WebLayers

Policy-Based Governance for the Enterprise

Introduction

> *"A large part of compliance activities within organizations are focused on developing formal processes, policies and procedures… IDC believes that, over time, the spending will shift to software…"*
>
> **IDC (2005)**

Table of Contents

EXECUTIVE SUMMARY

CIO's and IT leadership are challenged every day to support strategic business initiatives that are critical to the success of their companies. Every major business initiative requires some change within the infrastructure and application of their IT resources. While the changes are driven by business requirements, their success depends on the ability of the IT organization to rapidly and effectively respond to the demands of the business.

There are two significant challenges for IT organizations to overcome in support of these new business initiatives. The first is the proliferation of heterogeneous and highly distributed computing infrastructures. The very nature of the way IT resources have been deployed over the past dozen years or so make it extremely difficult, if not impossible, for IT leadership to exert the kind of control and influence over the work necessary to support the business. With so many projects being developed and deployed at the Line of Business level, IT can only "hope and pray" that they are being built with the enterprise requirements and guidance in mind that IT leadership has established. This lack of adherence to the policies established by IT from the project teams leads to systems being built and deployed that all have different interfaces, different ways to handle errors, different transaction processing models, different messaging support, and so on.

The second significant challenge is really a manifestation of the first. IT is being tasked with supporting these new business initiatives and, at the same time, being forced to reduce costs and squeeze every possible dollar of value from the investments that are being made in the systems and infrastructure. This pressure requires that the work that each individual does in the IT organization in support of the new business initiatives be built and deployed with ease of integration and enterprise reuse as fundamental requirements. Without the ability to enforce the policies that have been established to ensure these requirements are followed, IT is literally "flying blind" and investing millions of dollars in one-off projects that do not add to the enterprise IT assets of the company.

In this paper, we will explore these challenges in greater detail. We will also offer a solution, **Policy-based Governance,** which will allow IT organizations for the first time to exert control over the proliferation of distributed systems without hampering the productivity needed to rapidly respond to competitive pressures by the business.

As a company, WebLayers first identified these challenges during several strategic consulting engagements that we worked on in support of enterprise IT organizations that were building and deploying Service Oriented Architectures (SOA). We first started by working with the IT leadership team to understand what their policies and guidance were for their highly distributed IT teams that were building and deploying systems. We then audited the actual projects that were being delivered, and found that none of them were actually adhering to the policies that had been established. Project pressures like budget, time, and a general lack of resources required that these project teams cut corners to deliver their systems. This led them to ignoring the policies that were established, and IT leadership lacking visibility into their non-compliance. While our work initially focused on the development of SOA, we quickly discovered that this problem existed for any strategic IT initiative (SOA, Outsourcing/Offshoring, Enterprise Integration, etc.). All of the projects started off with great promise, but without a way for the IT policies to be enforced as part of the natural workflow of IT, it became impossible for the project teams to comply.

ABOUT WEBLAYERS, INC.

WebLayers is headquartered in Cambridge, MA. The company was founded in 2002 and is pioneering the market of Enterprise Policy-based Governance. The WebLayers team has extensive leadership experience in integration technologies, business modeling, distributed computing and Service Oriented Architecture. WebLayers is applying its expertise and experience to enable Policy-based Governance of strategic IT initiatives such as SOA, Outsourcing/Offshoring, Enterprise Integration, and many others.

WebLayers is a proud initiator and coordinator of **The SOA Forum**; an exclusive roundtable for Fortune 500 and Government Agency enterprise architects and IT executives. Current members include over 600 senior IT executives and Enterprise architects from companies such as Merrill Lynch, GE, Procter & Gamble, AT&T, Morgan Stanley, Fidelity Investments, Thomson Financial, Staples, Bank of America, Sabre Holdings, BP and others. The forum is also a media partner of Gartner, Inc. See www.weblayers.com/theSOAforum for more details.

For more info:

WebLayers, Inc.
125 Cambridgepark Drive, 6th Floor
Cambridge, MA 02140
Tel: 617.500.2282
Fax: 617.507.8003
info@weblayers.com

GOVERNANCE IS A BUSINESS IMPERATIVE

To ensure that the funded initiatives within the IT organization achieve the enterprise goals and objectives of the business, enterprises establish policies that will guide the IT project teams as they build and deploy their systems in support of the business. These policies range from what type of Open Source software is acceptable to use, to what type of security model to use, to what is needed for transaction archives.

The key challenge is how to seamlessly enforce the established policies.

An Example:

A Fortune 100 Financial Services firm is tasked with greatly reducing the costs of IT systems and maintenance, and to simplify the future integration of systems. This strategic initiative is classified as a “Business Transformation” initiative, and the IT leadership team settles on a Service Oriented Architecture (SOA) as the strategic direction for achieving the business goals of cost reduction, and simplification of IT systems.

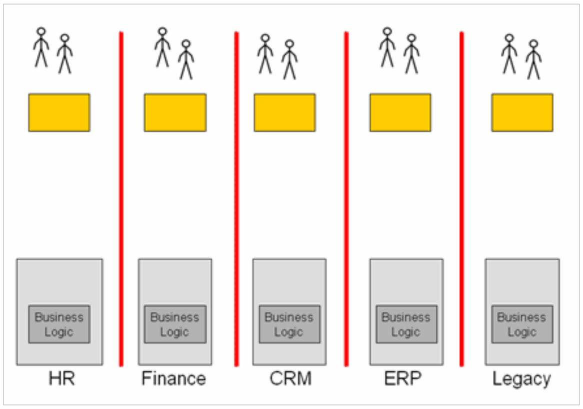

Figure 1 - Business today is limited by software silos

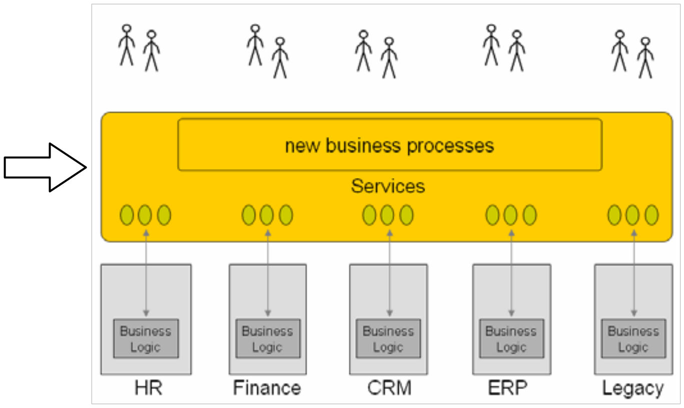

Figure 2 - SOA represents a business opportunity

They start by developing a set of guidelines (policies) for how their IT project teams should approach the development of Services and other XML artifacts as they build and deploy new systems. The focus of these policies is to ensure that the work they create is reusable, interoperable, scalable, and secure so that future systems that are developed can easily leverage the resulting work.

They then publish these policies to several distributed Line of Business IT teams working at the individual project levels. They commit resources from the Architecture team to work with these project teams and educate them on the new policies, help consult and guide them in their efforts, and to actually review the work that is created.

This seems to work well for the first 2 or 3 projects they work on, so they decide to make these policies more widely available by creating an internal IT portal and hosting them there in the hope that future IT projects will read, comprehend, and adhere to those policies. They assemble a “review board” within the Architecture group, and proceed to point all future projects to this board.

After a short period of time, the board is backlogged in their reviews, the projects they actually have time to review are constantly sent back to rework existing deliverables causing severe delays, and the business owners begin to look at the “review board” as an impediment to getting their systems deployed so they stop adhering to published policy.

The result? Almost all systems delivered without oversight contain significant integration challenges, a reinvention of the wheel for simple constructions like error handling, and no ability to reuse the work in future projects. Money is wasted, time is wasted, and the initial strategic objectives of cost reduction and system simplification are not fully attained.

WHY POLICY-BASED GOVERNANCE?

As we mentioned earlier, and illustrated in our previous example, every strategic IT initiative is driven by policies. At the inception of each initiative, the IT leadership team will define the policies that will guide the initiative throughout the projects’ life-cycle in order to achieve the business goals that have been established.

Most often, these policies are then translated into “rules” that are enforced at many different infrastructure points within the life-cycle of the initiative.

An Example:

According to industry analysts ZapThink!, many banks see SOA as a way to create families of shared Services for the purposes of identifying their most valuable customers and providing better value for them, across multiple lines of business.

For example, let’s say that a bank has created a Service domain (a family of related Services with a common business context) for customer information. They must resolve issues such as:

- Who is responsible for the shared customer information?
- How will they keep that information private?
- What are the policies and procedures call center staff and others need to follow to update this information?

- How will the organization resolve data cleanliness/inconsistency issues as a matter of policy?

Within a banking environment, of course, where strict local as well as federal regulations change frequently, but universally affects their core data services (everything from Sarbanes-Oxley to Basel II, and Check21), SOA is seen as a solution for continuous business agility. Regardless of the regulations the most important shared services are for customer data management and examining and evaluating common customer services (e.g. certain levels for opening accounts, providing general information to the customer). Policy-based governance is more than data exchange; it is about becoming more customer-centric, which means the integration of products and features across multiple groups with the result being renewed emphasis on improving customer satisfaction. That, and as banks transition from traditional informational services more to transactional services, the result is a more seamless, services-driven and compliance sensitive environment.

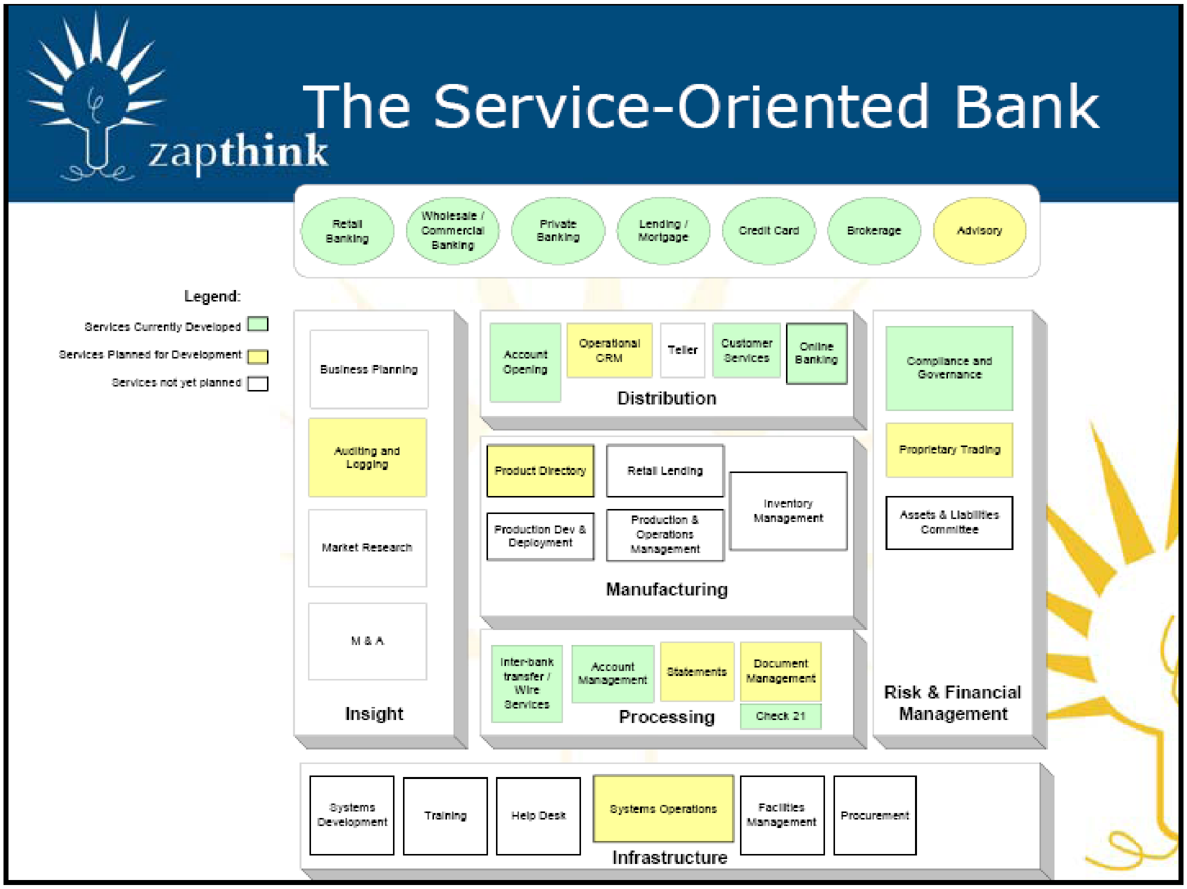

Figure 3: The Service-Oriented Bank

POLICY-BASED GOVERNANCE – An SOA Example

Service Oriented Architecture requires a major shift in the way software is developed and deployed within enterprises. Companies will have to move from the “Develop Now, Integrate Later” view to a “Develop for Integration” paradigm. The new paradigm, technologies, and standards created to support this shift require companies to implement their SOA in a well planned, well coordinated, and effectively managed way.

To ensure business continuity, reduce integration costs and complexities, limit corporate liabilities like security, and to effectively compete in the marketplace, companies must govern the design, development, deployment, and operations of any new Services in their enterprise.

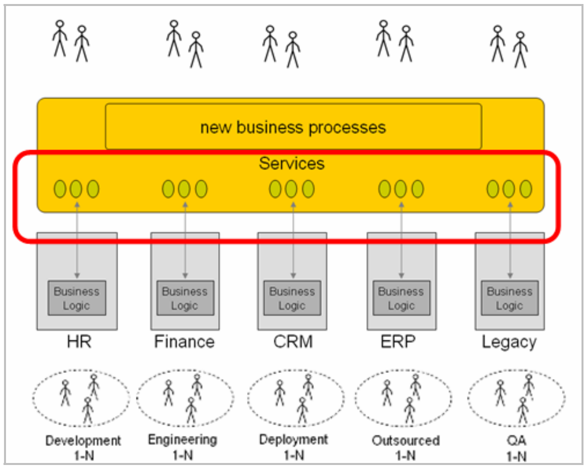

Figure 4 - SOA introduces a new layer to the Enterprise

For instance, a Fortune 500 Retail Bank is tasked with the challenge of integrating multiple backend systems in order to support a common view of customer data regardless of what channel the customers come in on. Whether they are standing in a Retail Branch, accessing their data via an IVR system, interacting with Customer Service through the Call Center, whatever the channel the bank wanted to deliver a consistent and common view of their data to them. By driving compliance and governance across each line of business – even virtually or through branch offices – they are able to introduce central control through a top-down modeling of Services, enabling this bank to reduce the number of service related inflection points, mitigate the actual number of Shared Services, and put into place a more holistic and actionable transaction-centric environment.

However, these critical requirements are being challenged by the very nature of the technologies and paradigms that constitute SOA, like XML, Web Services, business process…etc:

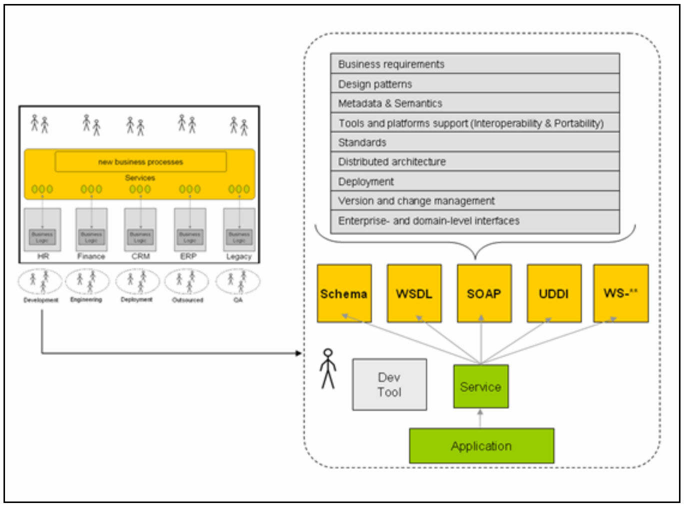

Figure 5 – Governed SOA ensures agile, reliable, and scalable operations

In this environment, policies are critical to ***ensure*** that all of the independent efforts (whether in the design, development, deployment, or operations of a Service) come together to meet the enterprise SOA requirements.

Several elements are required to achieve Policy-based SOA Governance:

1. Enterprise SOA Policies

Policies set the goals that you use to direct and measure success. Without policies, there is no Governance. Policy makers like IT Managers, Architects, Project Leaders, and Application Development Leaders are struggling to define, configure, and assign policies in a way that allows IT development teams to easily and transparently adhere to policies and practices. As a result, each team creates Services in a slightly differently way. This sacrifices interoperability, manageability, security, and the other benefits of SOA. Policies need to address the overall impact to the business of the Services that are being created and deployed. Policies need to create a strong connection between the business and technology. Companies need the ability to associate their business policies, technical policies and actual implementation in a transparent fashion. There are policies that all services must adhere to from an enterprise perspective. This then proceeds down through the enterprise, all of the way to the granular policies that a project team might implement, from the perspective of the division or business unit, department, or team. Policies are technical and business requirements that aim to create a common utilized language of information and process. Deployed in SOA, policies need to address the very distributed, asynchronous, and heterogeneous nature of the SOA environment.

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. (HIPAA)*
- *All financial transactions must provide traceability and tamper proof mechanisms for mandatory audit records. (SOX)*

Project outsourcing initiative might represent its requirements as:

- *Project must have interoperability policy passing score better then 80% during the acceptance testing.*
- *Any project failing key security policies must be scheduled for a manual review*
- *Outsourcer must provide signed acceptance checklist to the project manager prior to the acceptance testing.*

This is higher level policies will often need to be translated to highly 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

If any one of these sets of policies is not followed, the impact on company operations and bottom line can be enormous.

2. Auditing & Conformance

Policies should not be left to documentation. Policies should be an active part of the operations of companies. Following the policy definition stage, policies should be put to work to detect, analyze, and audit compliance. This process should be integrated with the design, development, deployment and operation of Services in an efficient and transparent manner. IT Developers, Architects, and Project Teams need the ability to conform to policies through an automated system that will enable them to easily trace and address noncompliance.

3. Management: Track, Review & Improve

Once policies are defined and conformance processes are in place, decision makers need to govern the implementation, encourage reusability, manage collaboration processes, and improve business metrics. These outcomes are the true value of integration. Completing these processes should answer the following questions:

- **Policies** — What policies do we have? Where are these policies implemented?
- **Enterprise Interfaces** — What enterprise Services are being developed?
- **Conformance Status** — How well do our services conform to our policies? Which interfaces are not in compliance? What is the impact of the noncompliance on the operations of the Services or our business operations? Are there any security breaches? What are our service levels?
- **Impact Analysis** — What happens to our SOA operations if we change our current SOAP policies? What if we need to add new elements to our SOAP message headers?
- **Interdependencies** — How will operations be impacted by changes made to Services? Which critical processes will be affected or even cease to operate?
- **Exception Management** — Can we grant an exception to a defined policy for a certain project? What will be the impact of an exception?

4. Integration

There are two aspects to the integration of SOA Governance: Process Integration and System Integration.

Process Integration. SOA Governance must integrate with the current flow of Service development and with the tools and systems available. This ensures that Service implementations are in conformance with enterprise policies throughout design, development, testing, implementation, deployment, and maintenance.

System Integration. SOA Governance must transparently integrate with EAI, development tools, and other enterprise applications that are producing and consuming Services.

CONCLUSION

In this paper we have explored the rising need for exercising greater control and influence over strategic IT initiatives as the pressure to deliver more capabilities with fewer budget dollars has continued to increase. This need for expanded control and influence is challenged intuitively by the very nature of our highly distributed, heterogeneous, and independently “owned”, silo-centric IT systems and resources.

The concept of policies is not a new one. We have been establishing, publishing, and enforcing them in our IT projects since we first started working with IT systems. In the past we have referred to them as standards, best practices, requirements, etc., but in all cases they were targeted at ensuring that the work that we were doing in support of the business actually delivered on what it was intended to do.

Time and again, we have gone down the path of researching, developing, and delivering enterprise policies, only to have the best intentioned project teams completely ignore them so that they can deliver their projects, on time, in support of the pressure from business. From the project’s team perspective adhering to these policies means that projects will be delivered late, over budget, and not advance, in general, personal agendas. What remains is an environment where the enterprise is publishing policies and “hoping and praying” that the project teams are ”buying into” them; and project teams delivering systems that simply cannot be supported, maintained, or leveraged for future development efforts.

We don’t believe it should be this way. With a focus on the policies necessary to ensure all initiatives are delivered according to the enterprise requirements, IT organizations can achieve the best of both worlds: delivering systems that support the short-term needs of the business, while building a foundation for policy-based governance that can be easily leveraged for its on-going and future needs.

ABOUT WEBLAYERS, INC.

WebLayers is headquartered in Cambridge, MA. The company was founded in 2002 and is pioneering the market of Enterprise Policy-based Governance. The WebLayers team has extensive leadership experience in integration technologies, business modeling, distributed computing and Service Oriented Architecture. WebLayers is applying its expertise and experience to enable Policy-based Governance of strategic IT initiatives such as SOA, Outsourcing/Offshoring, Enterprise Integration, and many others.

WebLayers is a proud initiator and coordinator of **The SOA Forum**; an exclusive roundtable for Fortune 500 and Government Agency enterprise architects and IT executives. Current members include over 600 senior IT executives and Enterprise architects from companies such as Merrill Lynch, GE, Procter & Gamble, AT&T, Morgan Stanley, Fidelity Investments, Thomson Financial, Staples, Bank of America, Sabre Holdings, BP and others. The forum is also a media partner of Gartner, Inc. See www.weblayers.com/theSOAforum for more details.

For more info:

WebLayers, Inc.
125 Cambridgepark Drive, 6th Floor
Cambridge, MA 02140
Tel: 617.500.2282
Fax: 617.507.8003
info@weblayers.com