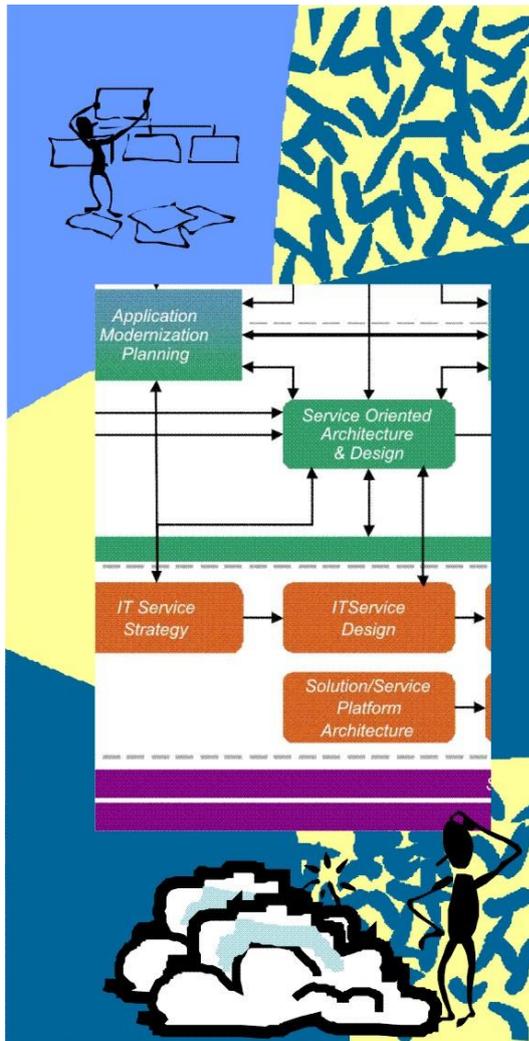# CBDIJournal

SOA Governance: Challenge or Opportunity

SOA Governance has taken on a renewed importance as organizations seek to scale up their early SOA experiences. Scarcely a week seems to go by without SOA governance popping up in a story on the newswires. Too often however the advice given is too vague with a lack of specific measures that can be taken by organizations that need to achieve much better accountability in challenging economic times, or is focused on the narrow view of governance that is supported by a vendor's products. Our experiences in the field show that despite the challenges there is now an opportunity to get to grips with overall IT governance, of which SOA is one, albeit key, part. This article distills the main lessons learnt in the form of a SOA governance framework with practical guidelines for progression in real world contexts.

By Paul Allen and Lawrence Wilkes

Independent Guidance *for* Service Architecture and Engineering

SOA Governance: Challenge or Opportunity

SOA Governance has taken on a renewed importance as organizations seek to scale up their early SOA experiences. Scarcely a week seems to go by without SOA governance popping up in a story on the newswires. Too often however the advice given is too vague with a lack of specific measures that can be taken by organizations that need to achieve much better accountability in challenging economic times, or is focused on the narrow view of governance that is supported by a vendor's products. Our experiences in the field show that despite the challenges there is now an opportunity to get to grips with overall IT governance, of which SOA is one, albeit key, part. This article distills the main lessons learnt in the form of a SOA governance framework with practical guidelines for progression in real world contexts.

By Paul Allen and Lawrence Wilkes

Introduction

Background

At CBDI we have always advocated that governance needs to be rooted in clear policy definition and in fact devoted an article to this in June 2007[1]. Since that time we have been busy assisting organizations improve SOA governance approaches based on an underlying foundation of clear policy definition. One thing that has emerged vividly from this work is that organizations must move forward at their own pace and in a way that is realistic in terms of their current SOA adoption level. Moreover the approach taken to SOA governance must be in tune with the overall governance requirements and political climate. We have therefore distilled these experiences into an SOA Governance Framework – embracing policy, process, infrastructure and capability maturity – that can be tailored to each organization's specific needs. At the same time we are finding increasingly that SOA governance represents an opportunity to improve overall governance capabilities, which are all too often well short of the bar. Indeed successful SOA governance has to be seen as one component in organizational change management.

SOA Governance Defined

It is now clear that SOA provides huge potential for agility, both in response to technology and business change, and in terms of initiating change for organizational advantage. The problem is however a price tag, which includes difficult governance issues. For example:

- if services are to be widely reused then this requires profound and difficult issues in ownership, funding and project management.

- If services are widely reused this requires a significant increase in complexity of service specification - how do we make sure services can be specified clearly and consistently in a manner that satisfies multiple consumers with possibly varying requirements, timescales and change cycle times?

- And in today's offshore, outsourced world, we need governance over the choice of service provider and critically the delegation of architecture, design and test.

SOA governance is essentially a response to these problems that we define thus:

The part of IT governance that refers to the organizational structures, policies and processes that ensure that an organization's SOA efforts sustain and extend the organization's business and IT strategies, and achieve the desired outcomes .

SOA Governance in Context

An understanding of the idea of business governance is necessary to provide organizational context for SOA governance. Business governance refers to the leadership and organizational structures and processes that ensure that an organization's resources (including its services and supporting IT resources) sustain and extend the organization's business processes and goals. Moreover, SOA governance does not sit in isolation, but is part of IT governance which in turn should be an enabler of business governance.

The Full Spectrum of Governance

An important part of SOA governance concerns technology. Frequently we see vendors promoting a fairly narrow view of governance that just so happens to reflect the capabilities of their products, often focused on the operational activites.

However if an IT organization focuses solely on how its services are deployed and managed without paying sufficient attention to the business architecture drivers and the development processes and practices used to build services in support of that architecture, that organization is very likely to have a set of well-managed "service spaghetti," not a true SOA. Implementing a series of point-to-point services masquerading as an SOA will simply revive the integration nightmare of a few years ago with just another layer of technology.

The Need for a Framework

What is needed is an SOA governance framework that is aligned to the desired business and IT outcomes of the organization and that is compatible with your organization's current approaches to both IT and business governance. At the same time as we argue strongly in this article the SOA Governance Framework should not only be seen as a tool for dealing with these challenges. It is also provides an opportunity to put IT's house in order. Many organizations are at a very immature level of overall IT governance. SOA really forces you to address governance issues if it is to work effectively beyond the state of toy projects. This in turn has a positive effect on improving overall IT governance; see figure 1.
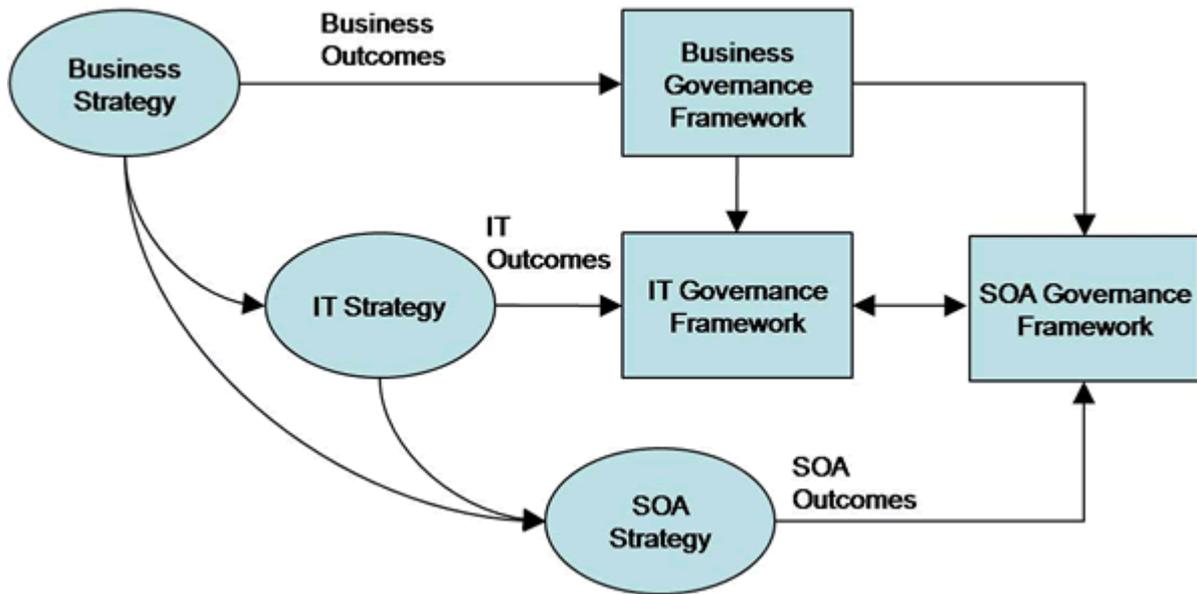
Figure 1: SOA Governance in Context

The CBDI-SAE SOA Governance Framework

It is important that SOA governance is approached in a balanced and complete fashion that addresses the What, How, Who and When aspects of the topic; see figure 2.
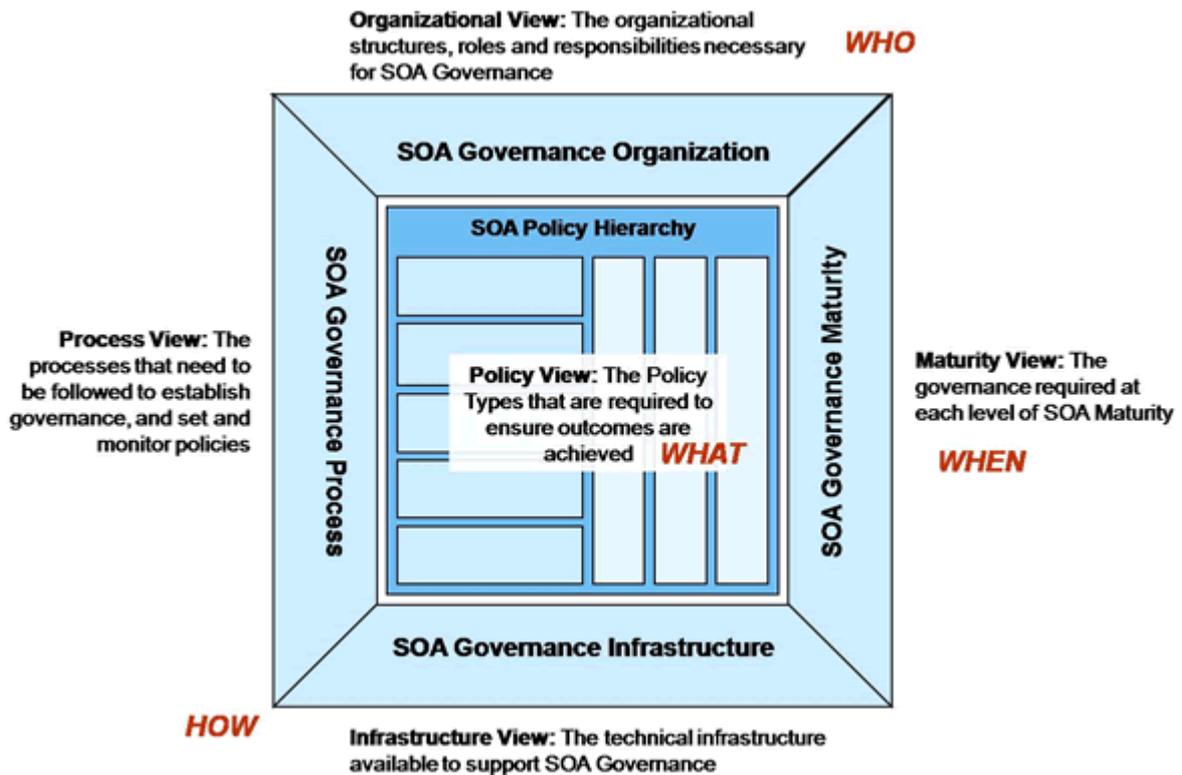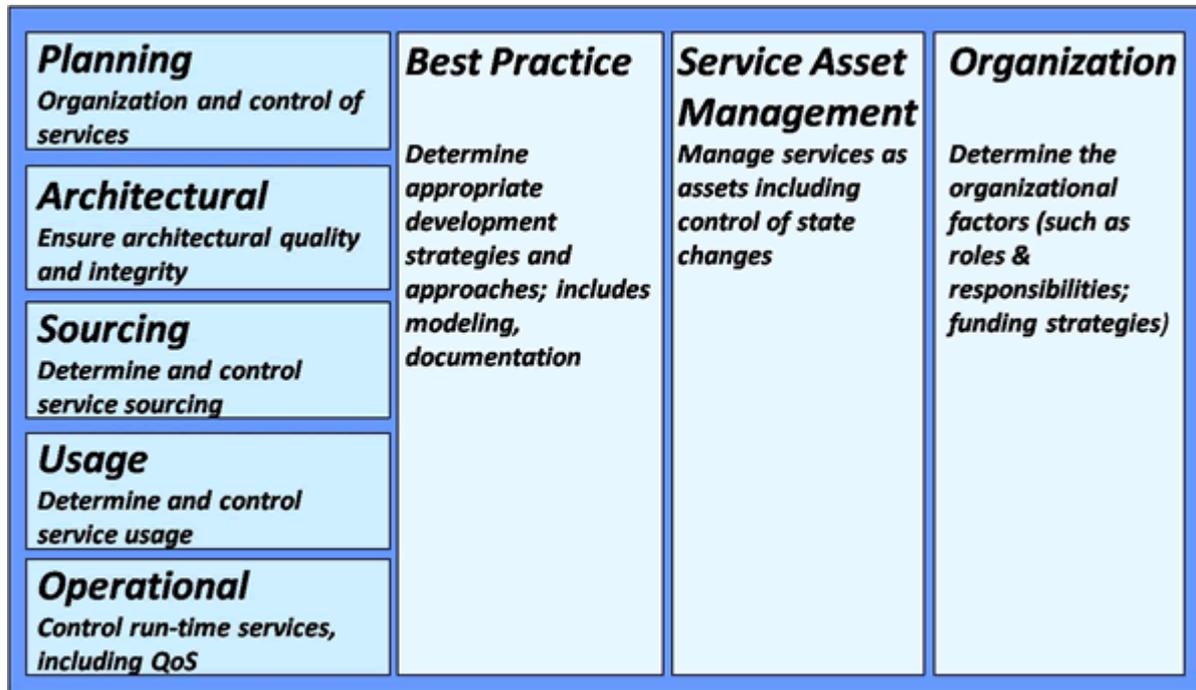

Figure 2: The CBDI-SAE SOA Governance Framework

Policy View

The Policy View is shown in figure 3. The policy categories on the left hand side of the figure represented by the horizontal rectangles correspond to the overall sequence of the service lifecycle from Planning through to Operations. The three vertical policy categories depict the ongoing activities that run right through this lifecycle.

Planning	*Best Practice*	*Service Asset Management*	*Organization*
Organization and control of services	*Determine appropriate development strategies and approaches; includes modeling, documentation*	*Manage services as assets including control of state changes*	*Determine the organizational factors (such as roles & responsibilities; funding strategies)*
Architectural			
Ensure architectural quality and integrity			
Sourcing			
Determine and control service sourcing			
Usage			
Determine and control service usage			
Operational			
Control run-time services, including QoS			

Figure 3: SOA Policy Categories

We have been busy cataloging and defining SOA policy types within the CBDI SAE Knowledgebase with respect to typically associated outcomes and risks; table 1 shows an analysis for a small portion of this hierarchy, which is too big to publish in its entirety in a report of this nature.

Business/IT Outcomes	Interpreted SOA Outcomes	SOA Risks
Easy exchange of well organized, accurate and timely information with customers.	Reuse and orchestration of services across different business processes in different channels and consumer contexts that a) resolve existing process and data quality, currency and completeness issues and b) improve customer satisfaction.	Well intentioned but misinformed integration of customer processes and data that support genuinely separate businesses within a single enterprise. Uncontrolled service usage that leads to data integrity issues or unsupportable scalability demands from consumers.
Data protection must not be compromised.	Common authentication and authorization services provide greater assurance of compliance with business security policies.	Conflict between SOA security and existing application level security. Trust boundaries necessary to avoid performance overhead of continual authorization and authentication reduce achievement of service autonomy.

Business/IT Outcomes	Interpreted SOA Outcomes	SOA Risks
ROI is ensured. Profitability is maximized.	Service architecture applied to business/IT projects delivers productivity, reduced cost, faster time to market.	Business value of SOA is properly articulated to include life cycle costs including future rationalization opportunities, shorter business change cycle time etc.
Widespread beneficial usage of services.	Solutions adopt and appropriately comply with an enterprise reference architecture and can demonstrate business value from architectural principles such as loose coupling, autonomy, composability and virtualization. Lowered dependence upon specific technologies and separation of concerns enables component based approach to business/IT – enabling ROI AND control from outsourcing, offshoring and commodity solution projects.	Narrow accessibility constrains usage reducing ROI.
Policy Strategy Area	**Policy Type**	**Leaf Node Policy Type**
Usage Permissions	Constituency	Constituency Type
		Approved Consumer Organization
		Approved Consumer Software
	Usage Security	Authentication
		Authorization
Usage Commercial Basis	**Usage Alignment**	
	Usage Pricing	
	Unit of Usage	
	SLA for Usage	

Table 1 – Policy Hierarchy Examples: Usage Policy Category

Process View

The process view focuses on the discipline of SOA Governance, its constituent process units, tasks and deliverables. Too often the complexity of SOA governance processes is exacerbated by mixing management with operational concerns. The discipline therefore separates these concerns, which are reflected in two different sets of process units.

The management level, which should be centrally controlled, ensures the SOA Governance Framework - in terms of policy, organization, process and infrastructure

requirements - is aligned to the requirements of the organization before embarking on detailed policy definition and enforcement.

The day to day activity of SOA governance is spread across different disciplines according to the type of policy being dealt with. For example policies of the architectural policy type are set up as part of the SOA Architecture and Design discipline, specifically in Service Portfolio Planning.

Organization View

The organization view sets out the roles necessary for SOA governance with guidelines on organizational structure. Some of these roles are specifically focused on governance matters; for example, the SOA Governance Board and the SOA Governance Lead. Others such as the SOA Review Board may have a "leaning" toward governance. And yet others, such as the SOA CoE, Enterprise Service Architect and Service Level Manager, may well be charged with significant governance responsibilities, but as part of a much wider brief.

Certain roles, such as the SOA CoE are group roles that may map to new organizational units or may be subsumed within existing units. In contrast, other roles such as the SOA Governance Lead are likely to be assigned to one (or more) individuals.

It is also important to define policy that states which roles are accountable for which SOA artifacts in terms of responsibility (R), authority (A), expertise (E) and work (W); RAEW analysis is used to assist here[2].

Infrastructure View

The infrastructure view sets out the infrastructure capabilities necessary for SOA governance. There is a wide variety of implementation types, both automated and manual, the purpose of which often extends beyond governance alone to areas such as SOA modeling and service execution. The rationale of the infrastructure view is to focus on the governance capabilities in terms of:

- Policy Management: how is policy defined and maintained, what level of support is available for assertion languages? For example, using a service catalog and repository with links to modeling tools using a standardized SOA meta model

- Enforcement Mechanisms: what is the actual means of achieving different types of compliance, how often is it checked and to what degree of precision? For example, using an ESB to provide run time policy rule checking and routing.

- Communication: how can governance be communicated and demonstrated? For example using a service level management dashboard to demonstrate compliance with Quality of Service thresholds.

- Change Management: how can governance changes be audited? For example, using a service catalog to enforce service life cycle state change policies (e.g. publish and discovery) with support for system of record via a repository.

SOA Maturity View

We have developed a rich SOA Governance Framework that identifies expected SOA governance capabilities at each of five stages of SOA maturity as defined in the CBDI SOA Maturity model[3] to provide overall consistency. The maturity view includes capability maturity tables for policy, process, organization and infrastructure; table 2 provides some overall examples together with outcomes and risks.

The SOA governance capabilities indicated in the cells are mapped to the organization's "as is" state of SOA governance and to the "to be" state in terms of projected SOA outcomes. An SOA Governance Roadmap is then constructed forming a foundation for transition plans.

While the SOA Governance Maturity Model is rich, in order to provide comprehensive coverage, the intention is that it should be workable in small manageable chunks within its target context. This is where outcome and risk analysis, together with a good understanding of organizational context, come into play as described in the second part of this article.

Governance Area	Early Learning	Applied	Integrated	Enterprise	Ecosystem
Desired Outcomes	Successful Proof of Concept (PoC)	Assurance of QoS for project level services Adoption of common reference architecture is enabling reuse and flexibility within individual business solutions	Assurance of QoS for shared services Coordination of scope between selected projects is delivering cross-project consistency	Implementation of Service Portfolio Plan delivering consistent business processes and data for enterprise Compliance with common reference architecture ensuring enterprise-wide sharing/reuse, agility Delivery of agreed Service levels Cross life cycle management of Service assets delivering portfolio rationalization and component delivery approach	Industry compliance delivering business benefits through shared information and processes

Governance Area	Early Learning	Applied	Integrated	Enterprise	Ecosystem
Exposure to external risks **Failure of external services**	SOA is applied to inappropriate projects that are doomed to fail. SOA never gets past the first post	Solution meets immediate requirements, but is no better able to respond to future changes. SOA applied for wrong reasons	Uncoordinated SOA activity results in duplication and inconsistency in service delivery and usage misalignment across projects in classification and granularity of services resulting in incorrect usage, lack of usage	Service anarchy Inconsistency between assets at different SLC states Uncontroled offshoring and outsourcing	Suboptimal partnerships, relationships with customers, suppliers and third parties
Policy	PoC goal definition.	Basic Service Concepts Architecture Layering Default standards and QoS levels Project Service Portfolio Plan (SPP) Basic Service Description Service Life Cycle	SOA ref arch Compliance Usage by constituency Runtime standards QoS levels Publishing/Discovery of Design time reuse assets Service Specification Provider/Consumer Service Lifecycle	Sourcing and Usage with SLA Service Level Management Multi-participant Service lifecycle Enterprise Service Portfolio Plan (SPP) Publishing /Discovery of runtime reuse assets	Certification Business QoS levels Common global Service Specification
Process	Existing SDLC process checkpoints	Solution designs reviewed with respect to Project Service Architecture	Service Specification forms contractual interface between solution projects and provisioning projects	Service specification forms contractual interface between solution projects and provisioning projects	Clear traceability between business programs and IT (solution and provisioning) projects
Organization	Establish SOA Community of Interest Initiate SOA Steering Board to start	Establish SOA CoE EA perform SOA Governance Lead role	SOA Program Office Service Integration Office	Twin-Track – separation of provide/consume activities Sourcing and	Vertical industry bodies set service standards

Governance Area	Early Learning	Applied	Integrated	Enterprise	Ecosystem
	managing SOA adoption		Dedicated SOA Governance Lead Service Architecture Review Board	usage manager Service Ownership/Sponsorship SOA Governance Board	
Infrastructure		Simple Service Catalog. Design time only. Monitor/log service run-time, alert to problems	Service Catalog – with governance over publish/discovery activities	Service Asset Management with SLC governance tools - Integrated with Service Catalog Service Management – Policy driven, SLA support	Service Asset Management with SLC Automation Policy Store/Management, Policy Enforcement Automation

Table 2 – Overall Governance Requirements by Maturity Stage

Applying the SOA Governance Framework

We recommend that a SOA Governance Maturity Assessment should be carried before introducing SOA governance measures. However, despite the necessity of understanding the organizations level of SOA governance maturity and tuning your adoption plan accordingly, our experiences show that it is a mistake to *lead* with change. The key driver of SOA governance should be business and IT improvement.

Business-IT alignment techniques

It is therefore necessary to identify the business outcomes that SOA should support and map these outcomes to desired SOA outcomes. The risks that threaten these outcomes must then be identified using appropriate techniques. One particularly effective technique is to use a business-IT alignment table[4] as illustrated, for a travel company, in table 3; note that outcomes and risks are numbered for ease of identification and traceability.

Business Outcome	SOA Outcome	SOA Risks
B1: The customer's experience is streamlined by automating verification checks for risk and creditworthiness.	S1: Services that reflect business needs.	R1: Incorrect scope. R2: Misalignment

Business Outcome	SOA Outcome	SOA Risks
B2: A reservation broker provides access to further flights, where company is unable to fulfill customer's travel requirement.	S2: Services are specified to a rigorous level that allows certification to validate stated availability and security requirements across organizational boundaries.	R3: Lack of cultural integration. R4: Lack of agreed service levels.

Table 3 – Example Business-IT Alignment Table for a Travel Company

Building an SOA Governance Maturity Roadmap

We then need to ask what factors might help foster the outcomes and inhibit the risks and use these factors to infer the required governance capabilities. The required governance capabilities are analyzed at different stages of SOA maturity to determine governance capabilities that may reasonably be attained stage by stage; see table 4, which provides a detailed picture in terms of specific capabilities. Coloring of cells indicates the broad level of maturity for each capability; red = immature, yellow = partially mature, green = mature.

Note that the SOA governance capabilities should be further analyzed using capability dependency modeling[5] to identify further capabilities and to ensure the governance capabilities are positioned at the correct level of SOA maturity

Risk	View	Capability Area	Early Learning	Applied	Integrated	Enterprise	Ecosystem
R1: Incorrect scope.	Policy	Planning	SOA PoC has clear goals.	Project scope defined for services.	Cross project scope defined for services.	Enterprise scope defined for services.	Ecosystem scope defined for services.
R2: Misalignment	Process:	Alignment	SOA PoC projects have project charter	Solution designs reviewed with respect to Project Service Architecture	Service specification forms contractual interface between solution projects and provisioning projects	SOA Efforts aligned with business programs.	Business programs are service oriented; business services form bridge between business and IT.
R3: SOA not culturally integrated.	Organization	Role Groups	SOA Community of Interest	SOA CoE	SOA Governance Lead	SOA Governance Board	Vertical Industry Bodies
R4: Lack of agreed service levels.	Policy	Best Practice	WSDL is generally viewed as sufficient.	Service Description is project standard	Service Description is contract between all participants	Service Specification is contract between all participants	Common global service specification

Table 4 : Example SOA Risks and Governance Capabilities for a Travel Company

Choosing SOA Governance Hot Spots

Having built the overall roadmap for the most relevant SOA governance capabilities we are now in a position to zoom in to a further level of detail. It is important to realize that SOA governance is a potentially huge undertaking and to tackle it in small chunks. SOA policies in particular need careful management as there are potentially hundreds of policies and we do not want to swamp the governance undertaking before it gets off the ground, making life too onerous for architects and developers alike. We need "just enough" policy; see figure 4.
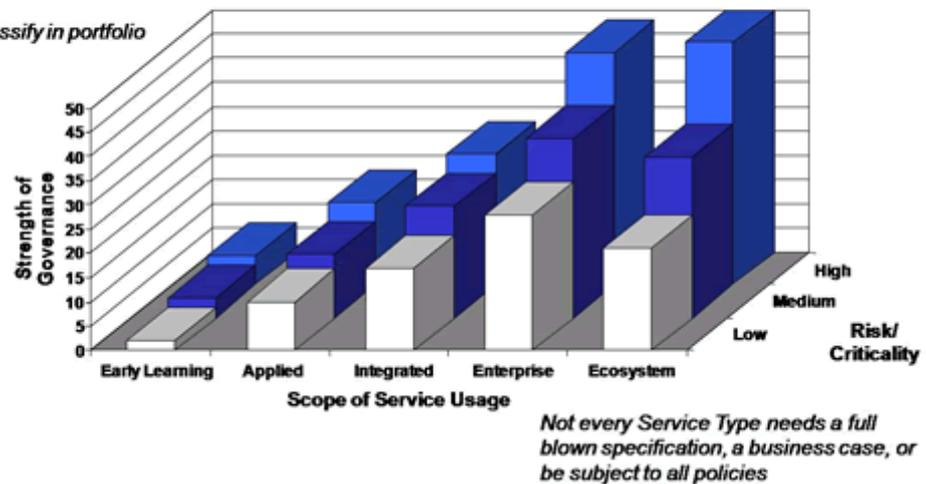
Figure 4: Balancing Freedom with Bureaucracy in SOA Governance

The real trick that emerges increasingly from our work is to identify those governance capabilities that address those risks that are the most relevant from a business point of view. These risks must then be broken down using triage and prioritized. This analysis and prioritization of risks should then be "reality checked" against the "as is" SOA governance capabilities. In the final part of this article we present some strategies that are designed to enable proposed improvements that are realistic and achievable.

In the example suppose that the Service Description policy is identified as a "root" capability upon which other the capabilities depend. In that case our attention would focus on developing and introducing policy for Service Description (R4). At the same time there will be changes required to the existing project planning policy (R1), system development lifecycle (R2) together with organization and cultural shifts (R3) that must be planned within the context of overall change management.

Using the Policy Hierarchy

We have found that use of a "ready made" hierarchy of policy types, such as the one we have developed in our Knowledgebase, can give governance work a real shot in the arm. The policy hierarchy is used a sounding board to flesh out the policy types required to hit the hot spots so to speak. At the same time it is always possible to think of more policy types and we are in fact evolving the policy hierarchy to reflect hard won experience, where relevant policy types are unearthed.

Dovetailing into the Broader Governance Picture

Most organizations have existing IT governance initiatives, which are often part of the overall EA function, into which SOA governance must fit. A holistic IT governance plan is called for that leverages what the organization has already learned while keeping key players on side. It is important not to throw the baby out with the bath water, though at the same time we don't want the baby to run the household! It is imperative to understand that each organization has its own culture into which SOA governance must fit. Key factors range from organizational reporting structures through the types of infrastructure technology in place such as repositories to existing use of EA frameworks; see figure 5.
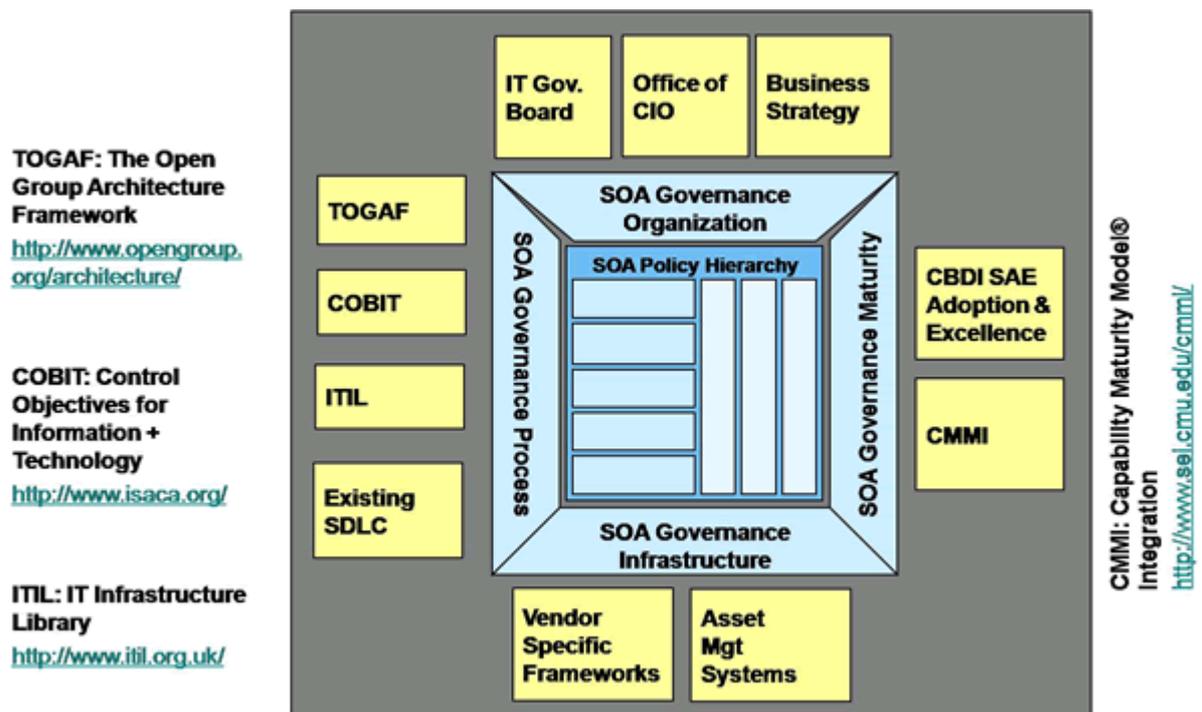

Figure 5: Establishing SOA Governance Context

A particular highlight of our recent experiences is that existing approaches to IT governance are often strong in technology infrastructure and standards but lacking with regards to business services and their management. So, certain pragmatism is called for in applying SOA governance framework to real world situations.

Tailoring the Lifecycle: Deliverables as a Compliance Mechanism

One of the main differentiators of an SOA approach is managing projects and programs according to contract. Deliverables therefore take center stage in the software process and form a key means of enforcing SOA policy, for example through the production of a specified deliverable at a certain point in the lifecycle.

It is important that each deliverable is clearly specified; CBDI SAE provides templates for SOA deliverables. The specific content that is required within each deliverable is governed by corresponding SOA policies, which will determine the required level of detail that is appropriate. For example, a Service Specification could potentially include a great deal of detailed information, which would be unnecessary for an organization that are not yet focused on wider reuse of services. The Best Practice SOA policies

must therefore include appropriate levels of detail in relation to the business value and need.

Phase	Service State	Example Deliverables (Artifacts)	Governance with
Feasibility	Planned	Business Process Business Type Model Business Case	Initial Scope Coordination
Approval	Planned	Project Service Plan Service Description	Coordinated Scope Reference Framework
Design	Specified	Service Specification Architecture Service Implementation Architecture Service Level Agreement	Service Specification Patterns Automation Unit patterns Conformance with Deployment patterns
Build/Integrate	Being Provisioned Provisioned Certified Published	Service Implementations	Service test profiles
Launch	Operational		Usage policies

Table 5 – Incomplete Example of Service Governance Items in the Project Life Cycle

Evolving the Lifecycle: A Pragmatic Approach

In many organizations it is too early to attempt the challenge of moving to a pure supply – consume software process in which service provisioning and solution assembly projects are strictly separated. A useful strategy here is for the solution team and the SOA CoE to work collaboratively on evolving a single Service Portfolio Plan, with the design approach focused on factoring out enterprise infrastructure services separately from the business domain services. This allows for the overall SOA to take shape with experience rather than being "forced" without sufficient knowledge at the outset. Such an approach involves introducing some of the key disciplines of the SOA process in an incremental fashion through the SOA CoE. The emerging new SOA disciplines should then work in iterative fashion within the context of the incumbent software lifecycle. End points of SDLC phases are aligned with SOA CoE disciplines through specified SOA deliverables. SOA governance is achieved by enforcing appropriate SOA policies through the software lifecycle phases. The SOA deliverables produced by these phases must comply with SOA policies before they are deemed certifiable for use in the next phase. In this way, SOA governance acts as a catalyst for evolving the software lifecycle, leveraging the status quo with minimal political disruption.

Evolving the Organization

This approach to policy enforcement requires a certain dynamic between the solution team and the SOA CoE working in a collaborative and iterative process, marshaled by the SOA Governance Lead role. In an EA context this role may be performed by the Enterprise Architect, again leveraging the status quo.

Again we need to keep in mind the cultural change aspect; a key topic that we can but touch on here. Collaboration and communication should be nurtured using mechanisms such as self service portals to encourage learning, such as an SOA CoE portal, along with collaborative environments (such as Microsoft's Sharepoint) for discussion, as well as more traditional approaches such as newsletters and emails.

In many ways, SOA governance is best introduced "under the covers" so to speak, using existing boards to perform SOA governance tasks such as formal reviews of SOA related documentation. Adding yet another board, such as the SOA Governance Board, might be seen by many as adding just another layer of bureaucracy, especially in the early stages. At the same time the SOA CoE is required sooner rather than later to provide necessary expertise in SOA; a full account of the SOA CoE is provided as part of Richard Veryard's article on SOA excellence[6].

Concluding Remarks

SOA brings with it a greatly increased emphasis on investment for reuse and software quality that is coming home to roost in those organizations that are progressing beyond early SOA proof of concept projects toward larger and larger solution scopes. In order to manage the risks SOA must be regulated according to various governance capabilities.

SOA governance is thus no longer simply an option but an imperative fuelled by increased pressure to regulate decision making and justify expenditure. This is why the spotlight has fallen so sharply on SOA governance.

Contrast this changing climate with the situation that we sadly find in many organizations today where overall IT governance is very much the pauper on the street. The larger the organization the larger the problem. It is all too common to find relevant documentation, from analysis to deployment, to be poorly structured, dispersed and fragmented. Often it is difficult to ascertain the status of documents (proposed, delivered, adopted) and to identify responsible owners. SOA governance represents an opportunity to put IT's house in order. In fact services are but one element in software solutions that are increasingly composed of a hybrid set of software pieces. We really need therefore to address the issue of governance as a whole and treat SOA governance as an opportunity for improving overall IT governance.

1SOA Policy, CBDI Journal , June, 2007
2 Towards the Service-Oriented Organization, CBDI Journal, Jan 2004
3SOA Maturity Assessment Survey, CBDI Journal, March 2007
[4] Service Orientation: Winning Strategies and Best Practices , Allen, P., Cambridge University Press, 2006
[5] Capability Dependency CBDI Journal May 2007
[6] SOA Excellence: Achieving quality and maturity in SOA adoption and use, CBDI Journal , February 2007

About CBDI

CBDI Forum is the Everware-CBDI research capability and portal providing independent guidance on best practice in service oriented architecture and application modernization.

Working with F5000 enterprises and governments the CBDI Research Team is progressively developing structured methodology and reference architecture for all aspects of SOA.

CBDI Products

The CBDI Journal is freely available to registered members. Published quarterly, it provides in-depth treatment of key practice issues for all roles and disciplines involved in planning, architecting, managing and delivering business solutions.

Visit www.cbdiforum.com to register.

Platinum subscription – A CBDI Forum subscription provides an enterprise or individual with access to the CBDI-SAE Knowledgebase for SOA delivering ongoing practice research, guidance materials, eLearning, tools, templates and other resources.

Everware-CBDI Services

At Everware-CBDI we enable large enterprises and governments to become more agile by modernizing their business systems. We have repeatable processes, resources, tools and knowledge-based products that enable enterprises to transform their current applications in an efficient, low risk manner, into an optimized service-based solutions portfolio that supports continuous, rapid and low cost evolution. Our consulting services range from providing practices and independent governance to architecture development, solution delivery and service engineering.

Contact

To find out more, and to discuss your requirements visit www.everware-cbdi.com or call

USA and Americas: 703-246-0000 or 888-383-7927 (USA)

Europe, Middle East, Africa, Asia, and Australasia: Telephone: +353 (0)28 38073 (Ireland)

www.everware-cbdi.com