

# The SOA Magazine

## Feature Article



### SOA Governance - How Best To Embrace it, Part 1: Introduction to Enterprise, IT and SOA governance

by Farzin Yashar

Published: November 6, 2009 (SOA Magazine Issue XXXIII: October 2009)

[Download PDF](#)

[Digg This](#) • [De.licio.us](#) • [Slashdot](#) • [Technorati](#) • [StumbleUpon](#) • [Google Bookmark](#)

*Abstract: With immense projected growth, the Government must modernize its IT systems. Air traffic will double or even triple in the next twenty years, the number of retirees will double throughout the States, infrastructure will boom, the population will skyrocket, and under such pressures, the legacy systems will surely collapse, and if no action is taken, problems will abound.*

*Some government agencies have considered Service Oriented Architecture (SOA) as the most effective means to address this dire issue. Moving to SOA, however, entails substantial challenges. To this end, one of the government agencies requested IBM to collaborate with other partners of the agency and produce a whitepaper that addresses these challenges. This article expounds such information beyond this agency to industries across the board.*

### Introduction

This paper integrates both industry agnostic recommendations and best practices developed in a white paper written to aid a government agency through its SOA journey. All sections with tedious specifics and customer references have been removed in order to focus on the most fundamentally important aspects of the original paper.

This paper will be presented in three parts:

- Part 1 - Introduces governance and discusses Enterprise, IT and SOA governance
- Part 2 - Discusses the governance lifecycle and how to organize for SOA and SOA governance
- Part 3 - Presents governance maturity, tooling, vitality and success patterns

### The Need for a Governing Process Providing the Required Checks and Balances to Assure Success

This white paper is not intended to address the broad topics of either enterprise governance or IT governance but is instead confined to consideration of SOA governance. SOA Governance may be viewed as an augmentation of IT governance since it is primarily focused on business services strategy and on the lifecycle management of services (single services as well as the network of services) to ensure their business value to the enterprise.

Moving to SOA represents a substantial challenge for organizations. Besides introducing new technologies and responsibilities, SOA requires a change from application-based thinking to an enterprise-wide perspective intended to control how workflows are accomplished and how services and a portfolio of services are developed, deployed and managed throughout their lifecycle to accomplish enterprise business objectives.

SOA governance certainly should include elements of enforcement, control and policing, but it needs to be much more. Since a primary SOA objective is the identification, development, deployment and lifecycle management of services (and portfolios of services), SOA governance cannot be rigid or autocratic but must become a collaborative effort involving centralized IT management with the active participation of internal (and external, if required) communities of interest (COIs).

The importance of involving Communities of Interest in the SOA Governance process cannot be overestimated. Many of the benefits of SOA are based on the sharing of services, as well as the sharing of information, best practices architectures and business processes and objectives. For this reason, strong consideration should be given to the early adoption of a federated SOA Governance model. This should include the early establishment of a Core SOA team, or SOA Center of Excellence (COE), whose role is one of collaboration with the Program Office to share needs, services, and resources for the good of the enterprise.

Collaboration between semi-autonomous, interconnected business units is often difficult. To overcome this natural institutional friction, SOA Governance can begin informally and on even an ad hoc basis, but it should naturally progress over time to more formalized oversight with standards, best practices, and enterprise alignment as its ultimate goal. A key element in making this collaborative process work is, of course, executive level buy-in. Without the commitment of both leadership and enterprise communities of interest, the potential benefits of SOA can be easily lost.

## Governance Introduction

Good governance is all about transparency - ensuring that everyone involved in an activity clearly understands their individual roles and responsibilities, what expectations the other team members have of them, and how they personally contribute to the overall goals. In this section we examine the importance of governance and we define SOA governance and its relationship with Enterprise as well as IT Governance.

### *Why Governance*

One definition of governance is "the set of rules, practices, roles, responsibilities and agreements - whether formal or informal - that control how we work". In another words, for each activity we need to define:

- What needs to be done
- How it should be done
- Who should do it
- How it should be measured

As obvious, trivial and self-evident the above may be, in many cases these precepts are not being followed. They are either eliminated or compromised in the name of SPEED, ("Just do it").

The key phrase in the above definition is "control how we work". This level of control can be at a level anywhere from very light and unobtrusive control (guidance) to a very tight and bureaucratic level of control (policing). Neither does the work of governance mean management, per se. Governance determines who has the authority to make decisions. Management is the process of making and implementing the decisions.

If we think about the What, How, Who, and measurement of the standard IT project, we see that these functional attributes are not always well defined either. The business reasons for having an Information Technology (IT) function has come about to bring agility to what the business does. But IT implementation has always faced the dilemma of not being a fast and agile process itself. Therefore, IT projects are very much prone to temptations of cutting corners and eliminating and bypassing vital steps. Many times, the "What" of an IT Project, in the form of functional and non-functional requirements, are not complete and it is left to the imagination of the IT individual(s)/department on what should be created. The "How" is normally influenced by individual styles and preferences. The "Who" could end up with whoever is available. Measurement of the project results will usually not happen as the development team moves onto the next project.

So, while the state of IT Governance leaves something to be desired, we are now faced with the challenge of

migrating to a services approach with SOA. Moving to SOA represents a considerable challenge for any organization, especially since: SOA introduces new technologies, roles and responsibilities; SOA requires new patterns of thought - taking an enterprise-wide viewpoint, rather than focusing on any one department, or specific Line of Business (LOB) area.

The potential benefits of SOA may not be achieved without the enforcement rigor around development, deployment and operational management of services across the enterprise. Lessons learned from past attempts at SOA indicate that the mere proliferation of services in the absence of governance policies will not realize a Service Oriented Architecture. Lack of SOA governance impacts any organization's ability to realize the potential benefits of service orientation, by allowing inconsistencies, gaps and overlaps in the software development process that makes reuse and business agility difficult, if not impossible. Thus, without governance, the SOA journey is likely to fail.

Implementing SOA successfully in any organization will create new and additional challenges to people, process and technology that must be addressed through sound and effective governance. Without such governance, business agility is impossible, service ownership will remain locked within silos, portfolio management will remain balkanized and ineffective, and security will be in islands instead of achieving a more holistic, enterprise-wide view.

### *Enterprise, IT and SOA Governance*

SOA governance extends, or augments IT governance further aligning IT and business by governing the lifecycle of business services as manifested in IT systems. Deploying SOA should serve as a catalyst for an organization to start thinking about improved corporate and IT governance in general, as well as how to best implement SOA governance practices specifically. Adoption of SOA raises new issues in IT decision rights, measurement and control.

SOA governance augments IT governance as enterprises focus further on Service-Oriented adoption. SOA provides a distinctive enterprise-level approach for designing and delivering cross functional initiatives, closely involving both business and IT in the collective pursuit of the enterprise's strategy and goals. This form of SOA governance introduces the use of business policies, both enterprise-level and department level policy invocation, which provides the discipline referenced above.

Establishing SOA Governance should also be seen as providing another opportunity to bridge any gaps between enterprise and IT governance. SOA governance would benefit from existing IT and Enterprise governance. However, lack of existing IT and Enterprise governance, or "operationalizing" the IT & Enterprise governance practices should not stop enterprises from establishing SOA governance. In many cases, the need for SOA governance has encouraged enterprises to revisit and reinvigorate their IT and Enterprise governance.

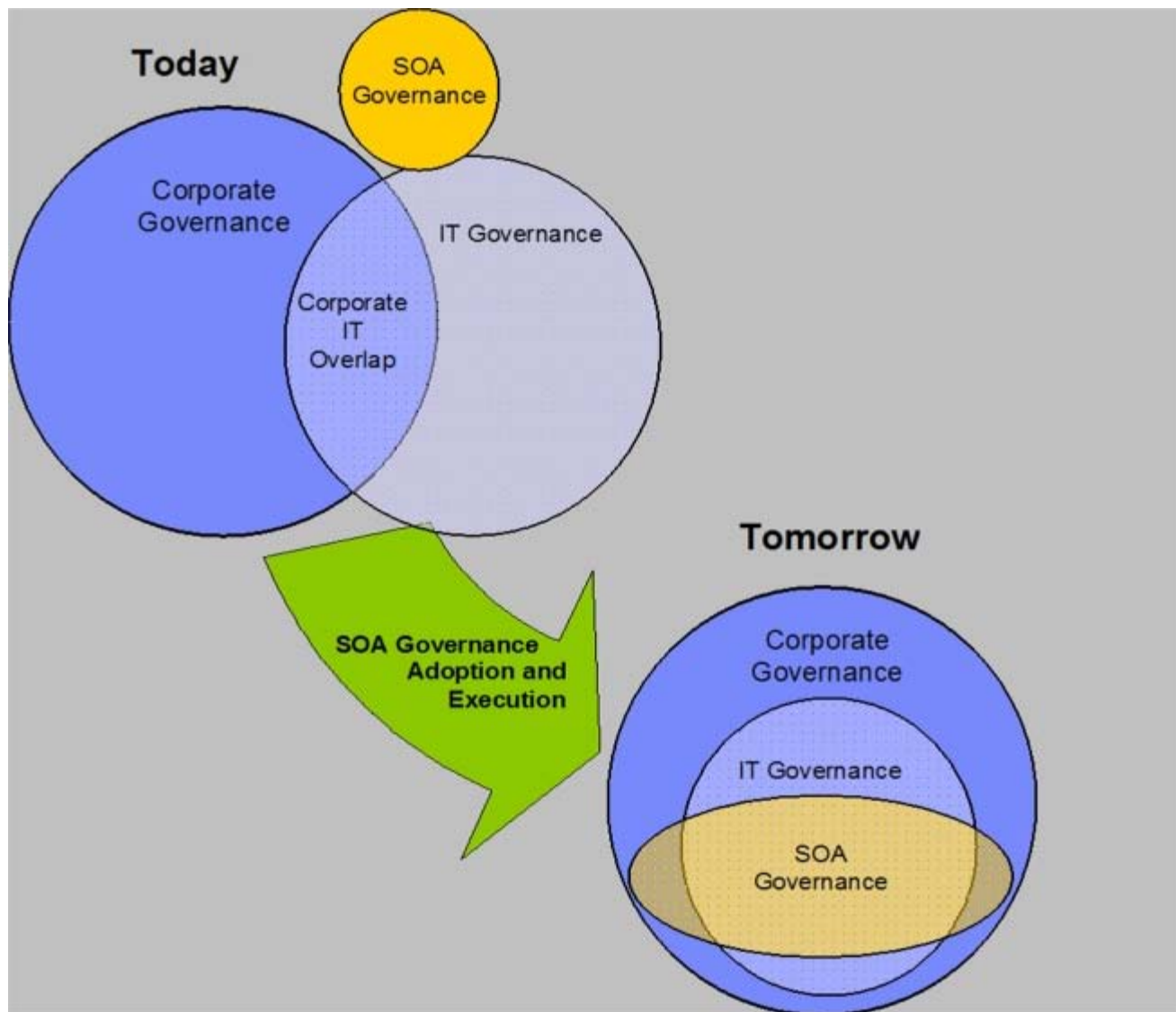


Figure 1: Enterprise, IT and SOA Governance

Conceptually, the way that the relationship between Enterprise, IT, and SOA governance changes over time is shown in figure 1 above.

Initially, SOA governance has limited scope and concerns itself mainly with a fairly limited area where IT and Business interests overlap.

As the organization increases its level of SOA maturity, the scope of SOA governance will expand significantly. The business and IT communities should gradually increase their degree of overlap until eventually an expanded SOA governance role merges with IT governance, and IT governance itself is subsumed into an overall corporate approach to governance.

Generally speaking, enterprise level governance establishes the rules and the manner in which an enterprise conducts its business. Enterprise governance includes establishing compliance goals, its strategy within the marketplace, according to its principles of doing business. IT governance represents a significant portion of enterprise governance, due to the horizontal nature of IT and the broad reliance on IT around the world. Since almost everyone in an enterprise uses IT assets to complete their responsibilities, and all persistent information is stored in IT systems, the impact of effective IT governance is highly visible.

SOA Governance typically defines additional nuances and changes to IT Governance to ensure that the concepts and principles for Service Orientation are managed appropriately and that the organization is able to deliver on the stated business goals for SOA. In addition, SOA Governance drives organizational change for better partnering between business and IT in order to achieve a higher degree of business value by optimizing return on investments and improving business agility. This is done by associating business requirements with business services instantiation. This association, if conducted rigorously, results in better

risk management and predictability in all phases of IT system implementation.

Since SOA is a distributed approach to architecture that may span multiple lines of business domains (internal and external) as well as IT domains there is a greater need for effective SOA governance. In addition SOA Governance provides a framework for the reuse and sharing of services, a key value derived from leveraging SOA.

#### *IT Governance*

IT Governance can be defined as:

- Establishing and implementing decision making rights associated with IT.
- Establishing mechanisms and policies used to control and measure the way IT decisions are made and carried out.

#### *Architecture Governance*

Architectures are controlled at an enterprise-wide level by practicing architecture governance. Enterprise Architecture (EA) plays a significant role in governance as the EA discipline defines and maintains the architecture models, governance and transition initiatives needed to effectively coordinate semi-autonomous groups towards common business and/or IT goals.

#### *SOA Governance*

SOA governance is an augmentation of IT governance focused on:

- Business services strategy
- Lifecycle of services to ensure the business value of SOA
- Enablement of the services approach
- Aligning business and IT governance towards the goal of achieving business objectives.

SOA Governance is frequently a catalyst for improving overall IT governance, particularly in large organizations with a reliance on legacy IT infrastructure.

#### *Mechanics of the Governance Model*

SOA governance ensures successful Business and IT alignment. It enforces agreed upon Policies and Standards. These policies and standards guide the governed processes that are managed and monitored by governing processes, standards and metrics; and implemented by procedures.

Figure 2 points out Compliance, Communication, Vitality and Exceptions/Appeals. These are the most important mechanisms in governance. We address each of them separately.

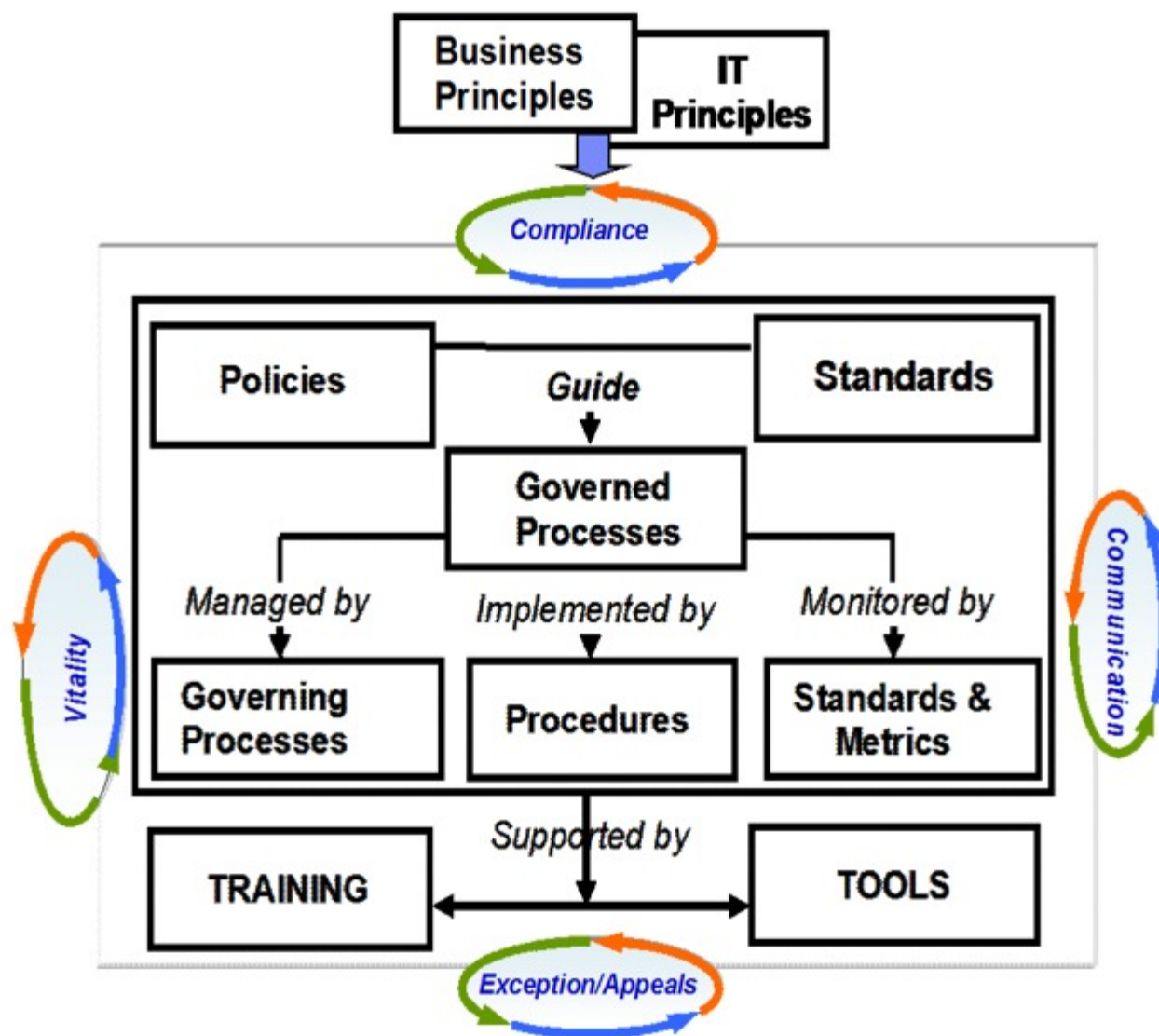


Figure 2: Mechanics of Governance

### Compliance

Governed processes are guided by policies and standards. Defining policies and identification of standards have a significant importance for governance best practices. However, policies and standards without compliance marginalizes their value. To this end, concepts such as control points, Policy Decision Points and Policy Enforcement points are essential in governance. Next section is dedicated to policies and policy management for this purpose.

### Communications

Clear communication is essential to governance. Communication is needed within the enterprise as well as with partners, providers/suppliers and clients. Communication is about delivering the right message, to the right people, at the right time. It is a key enabler to moving people through the various stages of any process requiring awareness, understanding, commitment and adoption.

Leveraging open standards such as XML based messaging and using the Web Services communication framework has the potential to transform how business class messaging is accomplished through new technology use.

### Exceptions and Appeals

Governance should not be a set of static processes without any flexibility. As part of the governance life cycle, governance processes may be appealed, or waived as exceptions require. In managing and monitoring policies and standards compliance, an appeal, or waiver process needs to be built for cases

where achieving compliance is either temporarily or permanently impossible. Appeals, or waivers are a very sensitive topic, because on the one hand it has to be flexible enough to accommodate these exceptions, while on the other be stringent enough prevent unnecessary exceptions that may set uncontrollable precedence.

### *Vitality*

As time goes by things will change and governance processes must adapt. This is called vitality.

### Governance Policies and Policy Management

Business process management (BPM) drives the creation of services through the identification, definition and creation of service operations. Compliance with the many rules and laws becomes a key driver behind governance. These service operations have design time and run time business processes that should be mapped, and benchmarked with key performance indicators established to enable service level agreements, based on Quality of Service (QoS) parameters.

Policy management provides a mechanism to allocate IT resources according to defined policies, or rules established by the enterprise. Policies dictate the data quality, integrity and retention requirements. Policies allow rules to take the form of if, then conditional statements, where actions are executed to account for a given condition. The application programs must be empowered to establish their formal program policies into procedures which are implemented into systems, tools for execution.

Policies are built into systems establishing policy decision points (PDPs), where events are defined and decisions made. The PDP's are configured to support various conditions and react accordingly. PDP's are synchronized with policy enforcement points (PEPs), which monitor events, and execute the policies within the context of the PDP. The Internet Engineering Task Force (IETF) has defined standards for localizing policy decision points, enabling a decentralized enterprise support structure, while integrating into a higher level policy management system.

Policy enforcement points exist within the network and IT infrastructure used for monitoring events. A myriad of tools are required to provide the proper IT governance and access control at a macro level. Each application program must support their own infrastructure; however, the key to a service-oriented architecture is the agility of data transport to new communities of interest. Tools for web services management, including service registries, repositories and metadata catalogs, asset tracking and fault/performance monitoring are required to enable the policy enforcement function. The IT Infrastructure Library (ITIL) standards define a configuration management database (CMDB) which hosts these data elements that require tracking. The IT tools are required to collect and report on the many data transactions, tracked to individual users, along with key performance indicators, and then report them accurately to the appropriate Application Program.

Here are some policy examples:

- Policies might start at the business level:
  - Projects must comply with Internal Architecture guidelines
  - Security and regulatory compliance policy reviews are mandatory for all IT projects
- Policies could represent more specific regulatory compliance issues:
  - Patient personal identifiable information must be communicated and stored securely. (HIPPA)
  - All financial transactions must provide traceability and tamper proof mechanisms for mandatory audit records. (Sarbanes Oxley)
- Project outsourcing initiative might represent its policy as:
  - Outsourced company must create same service lifecycle deliverables as are created in house.
- Higher level policies will often need to be translated to technical policies that can be effectively enforced by active policy enforcement tools.
- Information security examples:

- Messages must contain an authorization token
  - Password element lengths must be at least 6 characters long and contain both numbers and letters
  - Every operation message must be uniquely identified and digitally signed
- There are also design related technical policies that are needed to ensure interoperability and reuse:
    - Do not use RPC encoded style web services
    - Do not use Solicit-Response style of web service operations
    - Do not use XML 'anyAttribute' wildcards
  - Each organization, as part of the strategy and planning process for SOA, should think about and create its set of standards and policies for its SOA program and the SOA service development lifecycle. Specific policy service examples follow.
  - The Service Specification should contain:
    - Descriptions of what function is performed by each service operation
    - Input/output message formats, and sample data for each service operation
    - A definition of the corresponding task in the Component Business Model (CBM)
  - The Service Specification should NOT contain:
    - Any information on how the service will be implemented (provided the service contract is maintained, the provider may change the implementation of the service at any time, e.g. when retiring an obsolete IT system)
    - Any reference to a sequence or order in which operations should be executed. Each operation call should be considered as a discrete task, and sequences of tasks should be defined as business processes/automated business processes) in separate documentation

## Governance Standards

A *standard* is a rule or requirement that controls the service lifecycle. The governed service must adhere to the standard. Standards change very infrequently and a violation is not allowed or requires an explicit exception. In case an organization decides to deploy web services, the following table could be example of standards they may designate to follow:

Standard	Recommended	Alternatives Proposed	
Orchestration	<b>BPEL</b>	WS-Choreography	WS-CDL
Management		WS-DistributedManagement WS-Provisioning	WS-Management
Security	<b>WS-Security</b>	WS-Trust WS-Federation	WS-SecureConversation WS-SecurityPolicy
Transaction	<b>WS-Transaction</b> <b>WS-Coordination</b>	WS-CompositeApplicationFramework (WS-CAF)	WS-Context (WS-Ctx) WS-CoordinationFramework (WS-CF)
Reliability	<b>WS-ReliableMessaging</b>	WS-Reliability	
Description	<b>WSDL</b> <b>UDDI</b>	WS-Inspection Disco WS-Discovery	WS-PolicyFramework WS-MetaDataExchange
Messaging	<b>XML</b> <b>SOAP</b>	WS-Addressing WS-Notification WS-ResourceFramework	WS-Eventing WS-Policy SOAP with Attachment
Transport	<b>HTTP</b> <b>JMS</b> <b>RMI-IIOP</b>	TCP UDP	Jabber SMTP
Interoperability	<b>WS-1 Basic Profile</b>		

*Table 1: Examples of Standards for Web Services*

SOA borrows concepts such as Policy, Service Level Agreement and Quality of service from other aspects of Information Technology such as network management and managing IT infrastructure. Since at this time there is no SOA policy management and policy related standards in place, reference to standards defined by IETF (Internet Engineering Task Force) and or ITIL (Information Technology Infrastructure Library) is highly recommended.

Conclusion

In part one we learned about governance in general and discussed Enterprise, IT and SOA governance and how they are related. In part 2, we walk through governance lifecycle and how best we should organize for SOA and SOA governance.

References

- [REF-1] "The Next Revolution in Productivity", Harvard Business Review Article, 1 June 2008, Ric Merrifield, Jack Calhoun, Dennis Stevens, <http://harvardbusinessonline.hbsp.harvard.edu/relay.jhtml?name=itemdetail&id=R0806D>
- [REF-2] IBM EA Academy Study Team, Orlando Workshop, 12th-13th March 2004
- [REF-3] See COBIT Framework, Page 19: <http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172>.
- [REF-4] SOA and the Emergence of Business Technology: How Business Services are Changing the IT Landscape. Farzin Yashar & Robert Laird. <http://www.soamag.com/I4/0207-3.asp>.
- [REF-5] Several writings and presentations from Clive Gee, Phd.

*Acknowledgements: I would like to thank the following individuals who reviewed and contributed to the original paper: Les Robinson (Boeing), Jay Pollack (Computer Sciences Corp), Bob Riley (Harris Corp), David Almeida (Harris Corp), Mike Moomaw (IBM), Robert Laird (IBM), John Falkl (IBM), Al Secen (Lockheed-Martin), Chris Francis (L3 Communications), Peter Bostrom (Oracle), Kathy Kearns (SITA) and Mansour Rezaei-Mazinani (SITA). My special thanks go to Mr. Robert Laird who generously volunteered his time and expertise providing me with his input on every section of this paper.*

THE PRENTICE HALL SERVICE-ORIENTED COMPUTING SERIES FROM THOMAS ERL



