

BS ISO/IEC 17998:2012



BSI Standards Publication

Information technology — SOA Governance Framework

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™

Full document details: BS ISO/IEC 17998:2012



National foreword

This British Standard is the UK implementation of ISO/IEC 17998:2012.

The UK participation in its preparation was entrusted to Technical Committee ICT/-/1, Information systems co-ordination.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012

Published by BSI Standards Limited 2012

ISBN 978 0 580 77830 8

ICS 35.080; 35.100.05

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2012.

Amendments issued since publication

Date	Text affected
------	---------------

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)

AVA Documents
Document Sharing Hub
© ISO/IEC 2012



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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



Copyright © 2009, The Open Group

The Open Group hereby authorizes you to copy this document for non-commercial use within your organization only. In consideration of this authorization, you agree that any copy of this document which you make shall retain all copyright and other proprietary notices contained herein.

This document may contain other proprietary notices and copyright information.

Nothing contained herein shall be construed as conferring by implication, estoppel, or otherwise any license or right under any patent or trademark of The Open Group or any third party. Except as expressly provided above, nothing contained herein shall be construed as conferring any license or right under any copyright of The Open Group.

Note that any product, process, or technology in this document may be the subject of other intellectual property rights reserved by The Open Group, and may not be licensed hereunder.

This document is provided "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Any publication of The Open Group may include technical inaccuracies or typographical errors. Changes may be periodically made to these publications; these changes will be incorporated in new editions of these publications. The Open Group may make improvements and/or changes in the products and/or the programs described in these publications at any time without notice.

Should any viewer of this document respond with information including feedback data, such as questions, comments, suggestions, or the like regarding the content of this document, such information shall be deemed to be non-confidential and The Open Group shall have no obligation of any kind with respect to such information and shall be free to reproduce, use, disclose and distribute the information to others without limitation. Further, The Open Group shall be free to use any ideas, concepts, know-how, or techniques contained in such information for any purpose whatsoever including but not limited to developing, manufacturing, and marketing products incorporating such information.

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: ogspeccs@opengroup.org

Contents

1	Introduction	1
1.1	Objective	1
1.2	Overview	1
1.3	Conformance	2
1.4	Terminology	3
1.5	Future Directions	4
2	Background	6
2.1	SOA Challenges and Goals	6
2.2	SOA Governance	7
3	SOA Governance	9
3.1	SOA Governance Definition	9
3.2	SOA Governance Scope	10
3.3	SOA Governance Framework	10
3.3.1	SOA Governance Reference Model (SGRM)	11
3.3.2	SOA Governance Vitality Method (SGVM)	11
4	SOA Governance Reference Model (SGRM)	12
4.1	SOA Governance Guiding Principles	12
4.2	SOA Governing Processes	15
4.2.1	Compliance	15
4.2.2	Dispensation	16
4.2.3	Communication	16
4.3	Governed SOA Processes	18
4.3.1	Service Portfolio Management	19
4.3.2	Service Lifecycle Management	20
4.3.3	Solution Portfolio Management	21
4.3.4	SOA Solution Lifecycle	22
4.4	SOA Governance Roles and Responsibilities	24
4.5	SOA Governance Process Artifacts	27
4.6	SOA Governance Technology	29
5	SOA Governance Vitality Method (SGVM)	30
5.1	Plan Phase	31
5.1.1	Understand Current Governance Structures	31
5.1.2	Assess SOA Maturity	32
5.1.3	Develop SOA Governance Vision and Strategy	33
5.1.4	Develop SOA Governance Scope	33
5.1.5	Develop SOA Governance Principles	33
5.1.6	Develop SOA Governance Roadmap	34

5.2	Define Phase	34
5.2.1	Define Governed SOA Processes	35
5.2.2	Define Governing SOA Processes	36
5.2.3	Collect SOA Guidelines and Standards	36
5.2.4	Define SOA Governance Organization, Roles, and Responsibilities	36
5.2.5	Define SOA Governance Information Artifacts	36
5.2.6	Define SOA Governance Environment	37
5.2.7	Create Transition Plans	37
5.3	Implement Phase	38
5.3.1	SOA Governance Organization Transition Plan Implementation	39
5.3.2	SOA Governance Process Transition Plan Implementation	40
5.3.3	SOA Governance Technology Transition Plan Implementation	40
5.4	Monitor Phase	41
5.4.1	Monitor and Evaluate SOA Governed Processes	42
5.4.2	Monitor and Evaluate SOA Governing Processes	42
5.4.3	Monitor External Changes	42
5.4.4	Monitor and Evaluate SOA Guidelines Development	43
5.5	SGVM Use of SOA Governance Artifacts	43
A	SOA Governance Process Activities	45
A.1	SOA Governing Processes	45
A.2	SOA Governed Processes	48
B	SOA Governance Process Information Entities	72
B.1	SOA Governing Process Artifacts	73
B.2	SOA Governed Process Artifacts	73
B.3	SGVM Artifacts	79
C	SOA Governance Metrics Example	81
D	Relationships with Other SOA Standards	83

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'd 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

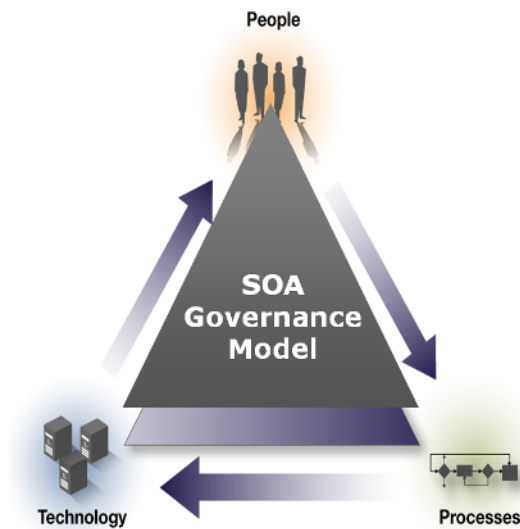


Figure 1: SOA Governance Aspects

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.

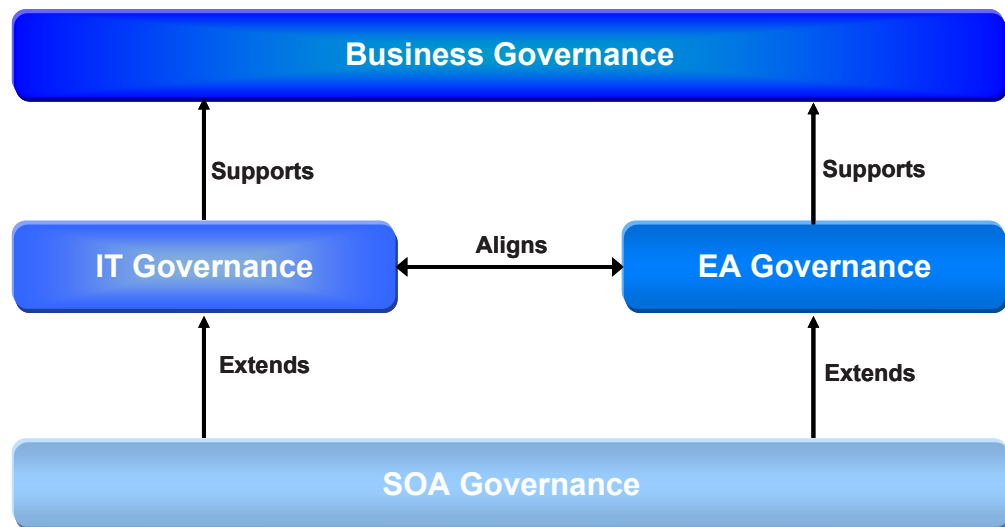


Figure 2: SOA Governance Relationships

- **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'd 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.

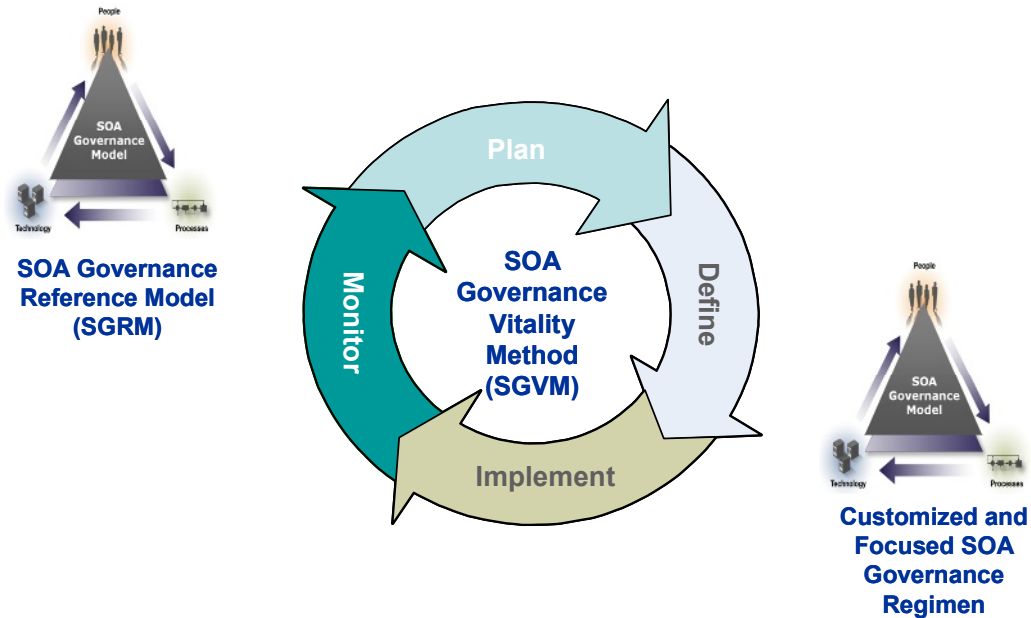


Figure 3: SOA Governance Framework

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 <i>ad hoc</i> 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 decrease 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.

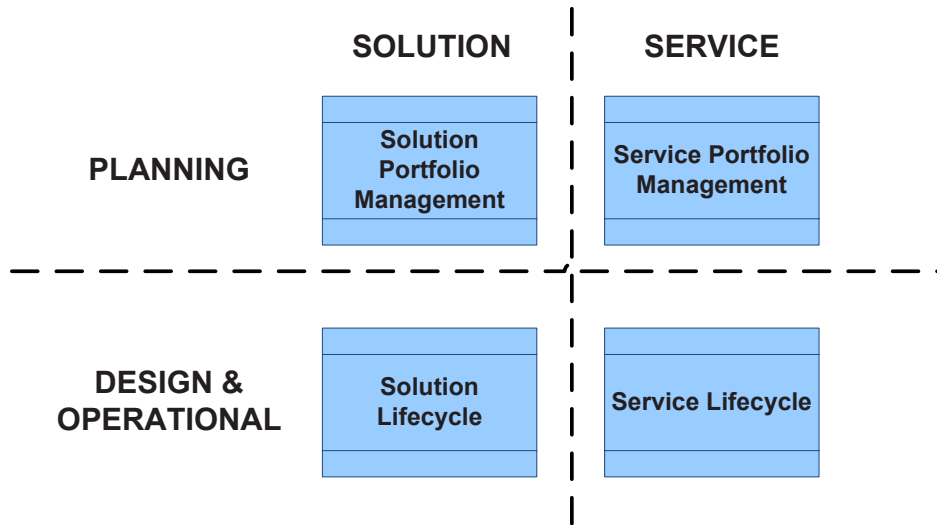


Figure 4: Governed SOA Processes

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 reusable 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.

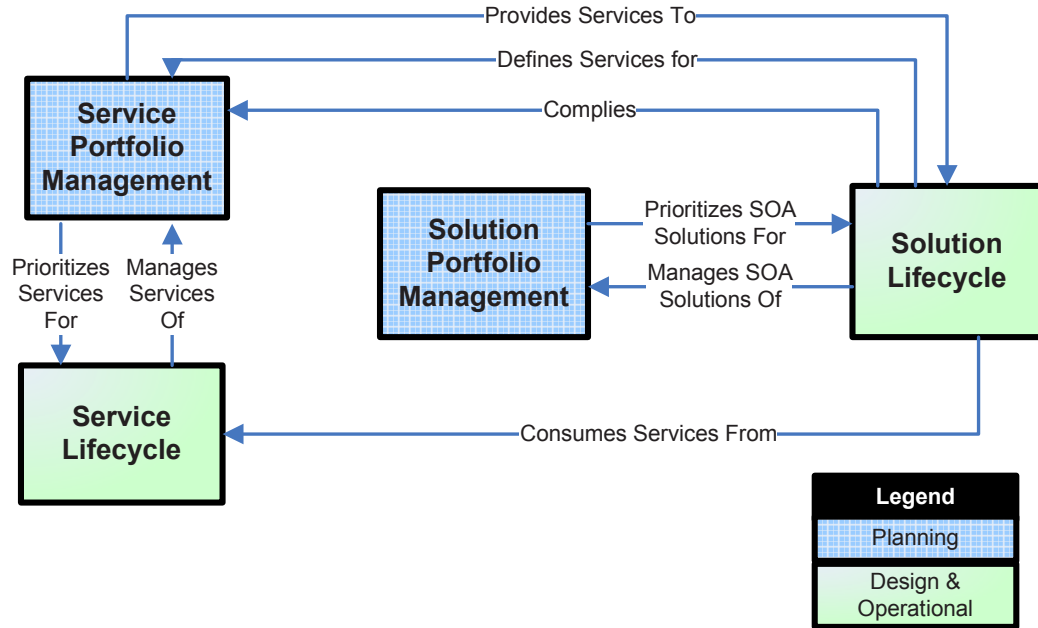


Figure 5: Governed SOA Process Relationships

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.