**SOA policy management**
**White paper**
April 2009

# Realizing business flexibility through integrated SOA policy management.

*How integrated management supports business flexibility, consistency and accountability*

*John Falkl, distinguished engineer and chief architect, SOA governance, IBM Software Group*

*Phil Fritz, marketing manager, data center transformation strategy and planning, IBM Software Group*

*Maryann Hondo, senior technical staff member, member of the academy of technology, Web services security and policy, IBM Software Group*

**Contents**

## Executive summary

Increasingly, companies are looking to service-oriented architecture (SOA) to reconcile and unify IT systems and business processes, and to support a more flexible and agile business. But the benefits of SOA are sometimes not immediately visible because it takes time to clearly define sets of governance processes and business goals, and to establish a way to enforce and monitor processes and goals.

Policy management, however, can be a powerful vehicle to achieve an SOA evolution. It plays a key role in enabling SOA governance practices, designed to help businesses identify and focus on key critical services. Adding policies establishes points of control and agility for business and IT, accelerating the adoption of SOA solutions by providing flexibility and responsiveness.

IBM defines SOA policy management as a methodology and a set of elements (software architecture, tools, infrastructure and processes) in an SOA solution that focus on the consistent authoring, transformation, deployment, enforcement, monitoring, and auditing of directives and requirements related to the operation of SOA-based services. Key activities for SOA policy management include the expression of a desired state—or an action to be performed—that is recognizable by humans; the creation of elements and attributes that can be understood and automated by machines; and the enforcement and monitoring of a desired state or action.

Within SOA governance, policy management makes business and technical decisions visible to the organization. Good SOA management practices enable business and IT to converge on a common strategy to achieve SOA. And using policy management, rather than hard coding application logic, to achieve business goals can drive business agility and flexibility.

**Highlights**

***Policy management can enhance existing business value by allowing organizations to conduct business and operational objectives as policy goals.***

Effective policy management, in fact, can preserve and enhance existing business value by allowing organizations to conduct business and operational objectives as policy goals. It can enable closer alignment between IT and business because it facilitates communication about business objectives and their required technical implementation and configuration details.

This white paper provides a launching point for deeper discussions of SOA policy management. It specifically addresses policy management within the context of SOA governance of domains such as business services, security management, service lifecycle management and service management.

### Understanding the importance of SOA policy management

SOA usage has grown tremendously across industries as organizations seek to achieve benefits from the increased business agility that the architecture provides. But to achieve those benefits, organizations need to identify and manage existing risks and complexities. They also need to look out for the challenges associated with using technology such as Web-based commerce or representational state transfer (REST) initiatives to move to service orientation.

***Service orientation has changed how people use applications—it enables practically anyone to reuse services for their particular needs.***

In the past, companies easily understood the roles and permissions required for all potential users of a particular application: It was assumed that those criteria were kept within the perimeter established by IT or were controlled and used only by a specific line of business (LOB). But service orientation allows users across project teams, LOBs and entire enterprises to reuse services for their particular needs. Companies need new methodologies and tools to update applications quickly so that they can respond to business needs and seize competitive opportunities.

**Highlights**

Policies play an essential role in supporting business agility in a service-oriented world because they represent the expression of the high-level business objectives or IT best practices traditionally captured in verbal or document form.

With the adoption of SOA, the requirement for robust policy management capabilities as core aspects of a services-oriented strategy has accelerated. This requirement surfaces in two primary ways:

***Policy expression and policy enforcement allow business and IT to define and enforce SOA policies in ways that are familiar to them.***

- ***Policy expression*** *provides a practical vehicle in the broader domain of SOA governance to capture the enforcement of goals, best practices, architectural principles, government regulations, laws and other business objectives covered by an SOA governance framework.*
- ***Policy enforcement*** *provides data points for IT management frameworks to assess the effectiveness of their operational run times and to determine how well they conform to the governance practices of the organization.*

In other words, business policies can express abstract business objectives or goals. In turn, architectural and operational teams can refine those policies to be more understandable and actionable. These operational policy expressions can then be interpreted and enforced by policy-enabled elements of the IT systems.

### Reaping the benefits of SOA policy management

Good SOA policy management provides three key business values:

***Good SOA policy management provides flexibility, consistency and context, and accountability.***

- ***Flexibility:*** *Implementing a policy management layer enables controlled changes to the environment without impacting functional services already in production. This policy capability enhances overall SOA flexibility by enabling the IT organization to respond to and implement changes quickly without recoding applications or deploying a new infrastructure to support those changes.*
- ***Consistency and context:*** *Integrated SOA policy management can ensure that proper business context is applied consistently across all service lifecycle stages in a controlled manner. For example, a new community may need to*

*reuse an existing service, but corporate or regulatory standards may require a different security mechanism to support the new community's needs. In a traditional environment, the security mechanism would be implemented and applications would be recoded to support the upgrade. A policy framework coupled with SOA security services or SOA appliances provides common elements that can minimize cross-domain impacts of a new policy requirement or policy change. It can help the IT organization reach the right level of enforcement with minimal churn in the data center.*

- ***Accountability:*** *Establishing a framework for SOA governance is critical to maintaining business accountability, ensuring compliance with regulatory requirements and implementing business and IT best practices. Integrated SOA policy management can help ensure that, once an operational environment is established, the ability to make changes to policies becomes part of the governance framework and is itself providing accountability. This integration of governance as part of policy management also helps ensure that changes are auditable with existing mechanisms—demonstrating what the change was, who authorized it and when it was enforced.*

**Highlights**

***SOA policy management can reduce the time and cost of changing business policies, thereby improving an organization's ROI for its SOA.***

Policy strategy and implementation can enhance an organization's ROI for its SOA. Traditional systems that implemented business requirements as a single data model in application code—with specific policy expressions embedded in individual product offerings—can be difficult, time consuming and expensive to maintain and modify as applications evolve and migrate to new platforms. An SOA policy management strategy can reduce the time and cost of changing business policies by introducing control points for IT policies. Consequently, it can improve agility and reduce the costs and maintenance of SOA business applications, which, as a result of proactive management via policy enablement, can increase revenue opportunities.

**Highlights**

***When determining SOA policies, it's critical to establish policy ownership so everyone knows who is responsible for which policy.***

***Every policy must have an owner. It's easier to determine owners based on where the policy falls in the development lifecycle.***

### Defining roles, responsibilities and policy ownership

In SOA policy management, the process of collecting and defining business polices must be incorporated into the business's organizational governance practices. This is because, in the process of creating a policy, a company may discover that an objective can be expressed by different parties in the organization in multiple ways, depending on the specific responsibilities of the author. A key aspect of SOA governance, therefore, is to establish policy ownership so parties can resolve how to represent a policy and who is responsible for the creation and maintenance of the policy.

Regardless of the specifics of the governance model, someone in the organization must be responsible for capturing high-level business policies, including industry or government mandates for compliance such as the Health Insurance Portability and Accountability Act (HIPAA) or the Sarbanes-Oxley Act. It is common for high-level requirements to be captured only in documents, but the requirements that the business policies express often need to be managed in IT operations and enforced by the organization's infrastructure and practices. Because, in the end, it's business application users who are business service users.

Knowing how to enable an SOA with policies requires that a policy practice be defined within governance. This practice can be assisted by a common policy framework spanning the SOA lifecycle. Following are some examples:

- ***Development governance****, which can include a policy for checking compliance policies along with the associated review and enforcement of development best practices.*
- ***Deployment governance****, which can include a service governance policy that challenges stakeholders (such as architects and development leads) to certify that the proper polices are in place. It ensures that service transitions (for example, the transition from test to production) comply with required development and architecture policies before the services are successfully deployed.*

- ***Operational governance**, which can include policies defined and declared at run time that correlate with the development governance practice and that regulate access control, compliance and identity. These policies can be reviewed by the IT organization, checked for governance and then consistently managed in operations and enforced at run time.*

**Highlights**

***A successful SOA policy management approach is not a single-unit, one-size-fits-all solution.***

A comprehensive SOA policy management solution manifests itself as services, functions, architecture principles and organizational discipline—not a single-unit one-size-fits-all solution. Businesses that implement a successful strategy will apply consistent discipline across multiple products in their SOA platform as part of a broader governance strategy and solution architecture.

### Building on the IBM policy framework

To help organizations create the appropriate SOA policy management solution, IBM provides a strategy for thinking about how policies impact different groups within the organization.

***IBM sees policies as belonging to one of three groups: business policies, architecture policies or operations policies.***

Through working with its customers, IBM has collected a set of categories for policies focused at different levels and domains of expertise within a company. Each type requires different expertise and levels of detail for successful implementation and enforcement. *Business policies* are captured as business statements and include security and privacy policies, business services policies and business policies. *Architecture policies* are captured as development patterns and architecture assets, which may be developed with a standard naming convention. And *operations policies* are rendered as settings and entitlements, including access control policies, service-level policies and reliable messaging policies.

**Highlights**

### Managing each stage of the policy lifecycle

Implementing an SOA policy management strategy requires identifying service enablement points across the three layers of abstraction: business, architecture and operations. The requirements at each of these levels may have previously been captured in disparate forms, so it's important that a company identify the locations (for example, service registries) and common expressions that services or service infrastructures can interpret and act upon.

To establish a policy-driven approach to SOA, it is important for practitioners to identify a specific approach to their targeted policy enablement tasks. Because policy enablement—like SOA—is evolutionary, organizations should start small and expand incrementally. They should consider and address specific services and the policy they affect, along with the roles that must be defined and assigned, and the architectural implications for how the policy will be enforced and audited.

***Every policy has a lifecycle. First it's authored, then it's transformed, then it's enforced, and finally, it's monitored.***

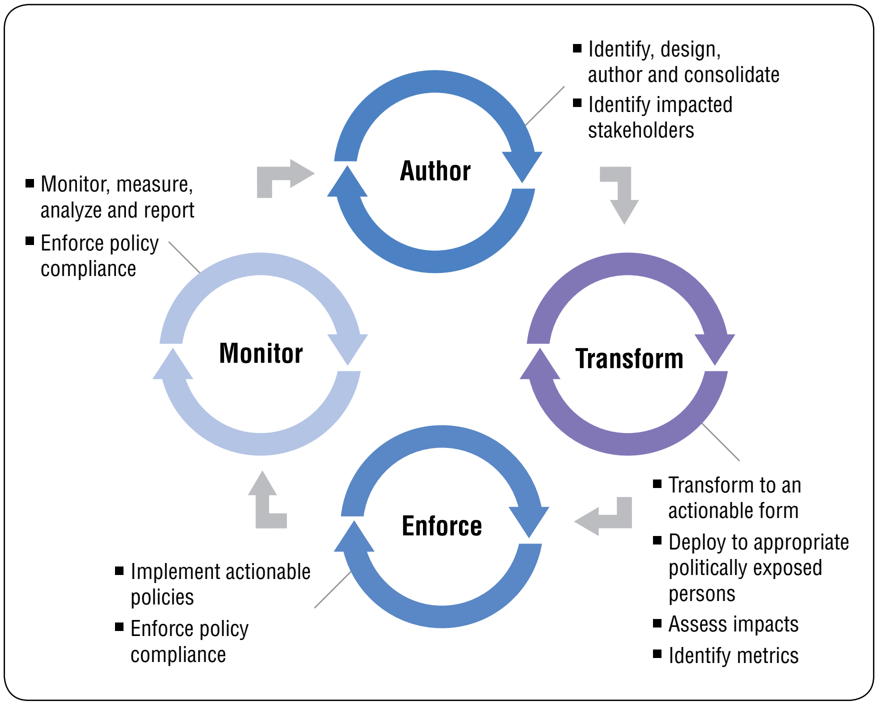
■ Identify, design, author and consolidate
■ Identify impacted stakeholders
Author
■ Monitor, measure, analyze and report
■ Enforce policy compliance
Monitor
Transform
■ Transform to an actionable form
■ Deploy to appropriate politically exposed persons
■ Assess impacts
■ Identify metrics
Enforce
■ Implement actionable policies
■ Enforce policy compliance

*Figure 1: The lifecycle of individual policies*

**Highlights**

As shown in the figure, every policy has a lifecycle. First, it is authored or defined; second, it may be transformed; third, it's enforced; and finally, it's monitored. Some organizations taking an SOA approach may already have established policies that they've captured in digital form, and they may be looking to start an SOA project that will enforce the.se policies across their infrastructure. Others may be starting to establish policies and are looking for tools and the infrastructure to help with basic authoring and policy expression management tasks, such as collecting the most common security policies. Still others may have policies already defined for their SOA and are looking for a way to map between different expressions into a canonical or common form.

### An SOA policy scenario: how management works

*The JKHL Enterprises scenario illustrates architectural and operational policies at work.*

The following scenario is an example of operational and architectural policies at work for JKHL Enterprises (JKHL), a hypothetical company. It shows IBM's integrated and federated approach to managing policies in an SOA. It also provides a common vocabulary that can be applied to a deeper investigation of policy management domains, such as security, business services and governance policies.

JKHL starts with a focus on service lifecycle management. Having already identified a set of services, it recognizes that they must be managed as new versions of the services created. The company starts with a set of policies and a Web Services Description Language (WSDL) for each service in its service registry. Responsible for governing the lifecycle of the services portfolio, the SOA architect encodes best practices into the service development lifecycle.

**Highlights**

***WebSphere Service Registry and Repository software enables SOA architects to define governance policies and associate them with services identified by the governance practice.***

JKHL selected IBM WebSphere® Service Registry and Repository software as its service lifecycle management tool. It enables the SOA architect to define a set of service governance policies reflecting JKHL's lifecycle management requirements and to associate those policies with the appropriate services identified by the governance practice. The authoring capability in WebSphere Service Registry and Repository makes this possible by creating and attaching policies to the WSDL service artifacts.

The company's SOA governance process also requires all services to be checked for a certificate of originality before they can be made available to consumers. The validators included with WebSphere Service Registry and Repository can help ensure that the service has been verified for confirmation of ownership and that an authentication policy exists to help ensure that the service is only accessible to authenticated users.

***Rational Asset Manager helps SOA architects verify that code has been checked for originality and is approved by the business for service lifecycle management.***

JKHL also uses IBM Rational® Asset Manager software in its development lifecycle tooling. To ensure compliance with corporate policy, development practices must include checking code that's created through the development lifecycle for originality before the service artifact is published to the registry. In this case, the SOA architect uses Rational Asset Manager to verify that the service artifact has been checked and is approved by the business for service lifecycle management. The Rational software can also automate compliance checks, and WebSphere Service Registry and Repository can check compliance for other services before accepting an artifact into the service lifecycle.

Next, JKHL's SOA architect must express the requirements of its corporate policy, which requires all personally identifiable information (PII)—such as clients' social security numbers—be encrypted and only accessible by specific personnel. This high-level business policy may need to be expressed as several

**Highlights**

operational policies. As a first step, the SOA architect uses the policy authoring capabilities of WebSphere Service Registry and Repository to define a high-level message security policy. Then the architect associates that policy with a set of services known to contain PII. Once the policy is defined and managed through the service lifecycle governance practice, it can be associated with other services.

***Tivoli Security Policy Manager and WebSphere DataPower SOA Appliance solutions push or pull artifacts so that policies associated with services can be interrogated at run time for compliance.***

The architect relies on a registry to maintain a set of services and policies that have been through the governance practice. In security operations, JKHL deployed IBM Tivoli® Security Policy Manager software for security policy administration and enforcement across multiple IBM WebSphere DataPower® SOA Appliances. In this process, policy artifacts are either pushed or pulled to the Tivoli and WebSphere DataPower solutions so that the policies associated with services can be interrogated at run time for compliance.

JKHL's business security policies require an additional level of expertise for security. IBM Tivoli Security Policy Manager software enables the SOA architect to author and administer application entitlements and granular, role-based authorization policies, helping to ensure that only authorized personnel can access JKHL's clients' PII. Through the integration of the Tivoli software and the WebSphere DataPower SOA Appliance, JKHL has the ability to deliver true run-time enforcement of the message security policy and fine-grained authorization policies into operations that leverage the appliance's run-time service. In this process, the Tivoli Security Policy Manager software generates access control policies to associate with the service and information. It subsequently uses the WebSphere DataPower SOA Appliance as an enforcement point for those policies.

### Summary: getting started with SOA policy management

Within the realm of SOA governance, SOA policy management offers essential capabilities for better management and control of services across the enterprise—supporting service reuse, a key SOA value. The resulting flexibility provides a means to translate business objectives into enforceable control points within the services portfolio.

Effective SOA policy management enables an organization to:

- *Reduce the code required to define and manage services policies.*
- *Abstract key logic such as access control and performance associated with policies.*
- *Implement policy enforcement points to support and monitor services compliance.*
- *Facilitate updates across services so that changes to operational or functional characteristics of services have minimal impact to the SOA infrastructure.*

### For more information

To learn more about how IBM solutions can help meet your SOA policy management initiatives, contact your IBM representative or IBM Business Partner, or visit:

**ibm.com**/soa/gov

and

**ibm.com**/software/tivoli/governance/action/01082009.html

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
April 2009
All Rights Reserved

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

The information contained in this document is provided for informational purposes only and provided “as is” without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice. Without limiting the foregoing, all statements regarding IBM future direction or intent are subject to change or withdrawal without notice and represent goals and objectives only. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.