utilize the data from this service? Yes / No

If yes, please move on to the next section.

Does the service allow access to non FTB agency data? _____

If so, what agency? _____

Does the service allow access to IRS or confidential data (ie: taxpayer info, personnel records, proprietary information, etc)? _____

APPROVALS

This section needs to be completed by EA and Operations.

Approver of Enterprise Service reuse: _____
I have reviewed this request, the impact analysis has been completed and the system is able to handle the new demand.

Approver of Enterprise Service reuse: _____

The Operational Agreement has been updated to add the new consumer. The consumer may move forward with this request.

This comes in through Manage Request – a change order is opened

State of California
Franchise Tax Board

Operation Agreement (OA)

Between

Customer

And

Service Provider

Table of Contents

Skeleton Operational Agreement

OPERATIONAL AGREEMENT FOR THE XXX SERVICE

Version 1.0

dd/mm/yy

Author: whoever

OPERATIONAL AGREEMENT FOR THE XXX SERVICE

This agreement is made between.....

and.....

The agreement covers the provision and support of the XXX **Services** which..... (brief service description).

This agreement remains valid until superseded by a revised agreement mutually endorsed by the signatures below. The agreement will be reviewed annually. Minor Changes may be recorded on the form at the end of the agreement, providing they are mutually endorsed by the two parties.

Version Control

This document is managed by the Service Level Management (SLM) group. Once a new version is issued for review, it will supersede all previous issues. Please discard any previous copy of this document dated before the last version dated below.

Version	Date	Name of Person Making Change	Description of Changes
1.1			
1.2			
1.3			

Submitting Changes

- Contact SLM to notify of the intent to make revisions to the document.
- Submit to SLM the suggested revisions.
- SLM will review, update document, and route to all parties involved for approval.

Roles and Responsibilities:

SOA Monitor – (link to glossary)

Incident Manager - (link to glossary)

Problem Manager - (link to glossary)

Configuration Manager- (link to glossary)

SOA Service Owner

Technical Development Owner

Technical Infrastructure Owner

Operational Owner

Business Representative

Service Description:

The ABC Service consists of .... (fuller description to include key **Business functions**, deliverables and all relevant information to describe the service and its scale, **Impact** and **Priority** for the business).

Service Hours

A description of the hours that the Customers can expect the service to be available (e.g. 7 x 24 x 365, 08:00 to 18:00 - Monday to Friday).

Special conditions for exceptions (e.g. weekends, public holidays etc).

Procedures for requesting service extensions (who to contact - *normally the **SOA*** Monitor - and what notice periods are required).

Details of any pre-agreed maintenance or housekeeping slots, if these impact upon service hours, together with details of how any other potential outages must be negotiated and agreed - by whom and notice periods etc.

Service Availability

The target Availability levels that the IT Provider will seek to deliver within the agreed service hours (normally expressed as a percentage - e.g. 99.5%).

Agreed details of how this will be measured and reported, and over what agreed period.

Service Level Objectives

Details of the expected responsiveness of the SOA Monitor (e.g. target workstation response times, details of expected service throughput on which targets are based, and any thresholds that would invalidate the targets).

Maximum transactions per hour
Average response time

Reliability

The maximum number of service breaks that can be tolerated within an agreed period (may be defined as number of breaks e.g. 4 per annum, or as a mean-time-between-failure (**MTBF**)).

Definition of what constitutes a 'break' and how these will be monitored and recorded.

SOA Support

Details of how to contact the Enterprise Service Section, the hours it will be available, and what to do outside these hours to obtain assistance (e.g. on-call support, third-party assistance etc).

Targets for Incident response times (how long will it be before someone starts to assist the Customer - may include travelling time etc). Definition is needed of 'response' - a telephone call back to the Customer? Or a site visit? - as appropriate.

Targets for Mean Time to Repair (MTR).

Required communications timeframe when an outage occurs.

Escalation process

Method of communication channels.

- Ensure system status page is updated

Brief description of the current incident management process.

Note. Both Incident response and resolution times will be based upon whatever Incident impact/priority codes are used - details of which must be included here.

Change Management Procedures

Brief mention of and/or reference out to the organisation's **Change** Management procedures that must be followed - just to re-enforce compliance. (Link to current Change management process)

Details of any known Changes that will impact upon the agreement, if any.

Versioning

Link to versioning standards

Security

Brief mention of and/or reference out to the organisation's Security Policy (covering issues such as password controls, security violations, unauthorised software, viruses etc). Details of any specific responsibilities on both sides (e.g. Virus Protection, Firewalls).

Service Reviews

Details of how and when the service targets will be reviewed. Details of reporting that will take place and of formal review meetings etc. Who will be involved and in what capacity.

Link to continual cycle of improvement & Governor Team

Glossary

Explanation of any unavoidable abbreviations or terminology used, to assist Customer understanding. (Link to SOA glossary)

Approval of the OA

Signatures:

Name..... Title..... Date .....

Name..... Title..... Date.....

Appendix A

Service Consumer
Application Area
Application Technical Owner
Application Business Owner
Application Representative

Application Help Desk (i.e TI, Service Desk)

Please describe the communication method

NOTE: special instructions specific to Service Consumer

Appendix B

Problem Management
Link to known errors
Problem management process
Communication method for problems
Reporting frequencies