INTERNATIONAL STANDARD

ISO/IEC 17998

First edition
2012-09-01

Information technology — SOA Governance Framework

Technologies de l'information — Cadre de gouvernance SOA

Reference number
ISO/IEC 17998:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 17998 was prepared by The Open Group and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Technical Standard

SOA Governance Framework

Technical Standard

SOA Governance Framework

ISBN: 1-931624-82-8

Document Number: C093

Published by The Open Group, August 2009.

Comments relating to the material contained in this document may be submitted to:

The Open Group, Thames Tower, 37-45 Station Road, Reading, Berkshire, RG1 1LX, United Kingdom

or by electronic mail to: ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service, including UNIX® certification.

Further information on The Open Group is available at www.opengroup.org.

The Open Group has over 15 years' experience in developing and operating certification programs and has extensive experience developing and facilitating industry adoption of test suites used to validate conformance to an open standard or specification.

More information is available at www.opengroup.org/certification.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards and Guides, but which also includes white papers, technical studies, branding and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

As with all *live* documents, Technical Standards and Specifications require revision to align with new developments and associated international standards. To distinguish between revised specifications which are fully backwards-compatible and those which are not:

- A new *Version* indicates there is no change to the definitive information contained in the previous publication of that title, but additions/extensions are included. As such, it *replaces* the previous publication.
- A new *Issue* indicates there is substantive change to the definitive information contained in the previous publication of that title, and there may also be additions/extensions. As such, both previous and new documents are maintained as current publications.

Readers should note that updates – in the form of Corrigenda – may apply to any publication. This information is published at www.opengroup.org/corrigenda.

This Document

This document is the Technical Standard for the SOA Governance Framework. It has been developed by the SOA Governance project of The Open Group SOA Working Group.

Trademarks

Boundaryless Information Flow™ and TOGAF™ are trademarks and Making Standards Work®, The Open Group®, UNIX®, and the "X" device are registered trademarks of The Open Group in the United States and other countries.

The Open Group acknowledges that there may be other brand, company, and product names used in this document that may be covered by trademark protection and advises the reader to verify them independently.

Acknowledgements

The Open Group gratefully acknowledges all contributors to the SOA Governance project, and in particular the following individuals:

- Ali Arsanjani, IBM
- Stephen G. Bennett, Oracle (Former Co-Chair)
- William A. Brown, IBM
- Tony Carrato, IBM (Former Co-Chair)
- Carleen Christner, HP
- Jorge Diaz, IBM (Co-Chair)
- Steve Dupont, The Boeing Company
- Mats Gejnevall, Capgemini (Co-Chair)
- Chris Harding, The Open Group (Forum Director)
- Andrew Hately, IBM (Former Co-Chair)
- Heather Kreger, IBM
- Nikhil Kumar, ApTSi
- Bob Laird, IBM
- Milena Litoiu, CGI
- Ranu Pandit, Deloitte
- Vishal Prabhu, Deloitte
- Madhu Reddiboina, Deloitte
- Chuck Reynolds, Deloitte
- Mohan Venkataraman, Deloitte
- Bobbi Young, Unisys

Referenced Documents

The following documents are referenced in this Technical Standard:

- Introduction to SOA Governance and Service Lifecycle Management, Bill Brown, IBM, March 2009; refer to: ftp://ftp.software.ibm.com/software/soa/pdf/IBMSGMMOverview.pdf
- Introduction to SOA Governance: The official IBM definition and why you need it, Bobby Woolf, IBM developerWorks, July 2007; refer to: www.ibm.com/developerworks/webservices/library/ar-servgov
- Navigating the SOA Open Standards Landscape Around Architecture", Joint White Paper from OASIS, OMG, and The Open Group, July 2009 (W096); refer to: www.opengroup.org/bookstore/catalog/w096.htm
- OASIS Reference Model for SOA (SOA RM), Version 1.0, OASIS Standard, 12 October 2006; refer to: docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf
- OECD Corporate Governance Principles 2004, Organization for Economic Cooperation and Development; available from: www.oecd.org
- SOA Source Book, C. Harding (editor), The Open Group, 2009; refer to: www.opengroup.org/bookstore/catalog/g093.htm
- The Open Group Architecture Framework (TOGAF); refer to: www.opengroup.org/architecture/togaf9
- The Open Group SOA Integration Maturity Model (OSIMM), Technical Standard, August 2009 (C092); refer to: www.opengroup.org/bookstore/catalog/c092.htm

See also Appendix D:

1 Introduction

1.1 Objective

This document describes a framework that provides context and definitions to enable organizations to understand and deploy SOA governance.

This document defines:

- SOA Governance, including its relationship between Business, IT, and EA governance; this assists organizations in understanding the impact that the introduction of SOA into an organization has on governance
- An SOA Governance Reference Model (SGRM) and its constituent parts, which assists organizations in specifying their appropriate governance regimes; and capturing best practice as a basis for a common approach
- The SOA Governance Vitality Method (SGVM) which assists organizations in customizing the SGRM and realizing their SOA Governance Regimen

This document is not intended to be used as provided; it is intended to be customized to create appropriate SOA governance for the organization. Many of the lists are non-normative and exemplary and intended to be filtered and as input to the customization process.

This document does not include an explanation of the fundamentals and value of SOA which is important for being able to understand and apply SOA governance. Many other specifications and books are available on SOA basics (see Referenced Documents and Appendix D).

1.2 Overview

Many companies have adopted Service-Oriented Architecture (SOA) as an approach to architecture to assist in closing the business and IT gap by delivering the appropriate business functionality in a timely and efficient manner. For more details on this, refer to available books and standards on SOA (see Referenced Documents and Appendix D).

Many companies that have approached SOA via a pilot project have not been seeing the same demonstrated SOA benefits once they have deployed a fully-fledged SOA project. While pilot projects achieved a level of re-use, they have tended to be within one division, but as soon as a project boundary crosses multiple divisions, new challenges are encountered.

One of the key disciplines to assist in addressing these challenges is governance. Whilst governance has been around a long time, SOA has heightened the need and importance of having a formal SOA Governance Regimen that sets expectations and eases the transition of an organization to SOA by providing a means to reduce risk, maintain business alignment, and

show business value of SOA investments through a combination of people, process, and technology. The role of the SOA Governance Regimen is to create a consistent approach across processes, standards, policies, and guidelines while putting compliance mechanisms in place.

Most organizations already have a governance regimen for their IT department covering project funding, development, and maintenance activities. These tend to have been defined using either one of the formal standard IT governance frameworks – such as COBIT, ITIL, etc. – or an informal in-house governance framework that has been built over many years. The focus of The Open Group's initial release of an SOA Governance Framework is primarily based on the IT aspects of SOA governance.

This document contains a description of the governance activities that are impacted by SOA, and puts forward some best practice governance rules and procedures for those activities. In order to specify the changes necessary to accommodate SOA in an existing governance regime, the governance activities described in this document must be mapped and integrated to the activities being utilized in the existing regime. Many of the lists provided with the explanations of the SGRM and SGVM are non-normative examples intended to provide a starting point for customization to the SOA solution.

This document is organized as follows:

- This chapter provides a general introduction.
- Chapter 2 discusses the background to SOA governance, describing the reasons why governance is important for SOA, the challenges involved, and the benefits that should be achieved.
- Chapter 3 defines SOA governance and explains The Open Group SOA Governance Framework.
- Chapter 4 defines the generic SOA Governance Reference Model (SGRM) used as a baseline for tailoring an SOA Governance Model for an organization.
- Chapter 5 defines the SOA Governance Vitality Method (SGVM) which describes a method using the generic SGRM to instantiate an organizational unique SOA Governance Model.
- Appendix A describes the SOA governance process activities.
- Appendix B describes the SOA governance process information entities.
- Appendix C provides an SOA governance metrics example.
- Appendix D describes the relationship of this document to other SOA standards.

1.3 Conformance

The SOA Governance Framework does not have strict compliance statements or testing. It is expected that this Technical Standard will be customized appropriately into a governance regimen for the industry or organization applying it.

For those SOA Governance Regimens to be conformant with this Technical Standard, they must have at least the following processes defined:

- Compliance process
- Dispensation process
- Communication process

The SGVM must also be defined for the organization.

The nature and extensiveness of the guidelines and the governed processes depends upon the SOA maturity of the organization; therefore, SOA governance conformance does not assert any requirements on them.

1.4 Terminology

Can — Describes a permissible optional feature or behavior available to the user or application. The feature or behavior is mandatory for an implementation that conforms to this document. An application can rely on the existence of the feature or behavior.

Implementation-dependent — (Same meaning as "implementation-defined".) Describes a value or behavior that is not defined by this document but is selected by an implementer. The value or behavior may vary among implementations that conform to this document. An application should not rely on the existence of the value or behavior. An application that relies on such a value or behavior cannot be assured to be portable across conforming implementations. The implementer shall document such a value or behavior so that it can be used correctly by an application.

Legacy — Describes a feature or behavior that is being retained for compatibility with older applications, but which has limitations which make it inappropriate for developing portable applications. New applications should use alternative means of obtaining equivalent functionality.

May — Describes a feature or behavior that is optional for an implementation that conforms to this document. An application should not rely on the existence of the feature or behavior. An application that relies on such a feature or behavior cannot be assured to be portable across conforming implementations. To avoid ambiguity, the opposite of "may" is expressed as "need not", instead of "may not".

Must — Describes a feature or behavior that is mandatory for an application or user. An implementation that conforms to this document shall support this feature or behavior.

Shall — Describes a feature or behavior that is mandatory for an implementation that conforms to this document. An application can rely on the existence of the feature or behavior.

Should — For an implementation that conforms to this document, describes a feature or behavior that is recommended but not mandatory. An application should not rely on the existence of the feature or behavior. An application that relies on such a feature or behavior cannot be assured to be portable across conforming implementations. For an application, describes a feature or behavior that is recommended programming practice for optimum portability.

Undefined — Describes the nature of a value or behavior not defined by this document that results from use of an invalid program construct or invalid data input. The value or behavior may vary among implementations that conform to this document. An application should not rely on the existence or validity of the value or behavior. An application that relies on any particular value or behavior cannot be assured to be portable across conforming implementations.

Unspecified — Describes the nature of a value or behavior not specified by this document that results from use of a valid program construct or valid data input. The value or behavior may vary among implementations that conform to this document. An application should not rely on the existence or validity of the value or behavior. An application that relies on any particular value or behavior cannot be assured to be portable across conforming implementations.

Will — Same meaning as “shall”; “shall” is the preferred term.

1.5 Future Directions

The current version of this Technical Standard defines a core SOA Governance Framework. Future versions could evolve the material and expand on a variety of relevant topics. The following are some possible areas:

- Meta-model: The current document expands on a variety of topics. It would be beneficial to have a meta-model that explicitly represents the various framework elements. This would help avoid possible ambiguities, and enable possible tool automation.
- Compliance: Most of the current conformance text (Section 1.3) is not normative. Future versions could provide more specific guidance regarding what constitutes adherence to this specification.
- Maturity Model: The method and model shown in this document provide key conceptual tools for defining an SOA governance effort. Complementary to them is an SOA Governance Maturity Model, which can be used within the Plan phase, helping to define more robust roadmaps. This maturity model would be synchronized with the OSIMM effort.
- Policy: The topic of policy is important to governance. Further versions expect to expand on its relationship with the rest of the model concepts.
- Control Gates: The topic of control gates is important to governance. Further versions expect to expand on its relationship with the rest of the model concepts.

- Business Governance: Business governance refers to the set of processes, customs, policies, laws, and institutions affecting the way in which an organization is directed, administered, or controlled. The primary focus of this SOA Governance Framework version is on the IT aspects of SOA governance, with a small number of key business governance items. However, additional business governance aspects will enhance the completeness of an overall SOA governance program.
- Governance Model Maps: More detail positioning to other relevant governance models; e.g. COBIT, ITIL, etc., could be added.
- Other Topics: For example, description of SOA governance for particular contexts; e.g., external ecosystems, and positioning of SOA governance with TOGAF governance, as well as working with OASIS and OMG to ensure alignment around SOA governance. Further information on this alignment work and its current status is in Appendix D.
- Examples: Future versions will have given time for examples of specification to be defined. These examples could be added to the effort to provide further clarity.

2 Background

2.1 SOA Challenges and Goals

While this Technical Standard focuses on the governance considerations of SOA solutions, it is important to set the stage with an understanding of SOA. Other specifications and books are available to provide grounding in SOA fundamentals and value, including The Open Group SOA Source Book, SOA Reference Architecture, SOA Ontology, and the OASIS Reference Model for SOA (see Appendix D). Deploying SOA does not come without its own challenges and over the last couple of years the following challenges have become commonplace:

- Service identification
- Demonstrating the value of SOA solutions
- SOA solution portfolio management
- Ensuring services satisfy business requirements
- Service funding
- Service management
- Service ownership
- Integrating web-delivered services
- Lack of service interoperability
- Appropriate re-use
- Uncontrolled proliferation of services
- Multiple silo'ed SOAs
- Cross-organization coordination
- Change management of services and solutions

But SOA also heightens the importance of addressing existing challenges that IT has been encountering for years, such as funding models, functional ownership, and standards compliance. Therefore, organizations should ensure that:

1. The correct services and solutions are built that meet the needs of the business.
2. There is a consistent approach to discovery, consumption, identification, design, development, implementation, and management of services and solutions.
3. The appropriate organization and Line of Business (LOB) decisions are made.

4. The SOA approach is being properly communicated throughout the organization.
5. Proper training on SOA is taking place in the organization.
6. The SOA Reference Architecture stays relevant.
7. Services are funded and have documented ownership.
8. Only approved services are deployed.
9. Services created adhere to governance policies.
10. Services are designed, built, and run in a secure manner.
11. Changes to services are managed.
12. Services are managed in a scalable way.
13. Service developers can easily publish and discover services.
14. Existing Service Level Agreements (SLAs) are validated when new consumers are added.
15. SOA governance controls and exception policies exist and are effective.
16. The appropriate and pragmatic SOA governance roles, responsibilities, and authority are understood and being executed in an acceptable manner.
17. There is vitality in the governance process; that SOA governance is maturing as the SOA capabilities of the organization mature.

2.2 SOA Governance

To address these challenges, organizations require a comprehensive and appropriately detailed SOA Governance Model that can be deployed in an iterative and incremental manner. A comprehensive SOA Governance Model should cover all of the three main aspects, including:

- Processes – including governing and governed processes
- Organizational structures – including roles and responsibilities
- Enabling technologies – including tools and infrastructure

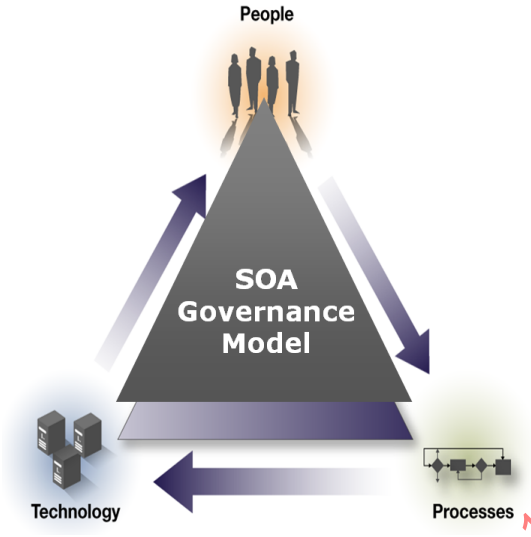

Figure 1: SOA Governance Aspects

This document defines an SOA Governance Framework containing an SOA Governance Reference Model (SGRM) and the SOA Governance Vitality Method (SGVM) that allows an organization to define a customized and focused SOA Governance Regimen.

3 SOA Governance

3.1 SOA Governance Definition

In general, governance means establishing and enforcing how people and solutions work together to achieve organizational objectives. This focus on putting controls in place distinguishes governance from day-to-day management activities [Source: Introduction to SOA Governance: The official IBM definition and why you need it].

As a discipline, governance has been with us for many years, but with the advent of enterprise SOA, the need has been heightened for organizations to take governance as a discipline more seriously. So, why is defining SOA governance and its scope so challenging?

With so many definitions of SOA coming from software vendors, standards bodies, analyst firms, and respected authors, it's no wonder that defining SOA governance and its scope causes so much confusion and disagreement.

SOA governance should be viewed as the application of Business governance, IT governance, and EA governance to Service-Oriented Architecture (SOA). In effect, SOA governance extends IT and EA governance, ensuring that the benefits that SOA extols are met. This requires governing not only the execution aspects of SOA, but also the strategic planning activities.

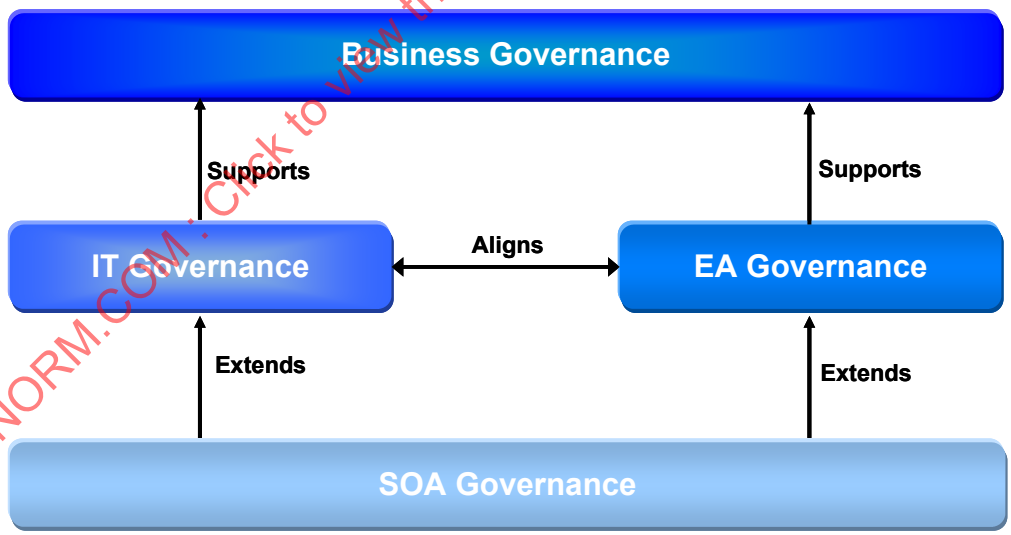

Figure 2: SOA Governance Relationships

- **Enterprise Architecture (EA) Governance** is the practice and orientation by which enterprise architectures and other architectures are managed and controlled at an enterprise-wide level. [Source: TOGAF 8.1.1]

- **IT Governance** includes the decision rights, accountability framework, and processes to encourage desirable behavior in the use of IT. [Source: Based on COBIT4.0]
- **Business Governance** is the set of processes, customs, policies, laws, and institutions affecting the way an organization is directed, administered, or controlled. [Source: Wikipedia, based on OECD Principles of Corporate Governance]

3.2 SOA Governance Scope

Many of the early definitions of SOA were very technology-focused and the differences between SOA and web services technology were blurred. A side-effect of this is the misperception that SOA governance can be solved by technology alone. Effective SOA governance requires equal focus on the people, process, and technology aspects of SOA governance; therefore, defining and scoping SOA governance can be a challenge.

As previously stated, SOA governance should extend the organization's existing IT and EA governance models to cater for the new SOA assets and SOA policies. Extending these existing governance models reduces the risk that organizations will create uncoordinated silo'ed governance regimens that will potentially duplicate existing coverage areas of their core governance regimens. Extending the existing governance regimen to ensure that the benefits of SOA are achieved is still challenging. It requires governing the strategic planning activities as well as the execution aspects of SOA.

3.3 SOA Governance Framework

The goal of the SOA Governance Framework is to enable organizations to define and deploy their own focused and customized SOA Governance Model.

Since aspects of the SOA Governance Model require culture change, an SOA Governance Regimen should never be deployed in a big-bang approach. The framework defines an incremental deployment approach so that organizations can continue to meet their current demands while moving towards their long-term goals for SOA.

There is no single model of good SOA governance due to variants within an organization. Examples of these variants include the existing governance in place, the SOA maturity level, size of the organization, etc. In effect, an organization's appropriate SOA Governance Model is one that defines:

- What decisions need to be made in their organization to have effective SOA governance
- Who should make these SOA governance decisions in their organization
- How these SOA governance decisions will be made and monitored in your organization
- What organization structures, processes, and tools should be deployed in your organization
- What metrics are required to ensure that an organization's SOA implementation meets their strategic goals

Organizations should frankly assess their current governance regimen and practical governance goals. From this, an achievable roadmap for delivering governance can be created.

The SOA Governance Framework consists of an SOA Governance Reference Model (SGRM) which is utilized as a starting point, and an SOA Governance Vitality Method (SGVM) which is a definition/improvement feedback process to define a focused and customized SOA Governance Regimen.

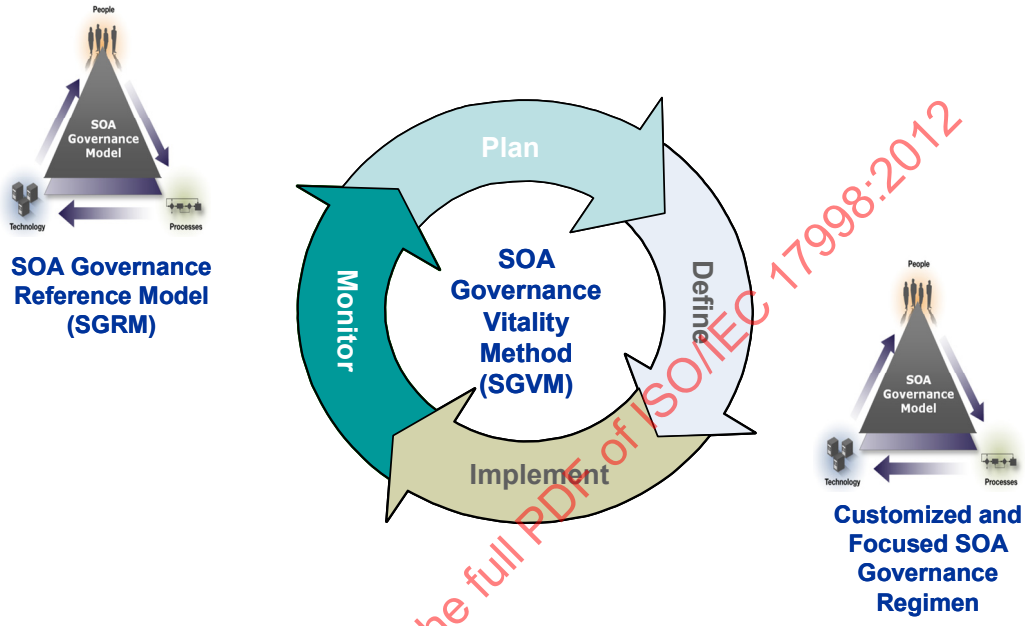

Figure 3: SOA Governance Framework

3.3.1 SOA Governance Reference Model (SGRM)

The SOA Governance Reference Model (SGRM) is a generic model that establishes a foundation of understanding and is utilized to expedite the process of tailoring the SOA Governance Regimen for an organization. All aspects of the SGRM should be reviewed and considered for customization to the organization's environment. The examples provided are intended to be a starting point for discussion which may be selected from or extended.

3.3.2 SOA Governance Vitality Method (SGVM)

The SOA Governance Vitality Method (SGVM) is a process that starts with the SGRM and then follows a number of phased activities to customize it for the organization's variants. SOA governance should be viewed as a process and not a project; therefore, the phases of the SGVM should be viewed as a continuous improvement loop, whereby progress is measured, and course-correction and updates to the SOA Governance Regimen are performed when needed.

4 SOA Governance Reference Model (SGRM)

The SOA Governance Reference Model (SGRM) is a generic model that is utilized as a baseline SOA Governance Model to expedite the process of tailoring an SOA Governance Model for an organization. All aspects of the SGRM are reviewed and considered for customization to the organization's environment.

The SGRM defines a number of constituent parts, including:

- SOA governance guiding principles
- SOA governing processes
- Governed SOA processes
- SOA governance process artifacts
- SOA governance roles and responsibilities
- SOA governance technology

4.1 SOA Governance Guiding Principles

SOA Governance Guiding Principles assist in the prioritization and decision-making for the design, deployment, and execution of the SOA Governance Regimen. This includes aspects of people/roles, processes, and technology. In addition, the SOA Governance Guiding Principles should be utilized to aid an organization to achieve stakeholder commitment to the SOA Governance Regimen.

Below are the SOA Governance Guiding Principles of the SGRM. The organization's SOA and governance maturity will affect how these principles are selected and how strictly they are applied. It is expected that a subset of these principles will be selected and modified. It is also expected that the principles will be expanded upon with principles unique to the organization.

Principle	Description	Rationale
SOA governance must promote the alignment of business and IT	The SOA governance program should support the business and IT drivers. Business and IT stakeholders must participate in governing and enforcing the organization's SOA program.	SOA is intended to drive flexibility and agility for the business and IT. Failing to govern to foster that alignment will reduce the benefits of a service-oriented approach.
Conform to organization's governance	SOA governance activities shall conform to Business, IT, & EA governance principles and standards.	The organization governance procedures are part of the strategy of the organization and should be a part of SOA governance as well.

Principle	Description	Rationale
An SOA Reference Architecture is required	An SOA Reference Architecture provides a set of architectural patterns, standards, and best practices for use in developing SOA solutions.	Use of the approved architectural artifacts, from the SOA RA, will reduce project risk and lower costs, by reducing the number and complexity of design activities in the project. Organization reference architectures may be based on standard SOA reference architectures or industry reference architectures. All SOA solution architectures should be created based on the organization's SOA Reference Architecture.
Provider & consumer contracts	Contracts should exist between service providers and consumers. Contracts may be dictated by one party.	To ensure the correct delivery of service.
Service metadata	To enable decisions and descriptions relating to services and their contracts to be stored in a well-known location, including relationships among services and their associated artifacts.	Understanding of the purpose of the service. Business continuity impact analysis. Root cause analysis.
Identified governance stakeholders	Stakeholders shall be identified and accept responsibility for the governance process(es).	To ensure proper execution of governance. To communicate SOA governance value. To communicate appropriate SOA governance processes and procedures.
Tailor SOA governance processes	SOA governance processes should be tailored based on objectives, project scope, and risk.	Only do as much governance as is needed. To prioritize SOA governance costs.
Automate SOA governance processes	It should be possible to automate the SOA governance processes.	Facilitates consistent and efficient application. Reduces personnel required to do the work. Reduces training of people. More reliable and traceable governance.

Principle	Description	Rationale
Implement funding model	All services and solutions should be covered by a funding model.	Ensure that an organization is willing to develop and support a needed service long-term, especially if services may be used across organization funding models. Services developed on an *ad hoc* basis may not be officially supported for defects, conformance, enhancement, and performance.

There is also a set of important SOA principles that should be governed:

Principle	Description	Rationale
Service re-use	Existing services should always be considered first when creating new SOA solutions.	Re-use before buy before build to decease cost and complexity.
Service description	Descriptions shall be adequate to support consumer decision to use the service.	Ensure consumers have adequate information to decide whether the service is appropriate for their objectives. This may include: • Service metadata • Policy • Contracts • Funding model (current and projected) Helps support consumers re-using existing services.
Service harvesting	Solutions should be reviewed for harvesting re-usable services.	Existing solutions are the best source for re-usable services with the least development and maintenance costs. New solutions should consider harvesting services during initial development and on an ongoing basis.
Service monitoring	Service contracts adherence should be monitored. Metrics should be gathered and available.	To ensure correct service delivery. To detect service contract violations. To feed service and SOA solution governance. To support consumers choosing a service with appropriate metrics.
Service policy enforcement	Service design and run-time policies should be enforced.	To ensure high-quality services. To ensure conditions are met that have been expressed to achieve stated goals.

Principle	Description	Rationale
Service security	Services contracts and descriptions should be reviewed for conformance to organization security requirements with identified security best practices and support of objectives.	To ensure correct security levels and risk levels.
Comply with EA	The SOA services and solutions should comply with the enterprise architecture (if one exists).	To ensure that the SOA solution and service fulfills the long-term goals of the organization.

Organizations may need to create their own SOA and SOA governance principles that target their needs.

4.2 SOA Governing Processes

Governing Processes realize the governance intentions of the organization. These are the processes that a governance model uses to govern any particular process. Governed processes are the actual processes being controlled, monitored, and measured (e.g., testing, design, deployment); they are further expanded in Section 4.3.

The SGRM defines three governing processes: Compliance, Dispensation, and Communication, which are performed on an ongoing basis. It is expected that organizations will define Compliance processes, but they should be customized and extended as appropriate for the SOA solution.

4.2.1 Compliance

The purpose of this activity is to define a method to ensure that the SOA policies, guidelines, and standards are adhered to. The Compliance process provides the mechanism for review and approval or rejection against the criteria established in the governance framework (i.e., principles, standards, roles, and responsibilities, etc.). In many cases, it is an add-on to the existing quality review process.

A suggested method is to insert SOA Governance Checkpoints into the defined SOA processes defined below (Service & Solution Portfolio and Lifecycle). These checkpoints can be manual reviews by responsible parties or automated, programmatic checkpoints. A set of possible checkpoints can be found in Appendix A.

The Compliance process is an ongoing process. When a checkpoint review is not approved or passed, then an exception to the Compliance process has occurred. The cause of the exception should be adjusted or realigned in order to meet the compliance requirements. If it cannot or should not be brought into alignment with policy, then the risk should be evaluated. To facilitate this evaluation, risk analysis criteria should be defined to determine the impact of the non-compliance to the organization, such as increased cost, deferred strategies, and implementation delays. If the organization chooses to accept the risks, then the Dispensation process is initiated.

4.2.2 Dispensation

The Dispensation process is the exception and appeals process that allows a project or application team to appeal non-compliance to established processes, standards, policies, and guidelines as defined within the governance regimen. Examples include service funding, service ownership, service identification, etc. The result would be a granted exception.

The following results may happen from a failed checkpoint assessment:

- Dispensation: Provides an alternative route to conformance by granting permission to remain non-conformant. These are granted for a given time period and set of identified service and operational criteria that must be enforced during the lifespan of the dispensation. Dispensations are not granted indefinitely, but are used as a mechanism to ensure that service levels and operational levels are met while providing a level of flexibility in their implementation and timing. The time-bound nature of dispensation ensures that they are a major trigger in the Compliance process.
- Comply: If dispensation is not granted, then the source of the failing checkpoint assessment must be brought back into compliance. The other option is to re-evaluate the risk using the risk analysis criteria, as additional facts may have been identified during the Dispensation process. Even if the dispensation is not granted, in some cases, an organization may still choose to assume the risk. While this is not the ideal scenario, it may occur, so the governing processes should address it during the process definition.
- Appeal: If the activity has caused an exception in a checkpoint and cannot or should not be adjusted to pass compliance, the activity exception can begin the appeals process to ask governance authority for a re-evaluation of the dispensation decision. Additional information to influence the decision should be brought forward.
- Escalation: Should the appeal not bring about a satisfactory result, an Escalation process can begin with the next level of governance authorities.
- Trigger for Vitality: Excessive exceptions and dispensations should trigger re-evaluation of the governance framework and possibly an iteration of the SGVM. Numbers of exceptions, appeals, and dispensations should be tracked as a Key Performance Indicator (KPI) for SOA governance vitality. Excessive dispensations may be caused by an error in the policies or guidelines as well as by a new business condition which impacts the current SOA solution or SOA Governance Regimen.

4.2.3 Communication

Communication processes educate, communicate, and support the SOA Governance Regimen and SOA policies, guidelines, and standards across the organization. This also includes ensuring that the governing processes are acknowledged within the governed processes. Communication processes should ensure that the governance is understood. It should also ensure access to and use of governance information.

Essential information to be communicated and available may include:

- Value of SOA and SOA governance

- Policies, standards, and guidelines
- Compliance processes
- Dispensation process including escalations and appeals
- Organization, role, and responsibilities
- Technology being governed and used by the governing processes
- Governed processes and checkpoints

Parties to be communicated with may include:

- Parties who are stakeholders; i.e., Business/IT Steering Group and Business Domain Representatives
- Parties responsible for SOA governed processes to ensure they understand and deploy the governance checkpoints appropriately; this includes the SOA Solution Architect, SOA Center of Excellence, Solution Development Team, Service Development Team, and IT Operations Team
- Parties responsible for enforcing SOA governing processes to ensure they understand the Compliance process and the Dispensation process; this includes the SOA Governance Board
- Parties responsible for the Compliance processes, including the SOA Governance Board and the Solution and Service Development Teams
- Parties responsible for the Dispensation processes, including the SOA Governance Board
- Parties responsible for defining and executing the SGVM to ensure it is re-evaluated appropriately; this includes the SOA Governance Board and the SOA Center of Excellence

Communication and information should be easily accessible via the use of technologies such as repositories and the Internet. A technology framework should be available for storing and accessing governance artifacts, such as the governance processes, stakeholders and responsible parties for those processes, current policies, guidelines, standards, and dispensation.

Communication is an ongoing process since changes in the policies and governance framework will need to be communicated. These changes come from either natural changes in business policy or iterations of the SGVM to keep the SOA governance current with business strategies.

Using service testing as an example of adding governance to an SOA governed process in an enterprise illustrates these processes. When an organization is doing service testing, it must ensure that application teams comply with the correct way to test services by defining checkpoints within the service testing process. These checkpoints have to be enforced in the Compliance process. The application teams are provided with means to challenge the test process through the Exception and Appeals process as part of the Dispensation process. Finally, application or project teams cannot be expected to follow the agreed process to properly test services unless this process was properly disseminated across the organization, which incorporates the Communication process. Of course it is also possible to do a much lighter

governance in a smaller organization where compliance checkpoints might only occur in testing exception processes.

4.3 Governed SOA Processes

SOA governance begins with alignment to Business, IT, and EA governance. This starts with alignment of organizational governance and concludes with continuous enforcement and compliance during operation. The governed SOA processes include planning, design, and operational aspects of SOA as described in Figure 4.

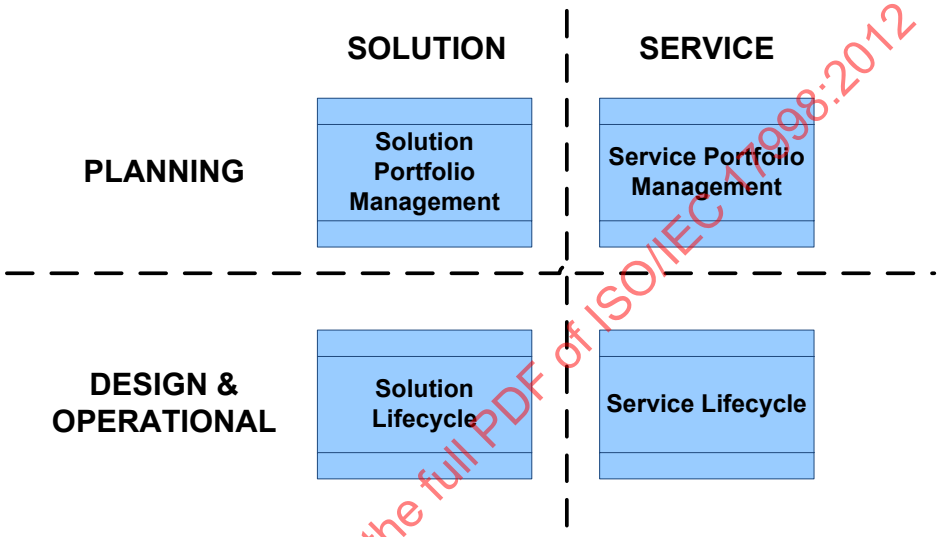

Figure 4: Governed SOA Processes

Instantiations of SOA should result in a set of SOA processes to provide ongoing management of the SOA solution. As shown in Figure 5, at the project level, the Solution Portfolio Management process focuses on planning and prioritization of individual SOA solutions. These individual solutions may consume existing services as well as define new services. Following the guidance of the Service Portfolio Management process, these solutions may consume the re-usable services developed by the Service Lifecycle process and/or define new services for Service Portfolio Management. The new services are thereby prioritized by Service Portfolio Management for the Service Lifecycle process to manage for consumption by the individual SOA solutions. The Solution Lifecycle then enforces the Solution Portfolio Management plans during the development, deployment, and management of the individual SOA solution. This Technical Standard does not provide detail on these SOA processes (those can be found in other SOA Reference Architecture standards), but focuses on governance of those processes.

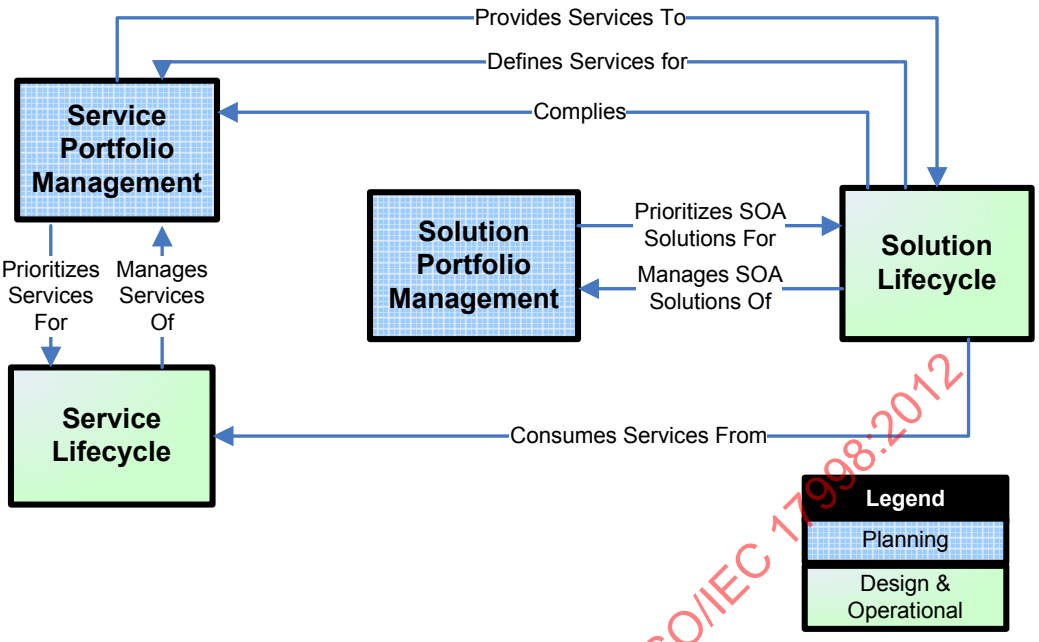

Figure 5: Governed SOA Process Relationships

SOA governance applies to the full lifecycle of SOA. To align with the SOA Guiding Principles within the SGRM, a number of additional process activities and governance checkpoints need to be defined and deployed in existing and new SOA processes to enable the governing Compliance process.

The SOA Governance Compliance process ensures continuous alignment and guidance of governance goals and policies, business goals, and the SOA solutions and services. The governance processes influence the goals and constraints of Service and Solution Portfolio Management which in turn focus on planning how to implement SOA governance at the applicable organizational level.

The next section details how to apply the SGRM to the SOA processes just discussed. Process activities, issues, and governance checkpoints have been provided as examples of SOA process activities and issues which are particularly important to govern. The important issues will certainly vary for organizations and SOA solutions. The governance checkpoints are examples of governance which could be applied to these processes. These are a starting point for customization for an SOA Governance Regimen for an SOA solution. A subset of these processes, process activities, and governance checkpoints could be selected; it is expected that additional ones unique to the organization will be defined.

4.3.1 Service Portfolio Management

Service Portfolio Management is the SOA process of ensuring that the organization has a set of services appropriate to its needs. Service Portfolio Management is normally a new set of activities not previously performed within the organization. It has some of the properties of Solution Portfolio Management, but many activities are brand new.

SOA Service Portfolio Management processes provide the most value when performed at an enterprise level. By establishing service planning strategies in accordance with Business, IT, and EA governance principles and goals, Service Portfolio Management has the responsibility to plan for, assign implementation to specific projects, and deploy the services at the right time. An important element of the Plan process is identification of services via decomposition of business processes. Projects should also be identified for implementing one or more of the planned services. The key is the correct services at the right time with the appropriate functional and non-functional requirements (e.g., capacity) in accordance with the long-term Business, IT, and EA strategies. It must also define proper service ownership, funding models, and usage plans based upon re-use plans and fiscal responsibility as well as SOA maturity progression strategies.

Key issues that arise for SOA:

- Planning for the appropriate identified services to create business agility and maximize re-use
- Funding models that support business agility and re-use across the organization
- Resolving service ownership issues across the organization

Service Portfolio Management governance helps ensure that these goals are achieved by:

- Inserting checkpoints into the services planning process, project planning process, service development lifecycle process, service ownership process, and service funding process at levels appropriate to the governance maturity of the organization
- Defining and monitoring metrics to trigger adjustment to the Service Portfolio Management process
- Service planning for decomposing services

Table 1 shows an illustrative set of activities for Service Portfolio Management. Further details including governance opportunities can be found in Section A.2.

Table 1: Service Portfolio Management Activities

Service Portfolio Management Activities		
Service Portfolio Planning	Service Ownership	Service Change Management
Service Identification and Business Justification	Service Funding	

4.3.2 Service Lifecycle Management

SOA Service Lifecycle Management is the extension of the organization's Software Development Lifecycle (SDLC) by adding or putting emphasis on activities necessary for Service Lifecycle. Service Lifecycle processes cover the design, development, deployment, management, and ultimate retirement of services.

Key issues that arise for SOA:

- Adapting organization current software development lifecycle to service development lifecycle

- Establishing and approving service contracts (e.g., business processes will have the necessary capacity)
- Publishing services to enable re-use
- Managing multiple versions of a service
- Detecting unexpected service usage
- Meeting SLAs and architecting to enable this
- Managing to policies

Service Portfolio Management governance helps ensure that the goals of Service Lifecycle are achieved by, e.g.:

- Inserting checkpoints in the Service Lifecycle at both design time and operation time at levels appropriate to the governance maturity of the organization
- Defining and monitoring metrics to trigger adjustment to the Service Lifecycle process
- Changing management governance to ensure changes are coordinated across projects
- Ensuring service registries and repositories stay current

Table 2 shows an illustrative set of sub-processes for Service Lifecycle management. Further details including governance opportunities can be found in Section A.2.

Table 2: Service Lifecycle Activities

Service Lifecycle Activities		
Service Definition	Service Implementation, Assembly, or Acquisition	Service Management and Monitoring
Service Realization Planning	Service Testing	Service Support
Service Modeling	Service Deployment	

4.3.3 Solution Portfolio Management

SOA Solution Portfolio Management is the process of ensuring that the organization has a set of SOA solutions appropriate to its needs and capability to implement and understand those solutions. Solution Portfolio Management processes identify the solution scope and develop solution plans for service re-use and new development in order to meet the solution requirements. SOA Solution Portfolio Management is the extension of IT Portfolio Management, adding or putting emphasis on a few activities necessary for managing the portfolio of SOA solutions. There is normally no need to create a new process for SOA Solution Portfolio Management since there will still be non-SOA solutions created and managed in the portfolio.

Effective enterprise transformation is assisted by the application of SOA principles to enterprise architecture in a synergistic fashion. SOA principles enable flexibility and improved time-to-market in IT supported processes and business solutions. Enterprise architecture merges strategic business and IT objectives with opportunities for change through portfolio gap analysis,

transition planning, and architectural governance. Leveraging service-oriented portfolio gap analysis, the enterprise planning cycle transforms strategy into a roadmap of specific change initiatives, and governs the execution of that resulting roadmap. The SOA lifecycle then drives solution delivery in the context of one or more specific projects in the roadmap.

In addition to common Solution Portfolio Management processes, SOA Solution Portfolio Management has particular key requirements due to the nature of SOA:

- Ensuring SOA is a valid solution pattern for addressing the business problem
- Ensuring return-on-investment analysis for SOA is performed
- Ensuring SOA solution funding is available
- Educating and training stakeholders on the SOA Solution Portfolio and its benefit to the business

Solution Portfolio Management governance helps to ensure that the goals of Service Lifecycle are achieved by:

- Inserting checkpoints to ensure the quality of the Solution Portfolio at levels appropriate to the governance maturity of the organization
- Defining and monitoring metrics to trigger adjustment to the Solution Portfolio Management process
- Ensuring training/communication is done and maintained as the needs of the organization change

Table 3 shows an illustrative set of activities for Solution Portfolio Management. Further details including governance opportunities can be found in Section A.2.

Table 3: Solution Portfolio Management Activities

Solution Portfolio Management Activities		
Solution Portfolio Planning	SOA Solution Validity	Solution Change Management
SOA Solution Funding		

4.3.4 SOA Solution Lifecycle

The SOA Solution Lifecycle supports the design, development, deployment, management, change, and ultimate retirement of SOA solutions. SOA Solution Lifecycle processes are where the majority of the solution development is governed. Key SOA-related challenges during the SOA solution development lifecycle include, but are not limited to:

- Ensuring business processes for the SOA process orchestrations include business rules, business process management, and associated technologies
- Ensuring Service Portfolio Management interfaces include service identification and service contracts used by providers and consumers
- Enabling service assembly for building composite services and applications

- Ensuring service certification during deployment includes the validation of service contracts as well as functional and non-functional requirements
- Enabling service operational management which includes Service Level Agreement (SLA) verification, service monitoring, and reporting
- Ensuring change management for SOA services which includes accurate impact analysis of deployed services
- Ensuring proper cost allocation for service development and execution

SOA Solution Lifecycle governance helps ensure that the goals of Solution Lifecycle are achieved by:

- Inserting checkpoints into Solution Lifecycle processes (design, development, deployment, management, change, retirement) at levels appropriate to the governance maturity of the organization
- Specifying all the solution elements as a coordinated program, and identifying and coordinating stakeholders and organizing authority to proceed
- Managing solution responsibilities and providing solution management capabilities including scope management, issue management, and change management
- Providing a solution review process and adjusting contributing factors to attain optimum overall solution performance
- Preparing complete, comprehensive accurate estimates of solution effort and schedule including recognizing dependencies, resources required, and expenses and identifying risks and contingency plans
- Defining and monitoring metrics to trigger adjustment to the Solution Lifecycle process

Table 4 shows an illustrative set of activities for Solution Lifecycle. Further details including governance opportunities can be found in Section A.2.

Table 4: Solution Lifecycle Activities

Solution Lifecycle Activities		
Solution Definition	Solution Modeling	Solution Management and Monitoring
Solution Realization Planning	Solution Implementation, Assembly, or Acquisition	Solution Support
Service Re-use Planning and Re-use Exceptions	Solution Testing	SOA Entitlement/Usage
Solution Deployment		

4.4 SOA Governance Roles and Responsibilities

Below are example roles and responsibilities that should be considered as part of an organization's SOA Governance Model. Which roles apply will be a function of the governance principles and SOA governance maturity. The role name is not as important as the responsibilities highlighted. Each organization has their own role naming conventions and it is more important to adopt/align the new governance responsibilities with the existing internal structures.

These roles and structures are exemplary and provided as a starting point for customization for an SOA Governance Regimen for an SOA solution. A subset of these roles and/or structures could be selected. Different organizations might decide, for simplicity, to have combined organizational structures to support the roles displayed in the table below. Additional roles unique to the organization may be defined.

Structure	Key Roles	Responsibilities
Business/IT Steering Group (Sponsorship of all IT Solutions and Services)	CIO CTO or Chief IT Strategist Chief Architect Business Domain Owners	Ultimate decision-makers for decisions regarding SOA solution, service, and business and IT-related matters Approve SOA strategic direction Approve governance principles
SOA Steering Board (Sponsorship of SOA Program and Leadership)	SOA Chief Architect SOA Program Director SOA Business Sponsor	Define future SOA strategic direction and roadmap Monitor SOA strategic direction Ensure SOA principles and practices will make an appropriate and necessary contribution to the overall enterprise business strategy Support the desired outcomes and objectives by providing funding and resources for the SOA and SOA governance Defines the SOA governance principles
EA Governance Board	Chief Enterprise Architect Enterprise Architects Chief SOA Architect	Define and develop the service portfolio Define and develop the SOA solution portfolio (segment/domain architecture)

Structure	Key Roles	Responsibilities
SOA Center of Excellence (Definition and Development)	Business Champion Chief SOA Solution Architect Organizational Change Consultant Test Strategist Roles responsible for: • SDLC • Project management processes • Operational processes management Tool strategist	Represents the business organizations in the CoE Collaborate to develop SOA Governance Roadmap, Transition Plans, and governance principles (SGVM) Definition and development of SOA governing processes and best practices Definition and development of governed SOA processes and best practices Defines where compliance checkpoints should be inserted into governed SOA processes Definition and monitoring of SOA metrics across the LOBs (SOA governance KPIs) Architectural definition and integration support across LOBs (consult) Initiate SOA and SOA governance organizational changes Develop governed SOA transformation plans Identify SOA training and mentoring plans Define and validate changes to the project management process Select and implement the SOA governance tool strategy
Business Domain Representatives (Scope and Delivery Management)	Program Manager Business Architect Process Engineer Business Subject-matter Expert	Responsible for the solution from a business perspective by justifying the solution and services existence and continuous operation to the stakeholders Determine business service functionality Communicate business requirements and identify business services for each domain Share information regarding specific business requirements and identify the cross-organizational SOA business services Work on prioritizing program requirements and services Develop service proposals to go through funding process
SOA Governance Board (Informing and Monitoring)	SOA Chief Architect Business Architects	Ensure compliance with standards and guidelines Dispensation Communication

Structure	Key Roles	Responsibilities
Solution Development Team (Execution and Delivery)	Project Manager Business Analysts Solution Architects Integration Specialist Operations Architect Developers Testers Security Architect	Manage the solutions within a specific domain Design, development, testing, deployment, execution, and delivery of the SOA solution within the domain Maintain consumer-side interfaces to services Follow standards and guidelines Understand and abide by the governing processes
Service Development Team (Execution and Delivery)	Project Manager Business Analysts Service Architects Integration Specialist Operations Architect Developers Testers Security Architects	Design, development, testing, deployment, execution, and delivery of the services Maintain interfaces to its services Follow standards and guidelines Understand and abide by the governing processes
IT Operations (Execution and Delivery)	Database Administrator Network Infrastructure Architect System Administrator Operations	Database administration services support Network infrastructure services support Systems administration support Support for central IT functions Follow standards and guidelines Understand and abide by the governing processes

Figure 6 is a diagram of how these organizations could relate to one another:

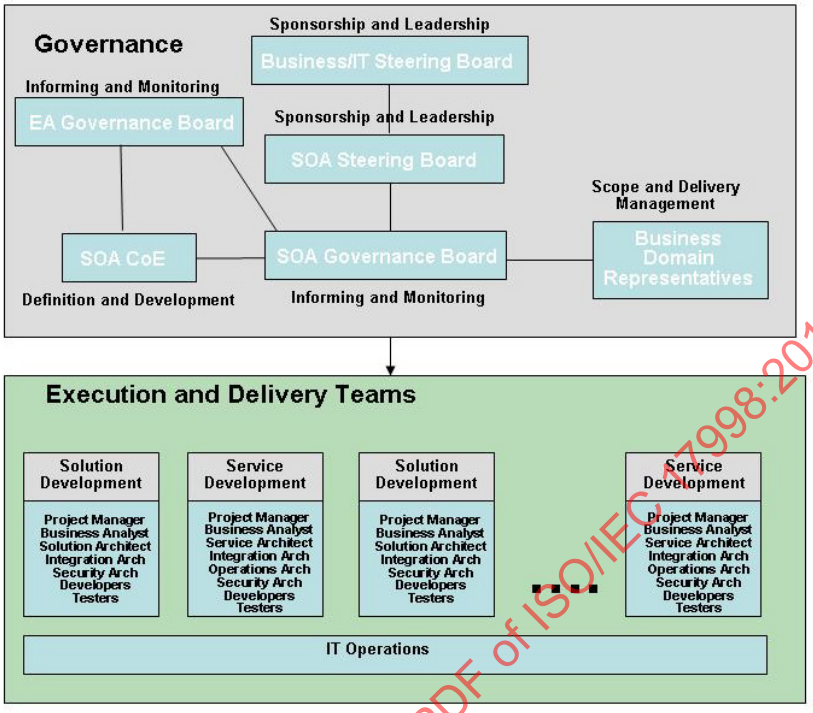

Figure 6: Example Roles and Responsibilities

4.5 SOA Governance Process Artifacts

SOA governance artifacts are new artifacts created explicitly to support SOA governance. These artifacts should be available to governance stakeholders and kept current. These artifacts are exemplary and provided as a starting point for customization for an SOA Governance Regimen for an SOA solution. A subset of these artifacts could be selected or additional ones unique to the organization may be defined.

The categories of artifacts are:

- Business-level: Business-level artifacts include those developed from a business perspective to guide the development of a governance regimen for the organization. Business-level artifacts may include documentation of SOA goals, requirements, and use-cases for the business, SOA solution, and services. More specifically for SOA governance, business-level artifacts would document the governance guidelines, governance vision, and scope.
- Organizational: Organizational artifacts would include documentation of the organization charts, roles, and responsibilities for those affected by SOA governance. RACIs are one way to document this information.

- Roadmaps: Roadmap documentation would be based upon the current and target SOA and SOA governance maturity assessments. It would also include documentation of the governance roadmap which identifies future iterations of the SGVM.
- Descriptions: Descriptions define solution and service descriptions, including interface descriptions, schemas, service-level descriptions, and documents of understanding.
- Processes: Process descriptions document governed processes and governing processes for compliance and dispensations.
- Policies: Policies document business policies, SOA solution policies, SLAs, as well as governance policies. Governance policies include policies and metrics for monitoring SOA governance and SGVM iteration triggers.
- Plans: Plans document Transition Plans for the organization, process, and technology. Plans for communication and implementation for SOA governance are also key artifacts.

Examples of artifacts used to drive the SGVM are as follows:

Artifacts	Description	Created by
Communication Plan	A plan describes how information about SOA governance is communicated.	SGVM
Guidelines	Provide prescriptive guidance to ensure compliance.	SGVM or earlier
SOA Metrics	Statistics that are regularly gathered as part of the normal SOA process to measure what is happening or not happening.	SGVM
SOA Governance Checkpoint Metrics	Statistics that are regularly gathered as part of the normal SOA Governance Checkpoints to measure what is happening or not happening.	SGVM Monitoring phase
SOA Processes Change Document	Document which identifies the changes needed in the current effort to optimally perform SOA at this organization. This document will be used by the SOA governance effort to drive the needed changes.	SGVM Monitoring phase

Artifacts are also used to feed governing processes; example processes and the artifacts used by them are found in Appendix A. The extent of these artifacts depends on the principles and the maturity of the organization. The detailed content is described during the Define phase of the SGVM. A sample set of governing process artifacts used in the SOA governing processes have been identified as follows:

Artifacts	Description	Created by
Appeal Record	Documentation of an appeal to an exception and the resolution.	Dispensation process
Exception Record	Documentation of an exception at a compliance checkpoint.	Dispensation process

Artifacts	Description	Created by
Dispensation Record	Documentation of a dispensation to an exception.	Dispensation process
Compliance Record	Documentation of the approval at a checkpoint.	Compliance process

4.6 SOA Governance Technology

The purpose of this section is to identify technology capabilities that can be used to perform the SOA governing processes. It will not discuss or identify capabilities for the governed processes, but in some cases the identified capabilities might support both the governing and governed processes (e.g., a repository or a policy enforcement tool).

SOA Governance Technology is technology to be used to enable governance and the whole or partial automation of the governing processes. A framework for technology capabilities can range in ability from manual processes to sophisticated software. Technology capabilities used by the governing processes include:

- Store and access capability – A technology framework should be available for storing and accessing governance artifacts, such as internal or external web sites, registries, repositories, configuration databases, or knowledge management repositories.
- Policy enforcement capability – An SOA governance policy framework helps to support and possibly automate the monitoring for violations of governance policy. This can include both design time and run-time governance.
- Monitoring capability – An SOA monitoring framework can be used to measure and gather metrics on the SOA services and policy enforcement and the appropriateness of the current governance regimen. A monitoring framework can be used to implement governance enablement and trigger the checkpoints in the Compliance process.
- Management capability – SOA management tools, such as change control or configuration management, can be used to implement and maintain governance. There may also be governance guidelines regarding the usage of these tools. Security management capabilities are also key to ensure visibility of the results of governed processes to appropriate stakeholders. This is especially important for the governance Compliance and Vitality processes.
- Workflow capability – Capturing Compliance and Dispensation processes as workflow documents and enabling automation of the processes.

SOA Governed Technology is technology that is used by the governed SOA processes. Other specifications, such as SOA reference architectures, define what technologies should be used to develop, deploy, and operate an SOA solution. SOA Governed Technology also needs governance, but the governance of these technologies is part of the Service and Solution Portfolio and Lifecycle Management processes, not detailed in the present document, just like the governance of SOA processes and SOA communications.

5 SOA Governance Vitality Method (SGVM)

The SOA Governance Vitality Method (SGVM) is a process that utilizes the SOA Governance Reference Model (SGRM) as a baseline and then follows a number of phased activities to customize this baseline model to cater to the organization's variants. SOA governance should be viewed as a process and not a project; therefore, the phases of the SGVM should be viewed as a continuous improvement loop, whereby progress is measured, and course-correction and updates to the SOA Governance Regimen and SOA Governance Roadmap are performed when needed.

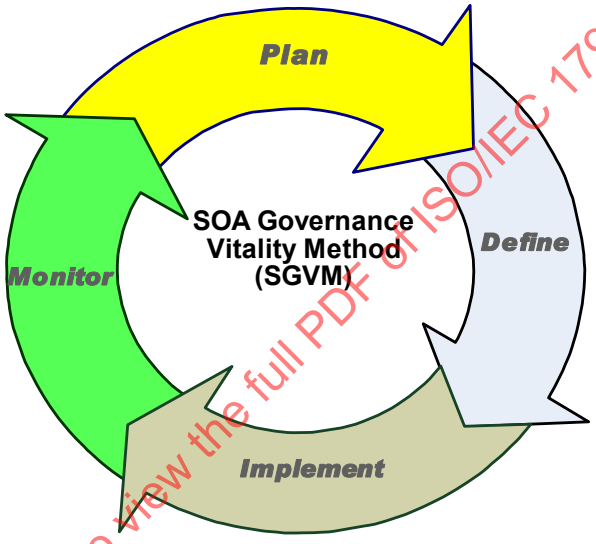

Figure 7: SGVM Phases

The phases of the SGVM as illustrated in Figure 7 are:

- **Plan** – Identify and analyze the core governance areas for improvement. Establish objectives/plan and specific measures for a proposed increment. Previously deployed increments are also evaluated for any necessary improvement.
- **Define** – Define the SOA Governance Model Transition Plans required to deliver the objectives defined in the Plan phase.
- **Implement** – Implement the Transition Plans including deployment of processes, organization, and technology aspects of the SOA Governance Model.
- **Monitor** – Monitor the effectiveness of the currently deployed SOA Governance Regimen and whether it is meeting its intended purpose. This phase may start another iteration of the SGVM.

5.1 Plan Phase

It is in the Plan phase that the needs and priorities of the business are documented, along with the role of the organization in meeting those needs. Also, the state and maturity of the current organization's governance are assessed and gaps are identified. From all this analysis, the SOA governance vision and strategy, as well as the scope, are documented. A governance roadmap may be created to describe planned future iterations of the SGVM.

Figure 8: Plan Phase Activities

5.1.1 Understand Current Governance Structures

The purpose of this activity is to understand the current governance structures of the organization and use them to understand how the generic framework should be adapted. The structures for Business, IT, and EA governance are examined from process, organizational, and technology points of views. If any SOA governance structure or IT governance structure that

would also be useful for SOA governance exists, it can be used as a starting point. Existing IT and EAe control points should be analyzed for re-use and relevance in the SOA context.

The main tasks within this activity are:

- Identify SOA governance stakeholders; this will include some that are pertinent on a tactical perspective, as well as strategic (which may include a different set)
- Investigate the current governance model by reading existing documentation, interviews, and workshops with stakeholders

5.1.2 Assess SOA Maturity

The purpose of this activity is to create an understanding of the maturity level of SOA within the organization and its change readiness to ensure the SOA Governance Framework is defined to a level appropriate for the organization.

Note: When the maturity level increases, the SOA Governance Regimen needs to be modified (detected in the Monitor phase and managed in the next iteration through the SGVM).

The maturity assessment allows you to have a good understanding of where an organization is at the present time. A complementary effort is to define where they want to be. These two activities can serve as input for the formation of a governance roadmap.

The OSIMM (see Referenced Documents) can be used to structure this assessment. Using OSIMM, the SOA maturity of the organization is assessed across a set of perspectives:

- Business – includes how the business has structured itself for change (e.g., whether any process management efforts exist).
- Organization – includes several governance elements, including assessing the current SOA governance capabilities (organization, processes, technology).
- Methods – includes the techniques used in the current SOA processes (from inception to delivery).
- Applications – includes assessing how applications are managed as a set, and particulars regarding their assembly and maintenance.
- Architecture – includes assessing the core structures and patterns influencing the current technical direction and used as foundation for designs in the organization.
- Information – includes assessing the approaches given to data management and business intelligence.
- Infrastructure – includes assessing the current infrastructure capabilities to support the needed SOA effort.

Tasks within this activity make use of workshops and interviews to achieve their goals. Complementary to the maturity assessment, a change-readiness assessment may also be delivered using tools like Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis.[1]

It should be noted that not all assessments need to include all the categories listed above. There may be situations in which a focus solely on the organizational perspective, including governance, would be preferred.

5.1.3 Develop SOA Governance Vision and Strategy

The purpose of this activity is to develop the long-term vision for SOA governance for the organization and the strategy to realize it.

The main tasks within this activity are:

- Use the SOA governance principles and SOA strategy to create the long-term SOA governance vision for the processes, organization, and technology for the organization
- Develop a high-level strategy for achieving that vision, including:
  - — Definition of the return-on-investment of governance activities
  - — Definition of the metrics necessary to be able to measure the value of the governance activities (examples can be found in Appendix C)
  - — Execution of an analysis of the organization strategic initiatives and their relation to possible SOA efforts; this will help clarify prioritization within the SOA governance strategy

5.1.4 Develop SOA Governance Scope

The purpose of this activity is to set the scope of the SOA governance effort including identifying the people and processes in the organization that will be affected and the level of control that will be applied. This is important because there could be a seemingly infinite number of governance mechanisms (e.g., control points, policies, etc.) that could be put in place. This activity focuses on making sure that only the needed governance elements, as scoped by particular SOA maturity, needs, and risks, are defined. The scope is defined using the principles, the current governance, and the maturity level.

5.1.5 Develop SOA Governance Principles

The purpose of this activity is to adapt the generic SOA governance principles from Section 4.1 to the specific organization.

The main tasks within this activity are:

- Validate the generic SOA governance principles against the organization:
  - — SOA strategy

[1] Refer to http://en.wikipedia.org/wiki/SWOT_analysis.

— SOA maturity

— Organization, business, and IT principles

- Add appropriate SOA governance principles unique to the organization
- Create an SOA governance principle list with descriptions, motivations, and implications
- Get approval of SOA governance principles from the proper stakeholders (including program sponsors)

5.1.6 Develop SOA Governance Roadmap

The purpose of this activity is to develop an SOA Governance Roadmap which will define a number of iterations of the SGVM cycle. The first SGVM cycle should provide for the practical initial deployment of the SOA Governance Regimen. Additional iterations are defined to eventually realize the SOA governance vision. As SOA maturity increases, this SOA Governance Roadmap will need to evolve. In addition, the SOA Governance Roadmap will need to be in synch with the SOA Roadmap as it is deployed and adjusted.

5.2 Define Phase

The generic SGRM is used with the results from the Plan phase to create the target SOA governance architectures for the organization, processes, and technology.

The gap between the current SOA governance and the target is analyzed and used to create a set of transition roadmaps. These transition roadmaps contain transformation initiatives for organizational, process, and technology areas for this iteration of the SGVM.

Figure 9 shows a set of activities to be performed during the Define phase, not necessarily in this exact order.

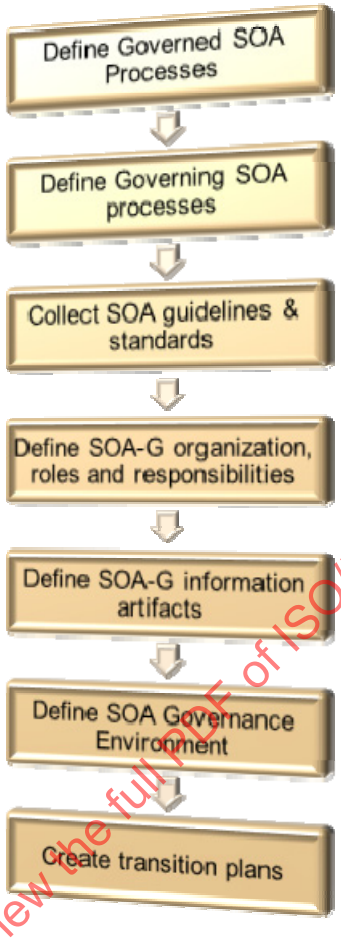

Figure 9: Define Phase Activities

5.2.1 Define Governed SOA Processes

The purpose of this activity is to identify the SOA processes used by the organization to be modified or have checkpoints added to enable SOA governance. The processes from Section 4.3 are:

- SOA Solution Portfolio Management
- SOA Solution Lifecycle
- Service Portfolio Management
- Service Lifecycle

Appendix A provides a set of exemplar SOA processes and suggested SOA governance opportunities and checkpoints. The main task of this activity is to review the existing SOA process together with the example processes and checkpoint and describe the target SOA processes and checkpoints according to the SOA governance scope, vision, and strategy.

5.2.2 Define Governing SOA Processes

The purpose of this activity is to adjust the SGRM governing processes to the organization. The governing processes are defined in Section 4.2 (Compliance, Dispensation, and Communication).

- Compliance – The purpose of this activity is to define a method to ensure that the SOA guidelines and standards are adhered to. Roles and organizational aspects should also be identified for execution of the Compliance process. A suggested method is to use the SOA Governance Checkpoints inserted into the SOA processes in the previous step. A set of possible checkpoints can be found in Appendix A.
- Dispensation – The purpose of this activity is to define the method to initiate Exception processes from Compliance processes. Define the detailed processes for the organization and the roles within the organization for carrying them out.
- Communication – The purpose of this activity is to educate, communicate, and support both the architecture and the SOA guidelines and standards across the organization. This activity should also identify communications mechanisms and technologies for making governance policies available.

5.2.3 Collect SOA Guidelines and Standards

The purpose of this activity is to collect existing SOA guidelines.

5.2.4 Define SOA Governance Organization, Roles, and Responsibilities

The purpose of this activity is to define the SOA governance organization and the associated roles and responsibilities.

The main tasks within this activity are:

- Adapt the generic organizations from the SGRM to the needs of the business
- Create additional specific, custom organizations which may be unique to the business
- Adapt the generic roles and responsibilities from the SGRM to the needs of the business
- Create additional custom roles and responsibilities for the organization which may be unique to the business

RACI diagrams may be used to document this.

5.2.5 Define SOA Governance Information Artifacts

The purpose of this activity is to define the information entities used in both the governing and governed SOA governance processes.

The main tasks within this activity are:

- Identify the governing processes information entities to maintain
- Identify the governed processes information entities to govern (ensure correctness)

The nature of the governed process information artifacts will depend on the governed processes defined in the previous steps.

A set of possible SOA information entities can be found in Appendix B.

5.2.6 Define SOA Governance Environment

The purpose of this activity is to define the target SOA Governance Technology solution.

The main tasks within this activity are:

- Derive the SOA technology needs from the SOA principles, SOA strategy, SOA maturity, SOA governing/governed processes, information artifacts, and information usage.
- Ensure that the technology can support the current maturity level of the organization.
- Identify technologies which could include tools, such as registries and repositories. Some of these technologies may be used by both governed and governing processes. Tools may also include tools to manage architectural assets, policy, and knowledge.

5.2.7 Create Transition Plans

The purpose of this activity is to create a set of Transition Plans using defined organizational, roles, and processes using the SOA governance principles, the SOA governance strategy, and information about the organization.

There are three different transitions plans produced.

Organization Transition Plan

This plan contains the organizational roles and responsibility changes needed. The Organization Transition Plan includes an organizational assessment, future organizational design, identification of roles and responsibilities within these new organizations, a change readiness assessment, and transition processes which outline the impact on the organization. Organizational changes are made in parallel with the Process and Technology Transition Plans. Different organization changes may be needed as different tasks of the Implement and Monitor phases of the technology transition are executed. Appropriate linkage to the IT Transition Plans should be identified.

Some tasks that may be part of the Organization Transition Plan include:

- Identifying the stakeholders
- Identifying the organizations relevant to SOA governance, and defining how they interact with each other
- Identifying changes in the specific roles and responsibilities of the personnel within the organizations defined
- Identifying development and governance teams
- Identifying plans to address resource or talent gaps identified during the Define phase

- Scheduling training and education on the governance process

Process Transition Plan

The Process Transition Plan contains the processes changes necessary to implement SOA governance. The SOA Governance Process Transition Plan includes the set of detailed activities necessary to migrate the current governance processes, if any, to the newly defined ones. This may mean defining changes to implement in current processes and education on those new processes. A Program Manager should be assigned to provide overall management and standard project management of the SOA Governance Process Transition Plan.

Each step in the Transition Plan will address a governance deficit that was identified in the governance planning and definition steps. Each step will be created as a result of a Work Breakdown Structure which specifies the set of activities that must be performed in order to rectify the governance deficit. Each step in the Transition Plan can be expected to:

- Make use of governance "assets" that provide information on best practices, examples, process diagrams, or other assets as defined by those knowledgeable in governance state-of-the-art
- Have specified roles and responsibilities
- Have a schedule associated with the Transition Plan implementation

Technology Transition Plan

This plan contains the technology transition needed to implement SOA governance. The SOA Governance Technology Transition Plan includes the set of detailed implementation and deployment plans for the necessary governance supporting application and IT infrastructure. This includes identifying supporting infrastructure like repositories, registries, policy evaluation engines, and tools. Any missing technologies will need plans to acquire them. The Technology Transition Plan will need to include:

- Technology gap analysis and proposals
- Technology funding and acquisition plans
- Technology deployment plans
- Guidelines for each implementation project
- Architecture contract to govern the overall implementation and deployment process

5.3 Implement Phase

The Implement phase is responsible for enabling and realizing the governance solution determined in the Plan and Define phases. This phase implements the Transition Plans including deployment of processes, organization, and technology aspects of the SOA Governance Model. At the end of this phase, the SOA solution will be ready to be managed and governed.

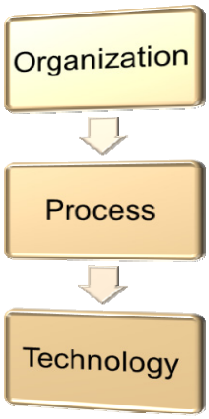

Figure 10: Implement Phase Activities

The Define phase provides the SOA Governance Organization Transition Plans, SOA Governance Process Transition Plan, and SOA Governance Technology Transition Plan. The Organization Transition Plan includes plans for implementing organizational changes and possibly identifying either an organization change lead or a responsible governing body like an Enterprise Review Board which consists of business and IT executives. The Process Transition Plan includes the set of detailed activities necessary to migrate the current governance processes, if any, to the newly defined ones. The Technology Transition Plan includes selection of SOA governance tools, SOA governance infrastructure, SOA governance process, and organization metrics. Most importantly, from an execute perspective, it includes the detailed Migration and Implementation Plans which must now be implemented.

Effective project management is important for the Implement phase of SOA governance, just as one would do for any strategic project. As this will consist of implementation of the defined Transition Plans, it is important to consider the best manner in which this plan should be considered for implementation, that is, "governance of the governance implementation". This should include at a minimum:

- Before starting implementation of these Transition Plans, develop guidelines for each implementation project.
- Create a project plan to govern the overall implementation and deployment process. Throughout this phase it is important to perform the appropriate governance functions while the system is being implemented and deployed. This includes identifying and contracting appropriate skills to execute the Transition Plan, including development, test, deployment, and executives.
- Be sure to review the Transition Plan and update it to reflect interim lessons learned, new initiatives, and approaches.

5.3.1 SOA Governance Organization Transition Plan Implementation

The Organization Transition Plan is executed over time and in a coordinated fashion with the Process Transition Plan and the Technology Transition Plan.

5.3.2 SOA Governance Process Transition Plan Implementation

The Process Transition Plan is executed to actually implement the governance checkpoints in the governed processes and to implement the governing processes.

5.3.3 SOA Governance Technology Transition Plan Implementation

Implementing the SOA Governance Technology Transition Plan includes doing gap analysis between available technology and the target technology. An acquisition and change to the current system may need to be made to fill the gap according to the Technology Transition Plan. During implementation this plan must perform appropriate governance functions while the system is being implemented and deployed. It must also ensure conformance with the defined architecture by implementation projects and other projects.

The following tasks are part of the implementation of any of these Transition Plans:

- Implementation of SOA Governance Framework Assets – Implement and/or acquire tools and mechanisms needed to support SOA governance. This includes instrumentation of existing SOA services, processes, and assets to enable their governance. Tools may require acquisition, installation, and configuration of hardware and software. Like any other development project, during detailed design and development milestones can be set to periodically check continued adherence to governance requirements and policies. Development tools doing model analysis and policy-based rules to support ongoing governance monitoring.

- Assemble the Governance Solution – Ideally the governance solutions should follow predefined rules and processes based upon defined SOA governance architectural principles and standards. In addition, techniques defined to implement and assemble SOA solutions in general should be used. This includes implementing flows, automated orchestrations, and business rules to drive governance. Ensure that these solutions adhere to the governance policies and requirements.

- System Verification – After the governance framework is built, conformance with the governance solution architecture, principles, design, and policies should be verified. Testing should include stress testing the governance framework for appropriate Quality of Service (QoS) and performance compliance.

- Deploy – Deploy governance mechanisms, governance IT infrastructure, and governance policies into different staging environments (e.g., testing, pre-production, production). This includes deploying governance policies into a repository for ongoing use during the Monitor phase. It also includes managing the deploy information, registration, configuration, and versioning of the SOA governance solution and release into production using service contracts and service policies that are deployed with the solution.

- Conformance Verification – Check for compliance at the end of the Implement phase to ensure conformance with the defined SOA governance architecture by implementation projects and other projects. Certify services and solutions as being compliant with the IT and Business Transition and Migration Plans.

Implementation concludes with initial verification of the deployed governance solution framework. Ongoing testing and verification of conformance of the SOA governance solution to

the governance principles and policies and the furtherance of SOA governance vitality will be done in the Monitor phase.

5.4 Monitor Phase

The Plan and Define phases defined previously have created the governance solution and the Implement phase has implemented the governance Transition Plans including deployment of processes, organization, and technology. The Compliance processes are now running to govern the SOA processes, organization, and technology. The Monitor phase is responsible for monitoring the governing and governed processes to determine whether the SOA Governance Regimen needs to be adjusted. If they do need to be adjusted, a new iteration of the SGVM cycle is initiated.

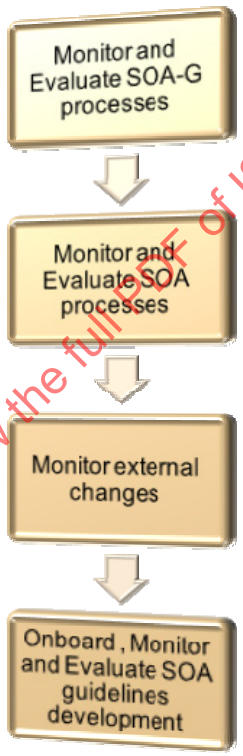

Figure 11: Monitor Phase Activities

Specifically, the Monitor phase must consider and evolve the governance policies, procedures, organizations, roles, and responsibilities. While the basic need for governance has not changed, the organization will acquire additional maturity that will require a proportional increase in governance maturity. Metrics will show what aspects of governance are working and what aspects require change. No matter how good a job has been performed in the previous phase of Plan, Define, and Implement of SOA governance, that governance needs to stay current and vital in its job of producing quality for services.

5.4.1 Monitor and Evaluate SOA Governed Processes

As governance events take place, various metrics should be gathered that provide information on the quality of the tasks that SOA governance is governing. Management and measurements of goals help an organization to judge the effectiveness of the SOA governance effort and where additional discipline is needed. SOA governance like any other discipline needs to first define a set of goals that it strives to achieve. A corresponding set of metrics should be defined to measure the goals that the governance framework strives to achieve. SOA governance is responsible for periodically reviewing these metrics and making the needed changes to governance policies, standards, and processes through iterations of the SGVM cycle.

The monitoring of metrics of the governed processes, Service Portfolio and Lifecycle Management as well as Solution Portfolio and Lifecycle Management, happens constantly. Evaluation may happen in real-time or periodically; i.e., weekly, monthly, quarterly, or yearly. Some real-time monitoring metrics could be provided by SOA business activity monitoring tools.

5.4.2 Monitor and Evaluate SOA Governing Processes

As a result of the gathering of such governance metrics, ongoing events may force changes to SOA governance. For example, metrics may notice that the percentage of rejections for service design is trending upward and it is necessary to find out why and take action. An investigation in this case may show that a particular policy is causing this rejection. The governance team would then need to consider whether the policy is too restrictive or if further education needs to take place. In any case, such periodic reviews will identify areas of concern and follow-up action.

Monitoring the governing processes (Compliance, Dispensation, and Communication) also happens constantly. However, evaluation happens periodically; i.e., weekly, monthly, quarterly, or even annually.

5.4.3 Monitor External Changes

External “shocks” may trigger a review of the SOA journey and the corresponding SOA governance. These triggers may cause an adjustment of the SOA Governance Regimen and another iteration of the SGVM to implement them. Overall, a monitor review should take place for:

- **Business strategy changes**: Any change in business strategy will likely cause an update of the business vision and perhaps changes to business processes. While the existing SOA governance processes will probably not change, care must be taken to ensure that the service portfolio planning is updated correctly. There may be some new governance planning and definition that needs to happen to accommodate the change in business strategy.
- **Organizational changes**: Decision rights will undoubtedly change as the result of significant organizational changes. An organization change should trigger a review of the governance processes and the corresponding decision rights.
- **Legal or regulatory changes**: SOA governance should already have a process to assess and process legislative and policy changes. Such a change may have such a huge impact,

however, that it is necessary to review the current SOA governance processes for increased control reviews. For example, Sarbanes-Oxley2 required more stringent audit procedures on financial systems. In some cases, these audits may have been new for the governance process and would have required a vitality review and subsequent insertion of new governance processes.

- **On board and change guidelines and standards**: New or updated significant industry standards should trigger a review of current standards used by SOA. The SOA governance function, as the leader of this review, should be able to identify where the new guidelines and standards are relevant and should drive the discussion and subsequent implantation of the changes.
- **Technology improvements**: As for standards, a significant technology change may result in a better technique for creating service quality. For example, better tooling may help in automating the governance control points, thereby providing earlier and better feedback on service quality.
- **Consistent or repeated non-compliance of the SOA governance policies and standards**: When the SOA governance function sees a pattern of non-compliance with the relevant policies and standards, then a vitality review should be triggered. Are the policies and standards too tight? Unrealistic? Is the compliance function too weak? Is leadership lacking and management support non-existent? While SOA governance cannot necessarily change these by itself, its duty is to call these out for notice and action.
- **Repeated requests for policy and standard exceptions**: Granting exceptions to the governance rules is a normal situation and, if used in a judicious manner, is no cause for concern. If a repeated pattern of exceptions is detected, however, then a vitality review is called for to ask similar questions as noted above for non-compliance.

5.4.4 Monitor and Evaluate SOA Guidelines Development

SOA guidelines development includes the articulation of and update of policies, principles, standards, and guidelines. This process needs to be monitored and governed just like the other SOA processes. Metrics should be established that can be monitored and evaluated periodically: weekly, monthly, quarterly, or yearly. Sufficient changes to these guidelines may cause an iteration of the SGVM cycle to bring the governance regimen into alignment with the new guidelines.

5.5 SGVM Use of SOA Governance Artifacts

The SGVM cycle produces and uses SOA governance artifacts. Figure 12 summarizes which SGVM phases create which artifacts.

[2] Sarbanes-Oxley Act (US Public Company Accounting Reform and Investor Protection Act 2002)

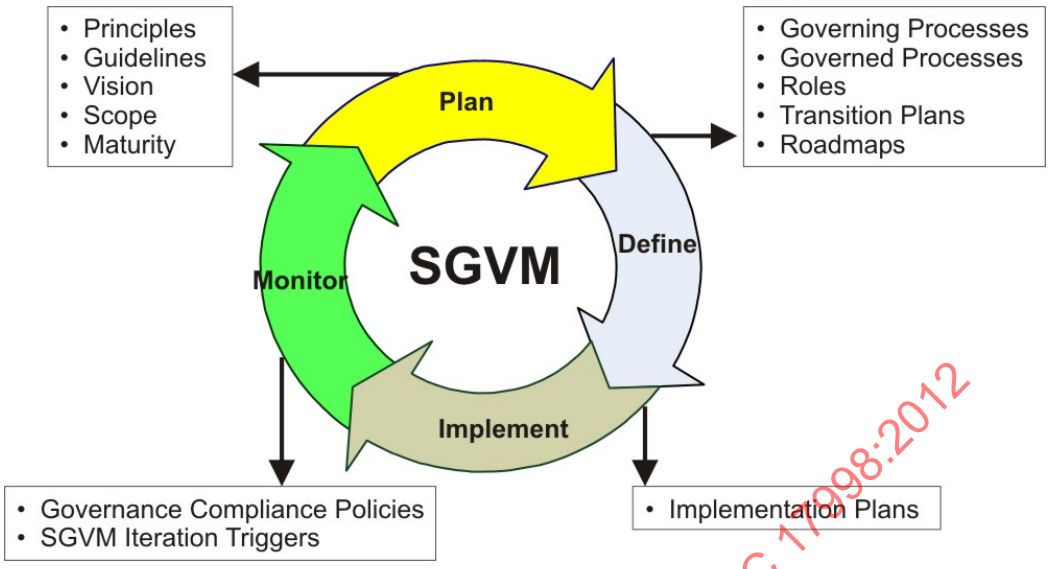

Figure 12: SGVM Cycle Artifacts

The Plan phase produces the SOA governance principles, guidelines, vision, and scope. This phase also produces SOA and SOA governance maturity assessments for current and desired maturity levels.

In the Define phase, the governed processes are identified and documented and the governing processes for compliance and dispensations are documented. SOA governance roles and responsibilities are defined and assigned and SOA Governance Roadmaps and Transition Plans for organization, process, and technology are documented.

During the Implement phase, the Transition Plans are translated to Implementation Plans and executed.

During the Monitor phase, the Compliance processes are running and being monitored via policies on metrics and checkpoints. Policies on triggers for re-evaluating the current SOA Governance Regimen are identified and monitored. Re-evaluation may result in a decision to do another iteration of the SGVM.

A SOA Governance Process Activities

The purpose of this appendix is to provide information regarding suggested governing and governed processes. The information is intended to provide guidance and thought-leadership for consideration as you define the governing and governed processes for your organization or company. They do not have to be followed verbatim. The activities in the appendix represent key SOA governance activities. There may be additional IT governance-related activities needed as part of normal portfolio and lifecycle management.

The appendix is divided into two major sections: governing processes and governed processes. The processes correspond to the content in the main sections of this SOA Governance Framework document. Each section is divided into subsections. Each subsection includes process and checkpoint tables. The process tables provide suggestions for process names, goals, inputs, activities, and outputs. Each process table is followed by a checkpoint table. The checkpoint is a key activity listed within the process table that serves as an approval point within the process.

A.1 SOA Governing Processes

The SOA governing processes are applied to the SOA governed processes as described in Section 4.2. They are Compliance, Dispensation, and Communication.

Compliance Activities

Compliance reviews may be triggered by multiple events:

- SOA process-based during the execution of the governed processes
- Project management-based, such as approval gates or project task milestones
- Vitality-based (triggered by the SGVM; could be temporal or event-based)

Compliance reviews may be conducted as part of a standard quality review, such as the checkpoint at the end of a Design phase within a system development methodology. Compliance may also be measured via an ongoing monitoring and analytics method, such as an information collection method during the operation of the governed processes.

Compliance reviews may also be initiated as part of an ongoing monitoring process cycle, such as the SGVM. The cycle may specify that processes be reviewed at specific temporal-based dates within a fiscal year, such as every three or every six months. The cycle may also specify event-based triggers related to business or IT events, such as major organizational changes affecting the membership of the SOA Governance Steering Board.

The compliance results indicate where the governed processes conform to the compliance requirements and non-conforming exceptions. The exceptions should be adjusted or re-aligned in order to meet the compliance requirements, or the Dispensation process may be initiated.

PROCESS	Perform Compliance Review
Goal	Determine adherence or non-conformance based upon the established SOA governance compliance criteria and strategies.
Input	Compliance review request Service change proposal Service contract Service policy Compliance evaluation criteria
Activities	Conduct compliance assessment Ensure that compliance gaps have been documented Ensure that gap resolutions are identified Evaluate risk of non-conformance Document governance vitality metrics
Output	Compliance validation Compliance risk analysis

CHECKPOINT	Document Compliance Completion
Input	Compliance review request Service change proposal Service contract Service policy Compliance evaluation criteria Compliance decision and resolution
Activities	Identify open compliance requests Collect compliance results, such as decisions, non-conformance risks, compliance follow-up action items, compliance reviewers, and compliance evaluation criteria used Close the compliance request
Output	Compliance documentation
Used Guidelines	SOA Governance Compliance Management Guidelines

Dispensation Activities

If compliance requirements cannot be met, the Dispensation process may be initiated. The Dispensation process activities are to conduct an appeal and request a dispensation. A dispensation approval may be fully or partially granted, or not granted. If the dispensation is not granted, then the items not in compliance must be corrected. If the dispensation decision is not agreed with, the issue may be escalated to the next level of governance.

If a new condition, obsolete condition, or error in the dispensation guidelines occurs, then a trigger should be issued to the SGVM process.

PROCESS	Manage a Dispensation Request
Goal	The processes defined within the governance framework or contract for resolving disputes between parties.
Input	Dispensation log Appeals request Escalation contacts Disputed service contract Service policy Incident reports (unresolved) Problem report Service audit reports Service performance reports Service user interaction report Service test results
Activities	Receive and log the appeals requests Identify the proper reviewers for the dispensation review Conduct the dispensations review Document the dispensation results Perform the dispensation follow-up activities at the specified time or event (relevant when the dispensation approval is for an interim time period until a final corrective solution is in place) Close the dispensation request
Output	Contract violation resolution (resolved dispute or escalation) Service change proposal (possibly) Service contract (possibly updated) Service policy (possibly updated) Dispensation log

CHECKPOINT	Document Dispensation Completion
Input	Contract violation resolution (resolved dispute or escalation) Service change proposal (possibly) Service contract (possibly updated) Service policy (possibly updated) Dispensation review results
Activities	Review open dispensation request Collect dispensation results, such as decisions, accepted risks, dispensation follow-up action items, dispensation reviewers, and dispensation evaluation criteria used Close dispensation request or schedule follow-up actions per the dispensation results
Output	Dispensation documentation
Used Guidelines	SOA Governance Dispensation Management Guidelines

Communication Activities

The SGVM Plan phase identifies the SOA governance stakeholders, defines the communication strategy and plan, and then identifies the communication channels to be used. The SOA governance communication activity is to execute the Communication Plan and measure the associated compliance.

PROCESS	Communication
Goal	Communicate according to the communication strategy.
Input	Stakeholder analysis (from SGVM Plan phase) Communication strategy (from SGVM Plan phase) Communication plan (from SGVM Plan phase) Communication channels (from SGVM Plan phase)
Activities	Execute the communication plan
Output	Media as specified in the communication plan

CHECKPOINT	Measure Compliance to Communication Plan
Input	Communication plan
Activities	Conduct compliance assessment of the executed communication plan tasks
Output	Compliance report Compliance exceptions Compliance corrective action plan Compliance dispensation plan
Used Guidelines	SOA Governance Metrics Guidelines Standard Project Management Guidelines

A.2 SOA Governed Processes

SOA governing processes are executed to provide governance to the planning, design, and operational SOA processes, referenced in this document as SOA governed processes. This section provides information regarding the goals, inputs, activities, and outputs of the SOA governed processes. Process checkpoints denote key approval points. This information may serve as the starting point for defining new SOA governed processes. It may also be used as a validation to identify gaps in existing SOA governed processes.

To better understand the interactions between the SOA governed processes, the information flow between the SOA governed processes in Figure 13 shows the relationships between the major process components.

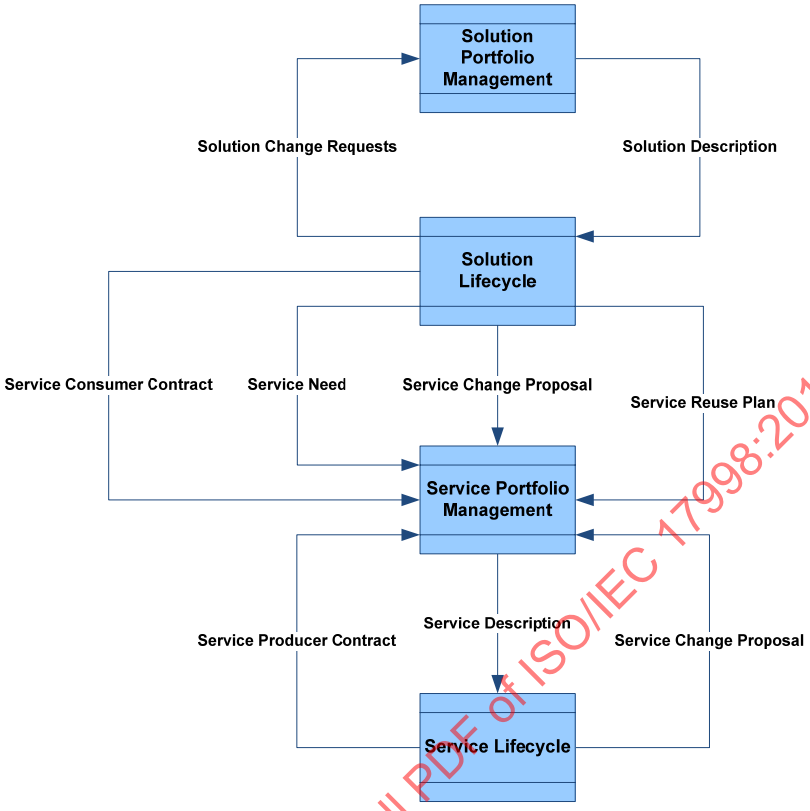

Figure 13: Main SOA Information Flows

Information Entity	Description
Solution Change Request	Description of proposal for solution change
Solution Description	Description of a solution
Service Consumer Contract	Description of the contract between a consumer and a service provider
Service Need	Description of the requirements of a service
Service Change Proposal	Description of proposal for service change
Service Re-use Plan	Description of the existing services a solution wants to use
Service Producer Contract	Description of the contract between Service Portfolio Management and the service producer
Service Description	Description of the service

A full set of possible SOA information entities can be found in Appendix B.

Service Portfolio Management Activities

PROCESS	**Service Portfolio Planning**
Goal	Identify needed changes to your service portfolio, including new services, changes to existing services, re-factoring of existing services, and retiring of existing services.

PROCESS	Service Portfolio Planning
Input	New service needs Service change proposals Service usage plan and contracts Service funding model Enterprise architecture plan
Activities	Manage new service needs received and analyze their business justification Manage service change proposals Manage new and changed service contracts Identify and manage changed service policies Identify service capacity in relation to service usage needs from the service contracts and propose changes to the services if needed Plan for service obsolescence Plan for service versioning Analyze emergent usage patterns to identify shortcomings or gaps in the current service portfolio Assign ownership to new services Assign funding to new services Assign appropriate classifications or other information used to locate the service within your service catalog Catalog the services that will be created, enhanced, used, or retired as part of the projects that implement the service roadmap Validate service planning against the enterprise architecture plan
Output	Service roadmap New overview service descriptions including, e.g.: • Service contracts for the first consumers • Service policy • Service classification • Service ownership • Service funding • Service version • Business justification • Usage plan (if the service will use other services) Updated service descriptions

CHECKPOINT	Approve Service Roadmap
Input	Service roadmap New overview service description including, e.g.: • Service contracts for the first consumers • Service policy • Service classification • Service ownership • Service funding • Service version • Business justification • Usage plan (if the service will use other services) Updated service descriptions
Activities	Approve service roadmap Approve service description (as above)
Output	Approval of service description Approval of service roadmap
Used Guidelines	Service Portfolio Guidelines Service Classification Guidelines Service Ownership Guidelines Service Business Justification Guidelines Service Change Management Guidelines Service Contract Guidelines Service Policy Guidelines

PROCESS	Service Identification and Business Justification
Goal	This process identifies services from a business process decomposition, requirements for information as a service, or application decomposition.
Input	Business needs Solution process Enterprise architecture Service portfolio (existing services, both planned and operational)
Activities	Analyze if the service is justified to the current business strategy and EA and fits with the long-term goals of the organization Analyze if the service can perform according to the desired business needs (both functional and non-functional) Analyze the re-use potential of the service Analyze the costs of operating and consuming the service
Output	Service identification Service characteristics Service portfolio (existing services, both planned and operational)

CHECKPOINT	Approve Identified Services
Input	Service identification Service characteristics Service portfolio (existing services, both planned and operational)
Activities	Review the identified services Approve identified service definitions
Output	Approve selected service definitions
Used Guidelines	Service Identification Guidelines Service Taxonomy Guidelines

PROCESS	Service Ownership
Goal	This process identifies and manages service domains and service ownership (need to identify domains and owners for the services that may arise from solution development and also services that may be consumed by the solution).
Input	Service portfolio
Activities	Classify the service to understand what domain it belongs to Analyze service ownership (has an impact on service funding)
Output	Service classification Service ownership

CHECKPOINT	Approve Service Ownership
Input	Service classification Service ownership
Activities	Ensure compliance to guidelines
Output	Approval of service ownership
Used Guidelines	Service Classification Guidelines Service Domain and Ownership Guidelines

PROCESS	Service Funding
Goal	This process establishes the rules for service funding as well as enhancing the services and mechanisms used to provide incentives for service re-use (or charge-back).
Input	IT funding model SOA governance principles Organizational & financial structures
Activities	Define the service funding model based on the IT funding model, governance strategy and principles, SOA maturity level, and organizational & financial structures
Output	Service funding model Service incentive model

CHECKPOINT	Approve Service Funding Model
Input	Service funding model Service incentive model
Activities	Ensure that a funding model exists and is used
Output	Approval of service funding model
Used Guidelines	Service Funding Guidelines

PROCESS	Service Change Management
Goal	Additional change management concerns beyond traditional deployments exist for loosely connected solutions where build dependencies are not easy to control within configuration management. Examples include: 1. A package application which is interfaced via an API is upgraded to a newer version. 2. A package application which is interfaced via an API has new configuration applied which gives it different behavior to the integrated transaction. This can also happen if the underlying data changes in context; that is, the business rules associated with that data are altered. 3. A database which is interfaced via a database connector is altered at the table, element, index, or table space level. This type of change can break the implicit binding between the database and the connector. 4. The operating system can be altered via an upgrade or completely swapped out to a different O/S. This type of change can impact a remote connector software driver and disable it. 5. The network can be altered in many ways, where changes to the DMZ, firewall, routers, and hubs can negatively impact the lower-level bus services of the integrated solution. 6. Other application services which provide support to the distributed solution can change without warning; proxy server, web server, LDAP, etc. 7. Components outside of the LAN and WAN can negatively impact the integrated solution; for example, loss of Internet, remote SOAP/XML/HTML packets are altered. Any B2B transaction has this type of issue. These application, infrastructure, and environmental impacts are outside of the scope of classic configuration management tools. Appropriate change control processes have to be stringent and well devised to capture such a large scope, and are difficult to implement (and rarely are). Integration solutions are notorious for being susceptible to such events. Managing services potentially adds one more risk to the integrated enterprise; however, there are techniques which can minimize the risk and actually make them less risky than the aforementioned.
Input	Service change proposal Service contract (new and revised) Service policy (revised) Service implementation change Service portfolio

PROCESS	Service Change Management
Activities	Analyze possible service implementation change to ensure service consistency; if necessary define changes to service interface Analyze service change proposals Analyze revised service policy Analyze new and revised service contracts Analyze the change request including the cost of redevelopment, revalidating the service, and the solutions using the service Prioritize service changes and revise service roadmap
Output	Service portfolio (revised) Service change

CHECKPOINT	Approve Service Change
Input	Service portfolio Service change
Activities	Ensure compliance to guidelines
Output	Approval of service change
Used Guidelines	Service Change Management Guidelines Service Versioning Guidelines Service Policy Guidelines Service Contract Guidelines

Service Lifecycle Governance Activities

PROCESS	Service Definition
Goal	The process of creating new or changed functional and non-functional requirements for the service based on the service needs and consumers the service will support.
Input	Service Description (from Service Portfolio Management) including: Contracts for the first consumers: • Policy • Classification • Ownership • Business justification • Usage plan (if the service will use other services) Service Processes
Activities	Using the services need, the contract, and the requirements from the service consumers: • Define the functional requirements for the service • Define the non-functional requirements for the service Using the change proposal for existing services: • Define requirements for changes needed • Define requirements changes due to contract or policy changes
Output	Service requirements

CHECKPOINT	Approve Service Requirements
Input	Service requirements
Activities	Ensure that the requirements were defined according to the service requirement guidelines
Output	Approval of service requirements
Used Guidelines	Service Requirement Guidelines

PROCESS	Service Realization Planning
Goal	This process defines the key activities of the analysis to build a service and the techniques required in design, assembly, testing, and deployment of services. Some of the variables may be predetermined by portfolio decisions and reference architectures.
Input	Service description Service metrics Service processes
Activities	Analyze the service requirements to detect if the service should: • Be a new implementation • Use existing legacy functionality • Be an external service • Be a composite of existing services • Be a change of existing service Create a realization plan for the service development and deployment
Output	Service realization plan Service techniques

CHECKPOINT	Approve Service Realization Plan
Input	Service realization plan Service techniques
Activities	Ensure conformance to guidelines
Output	Approval of service realization plan
Used Guidelines	Information Exchange Guidelines ESB Guidelines Pattern Usage Guidelines Security Guidelines Service Development Guidelines Service Interface Guidelines Service Logging/Audit Guidelines Service Project Management Guidelines Service Taxonomy Guidelines Service Versioning Guidelines

PROCESS	Service Modeling
Goal	The detailed design and specification of a service based upon design techniques, patterns, and standards.
Input	Service policy Service realization plan Service techniques Service requirements
Activities	Create the service interface (contact first) or do the interface changes for an existing service: • Use the information exchange model to specify the parameters of the operations • Create a service description using the service taxonomy • For web services interfaces, create a WSDL definition file • For non-web services interfaces, create associated artifacts Create the service implementation model: • Identify applicable service design patterns • Identify appropriate legacy integration patterns, if necessary • Identify possible external service usage • Use the local software development method to create the design
Output	Service model Service policy Service modeling metrics

CHECKPOINT	Approve Service Model
Input	Service model Service policy Service modeling metrics
Activities	Ensure conformance to guidelines Ensure modeling metrics have been collected
Output	Approval of service modeling
Used Guidelines	External Service Usage Guidelines Information Exchange Guidelines ESB/Integration Guidelines Pattern Usage Guidelines Security Guidelines Service Contract Guidelines Service Development Guidelines Service Interface Guidelines Service Logging/Audit Guidelines Service Modeling Guidelines Service Policy Guidelines Service Versioning Guidelines Service Taxonomy Guidelines

CHECKPOINT	Approve Service Model
	Service Pattern Guidelines Legacy Modernization Guidelines

PROCESS	Service Implementation, Assembly, or Acquisition
Goal	Service assembly allows developers to create new services that follow predefined rules and processes based upon defined architectural standards.
Input	Service model Service policy
Activities	Implement the service using the implementation model
Output	Implemented service Service implementation metrics

CHECKPOINT	Approve Service Implementation
Input	Implemented service Service implementation metrics
Activities	Ensure compliance with guidelines
Output	Approval of service implementation Approval of service implementation metrics
Used Guidelines	External Service Usage Guidelines Information Exchange Guidelines ESB/Integration Guidelines Pattern Usage Guidelines Security Guidelines Service Contract Guidelines Service Development Guidelines Service Interface Guidelines Service Interface Guidelines Service Logging/Audit Guidelines Service Policy Guidelines Service Project Management Guidelines Service Taxonomy Guidelines Service Versioning Guidelines Legacy Modernization Guidelines

PROCESS	Service Testing
Goal	Services must be tested at multiple levels to ensure they meet the stated functional and non-functional objectives according to the service contract criteria.

PROCESS	Service Testing
Input	Implemented service Service description Service processes Service requirements
Activities	Development of service test plans including functional, performance, scalability, and security testing and fulfillment of guidelines Execution of service test plans Documentation of service test results
Output	Service test plans Service test results Service test metrics

CHECKPOINT	Approve Service Test
Input	Service test plans Service test results Service test metrics
Activities	Ensure compliance to guidelines Ensure test metrics have been collected
Output	Approval of service testing
Used Guidelines	External Service Usage Guidelines Information Exchange Guidelines ESB/Integration Guidelines Security Guidelines Service Contract Guidelines Service Development Guidelines Service Interface Guidelines Service Logging/Audit Guidelines Service Policy Guidelines Service Project Management Guidelines Service Taxonomy Guidelines Service Testing Guidelines Service Versioning Guidelines

PROCESS	Service Deployment
Goal	The Service Deployment process manages the registration and configuration of services and release into production. Service release management is included in this process.
Input	Service description The service itself Service test results

PROCESS	Service Deployment
Activities	Manage the deployment of the service to different staging environments (e.g., test, pre-production, production) Register the service in the repository to ensure in can be discovered Document specific deployment information Certify deployed service Define capacity and operational and virtualization plan based on load requirements Ensure service approval from consumers
Output	Updated service description with deployment information Updated service catalog Report of certification for the deployed service: • Verification of test results for the final configuration and execution of tests that can only be done on final configuration due to variance from test configuration (such as confidentiality verification) Report of capacity and operational and virtualization plan: • Document describing the IT environment configuration and virtualization techniques used (if any) to meet the service contracts • Should include a list of any shared infrastructure or other services used for service dependencies Approvals/acceptance of the service from the service consumers (serves as approval of service contracts): • Should include monitoring/reporting requirements from each service consumer

CHECKPOINT	Approve Service Deployment
Input	Updated service description with deployment information Updated service catalog
Activities	Ensure that the service is published Ensure that service deployment information is maintained Ensure that the service is deployed in a manner the fulfills the contracts and policies Ensure that service monitoring and management have the correct information available Ensure that the service follows the organization service naming taxonomy
Output	Approved service deployment
Used Guidelines	Service Deployment Guidelines Service Publishing Guidelines Service Taxonomy Guidelines

PROCESS	Service Management and Monitoring
Goal	This process is used to monitor workload and system events that could cause service outages/problems as well as security incidents.

PROCESS	Service Management and Monitoring
Input	Service contract Service deploy results Service infrastructure Service metrics Service policy
Activities	Collect service metrics Audit service Manage service exceptions Enforce service policy Monitor service execution in relation to service contracts Manage service problems Manage rogue services
Output	Service audit reports Service exceptions Service performance feedback Service performance reports

CHECKPOINT	Approval of Service Monitoring and Management
Input	Service audit reports Service exceptions Service performance feedback Service performance reports
Activities	Ensure compliance to guidelines
Output	Approval of service monitoring and management
Used Guidelines	Security Guidelines Service Contract Guidelines Service Policy Guidelines Service Logging/Audit Guidelines Service Monitoring and Management Guidelines

PROCESS	Service Support
Goal	The service support process manages problems, incidents, and the interaction with service consumers.
Input	Service contract Service infrastructure Service policy Service exception Service description Service requirement Service consumers

PROCESS	Service Support
Activities	Resolve service exceptions Create service change proposals when needed Manage interaction with service consumers
Output	Incident report Problem report Service consumer interaction report

CHECKPOINT	Approve Service Support
Input	Incident report Problem report Service consumer interaction report
Activities	Ensure compliance to guidelines
Output	Approval of service support
Used Guidelines	Service Retirement Guidelines Service Change Management Guidelines Service Support Guidelines Service Policy Guidelines Service Contract Guidelines

SOA Solution Portfolio Governance Activities

PROCESS	SOA Solution Portfolio Planning
Goal	Ensure that future business plans are appropriately supported by an up-to-date roadmap of planned development and integration activities.
Input	Business needs and related business cases from either enterprise architecture, business units, or other sources Business objectives, strategies, principles, and budget constraints Solution change proposals and their business cases
Activities	Using the current business objectives, strategies, principles, and budget constraints to: • Identify new initiatives defined since previous roadmap • Identify proposed solution changes • Create a prioritized list of solutions efforts planned for the upcoming two to three years, and map these to development projects • Analyze if SOA is the correct solution for proposed SOA projects
Output	Solution roadmap

CHECKPOINT	Approve SOA Solution
Input	Solution roadmap
Activities	Ensure that the solution roadmap has been created according to the guidelines Ensure that SOA is the correct solution for the business needs

CHECKPOINT	Approve SOA Solution
Output	Approval of SOA as a solution
Used Guidelines	Current IT Portfolio Management Process & Guidelines SOA Initiative Guidelines Solution Change Management Guidelines

PROCESS	SOA Solution Validity
Goal	Provide a mechanism to evaluate initiatives and/or projects with regard to the corporation's desired degree of SOA focus based on overall SOA strategy and current maturity level. The Portfolio Management process may need to be updated to ensure the right mix of projects is selected that advance the ability of the business to be agile. This includes an assessment of services from a project to determine the value of those services beyond that of the project itself. SOA governance needs to ensure that the benefits of service re-use for a particular project are reflected in project selection and prioritization.
Input	Business case Business, IT, & SOA principles Solution requirements Solution constraints Solution process (the process performed by the solution) SOA maturity
Activities	Analyze the validity of the SOA solution
Output	Solution roadmap

CHECKPOINT	Approve SOA Solution Validity
Input	Solution roadmap
Activities	Ensure that the analysis is compliant with the long-term goals of the organization
Output	Approval of SOA solution validity
Used Guidelines	SOA Solution Validity Guidelines

PROCESS	Solution Change Management
Goal	When an incident report is resolved by recommending a change to the solution, a record should be established which justifies the changes to the solution and the cost of revalidating and testing the solution conformance.
Input	Solution change proposal
Activities	Analyze the change request including the cost of redevelopment, revalidating the solution
Output	Updated solution roadmap with the approved solution change proposal

CHECKPOINT	Approve Solution Change Proposal
Input	Updated solution roadmap with the approved solution change proposal
Activities	Ensure compliance to guidelines
Output	Approval of change request
Used Guidelines	Solution Change Management Guidelines

Solution Lifecycle Governance Activities

PROCESS	Solution Definition
Goal	The process for creating a specification of the solution based on the business needs. Important issues due to SOA are: • Define exact process steps and their relationships (used for the choreography and orchestration of the solution) • Define where agility and other SOA properties are needed in the solution
Input	Business needs Business case
Activities	Define the business processes in scope Define the information in scope Define the business rules in scope Define the IT functionality needed to support the business processes and information (including what should be automated and what should be manual) Define agility levels for different parts of the solution Define SOA prioritization for different parts of the solution
Output	Solution requirements including principles, processes, information, business rules, and IT functionality needs SOA prioritization SOA agility levels

CHECKPOINT	Approve Solution Requirements
Input	Solution requirements including principles, processes, information, business rules, and IT functionality needs SOA prioritization SOA agility levels
Activities	Ensure that the business processes, information, business rules, and automated functionality have been defined to appropriate level Ensure that areas of importance for SOA have been defined
Output	Approval of solution requirements
Used Guidelines	Solution Requirement Guidelines

PROCESS	Solution Realization Planning
Goal	This process defines the key activities of the analysis to build the solution and the techniques required in design, assembly, testing, and deployment of the solution. Some of the variables may be predetermined by portfolio decisions and reference architectures. Important changes due to SOA: • Define the relationship between the solution and service development (e.g., will the services be done in the same project or by different project groups)
Input	Business, IT, & SOA principles Solution requirements
Activities	Plan how to develop the SOA solution
Output	Solution realization plan

CHECKPOINT	Approve Service Realization Plan
Input	Solution realization plan
Activities	Ensure compliance to guidelines
Output	Approval of service realization plan
Used Guidelines	BPM Guidelines Portal Guidelines Security Guidelines Service Discovery Guidelines Solution Development Guidelines Solution Project Management Guidelines

PROCESS	Request a Dispensation
Goal	The process defined within the governance framework or contract to request a dispensation based upon a dispute of the compliance review results.
Input	Dispensation request Disputed compliance review results
Activities	Analyze the impact of the dispute results Determine if dispensation should be requested Submit the dispensation request
Output	Dispensation request results Service change proposal (possibly) Service contract (possibly updated) Service policy (possibly updated)

CHECKPOINT	Gain Dispensation Approval
Input	Dispensation request Escalation contacts Impact analysis of the disputed compliance results
Activities	Propose the dispensation plan for future compliance Propose the plan for non-dispensation (for immediate corrective action/fix) Obtain the dispensation approval or non-approval
Output	Dispensation request results Trigger for vitality update (possible new condition or change in Dispensation Management Guidelines)
Used Guidelines	Service Contract Dispensation Management Guidelines Service Contract Guidelines Service Policy Guidelines Security Guidelines

PROCESS	Solution Modeling
Goal	The detailed design and specification of the solution based upon design techniques, patterns, and standards. Important changes due to SOA: • Modeling of processes should be done in a re-usable way. • Design techniques, standards, and patterns are often unique for SOA.
Input	Solution requirements Solution realization plan
Activities	Model the business processes including business functionality Model the user interfaces Model the business rules Identify service needs
Output	Service needs Solution model Solution modeling metrics

CHECKPOINT	Approve Service Model
Input	Service needs Solution model Solution modeling metrics
Activities	Ensure compliance to guidelines
Output	Approval of service model

CHECKPOINT	Approve Service Model
Used Guidelines	BPM Guidelines Portal Guidelines Security Guidelines Service Discovery Guidelines Solution Modeling Guidelines Business Rules Guidelines

PROCESS	Service Re-use Planning and Re-use Exceptions
Goal	The process of evaluating existing services identified from the service identification and services found in a more thorough service discovery process.
Input	SOA solution model SOA solution requirements Service characteristics
Activities	Identify services to be re-used Identify existing services possible to re-use after some changes
Output	Service usage plan Service change proposal

CHECKPOINT	Approve Service Usage Plan
Input	Service usage plan Service change proposal
Activities	Ensure service re-use
Output	Approval of service usage plan
Used Guidelines	Security Guidelines Service Change Management Guidelines Service Portfolio Planning Guidelines Service Policy Guidelines

PROCESS	Service Entitlement/Usage
Goal	The processes for requesting access to a service and determining who can use a service, how often they can use it, and what qualities of service can be expected by consumers of the service.
Input	Solution requirements Service usage plan Service characteristics Service performance feedback Service roadmap Service funding model

PROCESS	Service Entitlement/Usage
Activities	Negotiate the contracts for the services used Identify changes to existing services to fulfill business needs and define new contracts for them
Output	Service contract Service policy Service change proposal

CHECKPOINT	Approve Service Usage
Input	Service contract Service policy Service change proposal
Activities	Ensure contracts exist for all services Ensure service change proposals are appropriate Ensure compliance to guidelines
Output	Approval of service usage
Used Guidelines	Security Guidelines Service Contract Guidelines Service Policy Guidelines Service Discovery Guidelines Service Change Management Guidelines Service Portfolio Planning Guidelines

PROCESS	Solution Assembly, Implementation, or Acquisition
Goal	Solution assembly allows developers to create new solutions that follow predefined rules and processes based upon defined architectural standards. Important changes due to SOA: • New tools and techniques to implement and assemble SOA solutions • Acquisitions may require new tools and testing methods
Input	Solution model Solution techniques (from reference architecture) Solution architecture Services from the Service Lifecycle
Activities	Implement workflows using BPM Implement automatic workflows using orchestration Implement user interfaces Implement business rules
Output	SOA solution components and services Solution implementation metrics

CHECKPOINT	Approve Solution Implementation
Input	SOA solution components and services Solution implementation metrics
Activities	Ensure compliance to guidelines
Output	Approval of solution implementation
Used Guidelines	BPM Guidelines Portal Guidelines Security Guidelines

PROCESS	Solution Testing
Goal	The testing of the solution needs to include verification of solution adherence to service contracts.
Input	Solution requirements Solution design Solution Solution test cases
Activities	Development of solution test plans including functional, performance, scalability, and security testing and fulfillment of guidelines Plan for testing of SOA capabilities (agility) Execution of solution test plans Documentation of solution test results
Output	Solution test plan Solution test results Solution testing metrics

CHECKPOINT	Approve Solution Testing
Input	Solution test plan Solution test results Solution testing metrics
Activities	Ensure compliance to guidelines
Output	Approval of solution testing
Used Guidelines	Solution Testing Guidelines Solution Development Guidelines

PROCESS	Solution Deployment
Goal	The Solution Deployment process manages the registration and configuration of the solution and release into production. Important changes due to SOA are: • New and updated service contracts and service policies are deployed with the solution. • New ways of deploying processes are included in the solution.
Input	SOA solution components and services Solution deployment architecture (staging environments) Used services contracts and policies New and updated services
Activities	Deploy solution into different staging environments (e.g., testing, pre-production, production) Manage deployment information
Output	Deployed solution information Version of solution in different staging environments

CHECKPOINT	Approve Solution Deployment
Input	Deployed solution information Version of solution in different staging environments
Activities	Ensure that the solution is deployed correctly Ensure that the tracking of the solution in the staging environments is up-to-date Ensure that necessary production environment testing has been performed
Output	Approval of the solution deployment
Used Guidelines	Solution Deployment Guidelines BPM Guidelines (deployment) Portal Guidelines (deployment) ESB Guidelines (deployment) Service Guidelines (deployment) Security Guidelines (deployment)

PROCESS	Solution Management and Monitoring
Goal	This process is used to monitor workload and system events that could cause solution outages/problems as well as security incidents.
Input	Service policy Service contract Solution deployment results Solution requirements (non-functional metrics)
Activities	Monitor solution adherence to solution Quality of Service (QoS) attributes Manage solution execution to ensure correct capacity Create solution audit reports Create solution performance reports