
SOA Governance: Control of SOA and Web 2.0

Enterprise Integration Summit

L. Frank Kenney

April 16-17, 2008
Centro Banamex
Mexico City, Mexico

For more information about our research policies, processes and methodologies, please visit [Gartner Research Methodology](#) on gartner.com.

These materials can be reproduced only with written approval from Gartner. Such approvals must be requested via e-mail: vendor.relations@gartner.com.

Gartner

The Push for Innovation: New Devices and Technologies Further Complicate Governance



Use of this site is subject to express [terms of use](#). By continuing past this page, you agree to

Google LABS

Labs.google.com, Google's technology
Google labs showcases a few of our favorite ideas and how we use them to improve them. Please play with these prototypes and let us know what you think.

New! Experimental Search
Check out Google's latest ideas
05/16/07 - [Give us feedback](#) - [Discuss with others](#)

New! Google Voice Local Search
Search for local businesses using your voice, from any phone, for free.
Dial 1-800-GOOG-411.
04/06/07 - [Give us feedback](#) - [Discuss with others](#)

New! Google Code Search
Search public source code
10/05/06 - [Give us feedback](#) - [Discuss with others](#)

New! Google Reader
Use Google's web-based feed reader to keep track of your favorite web sites
09/28/06 - [Give us feedback](#) - [Discuss with others](#)

Google Transit (currently available in select cities)
Plan trips using public transportation
09/25/06 - [Give us feedback](#) - [Discuss with others](#)

Gartner

We believe that "don't ask, don't tell" is a dominant approach among IT organizations regarding users exploiting non-approved applications, Web sites [including software as a service (SaaS)] and devices. ("Don't ask, don't tell" appears to coexist with content monitoring and filtering, encryption, digital rights management, selective activity monitoring, strong authentication and minimal inspection approaches that many enterprises have adopted.) "Don't ask, don't tell" is a product of IT professionals believing that active endorsement of user experimentation will be viewed as a dangerous strategy, outside the mainstream. From an innovation point of view, we believe that no IT organization can stay on top of innovation on the Web, and that users can (and do) produce innovative ways of exploiting new and existing technologies with far greater speed, volume and effectiveness than an IT organization can. Over the history of our industry, most of the innovation has come from users, and this applies to every stage of the value chain — from subcomponent manufacturer to system manufacturer to IT organization to end user. The further down the value chain, the higher the level of creative innovation.

Key Issues

1. What effect will Web 2.0 technologies have on underlying SOA infrastructures, and why?
2. What technologies and methodologies should you have in place to ensure continued governance of SOA and Web 2.0 initiatives?
3. What are the vendors' approaches to SOA governance and Web technology governance?

Gartner

Key Issue: What effect will Web 2.0 technologies have on underlying SOA infrastructures, and why?

The Assembly of Web 2.0 Artifacts Demands Attention and Governance

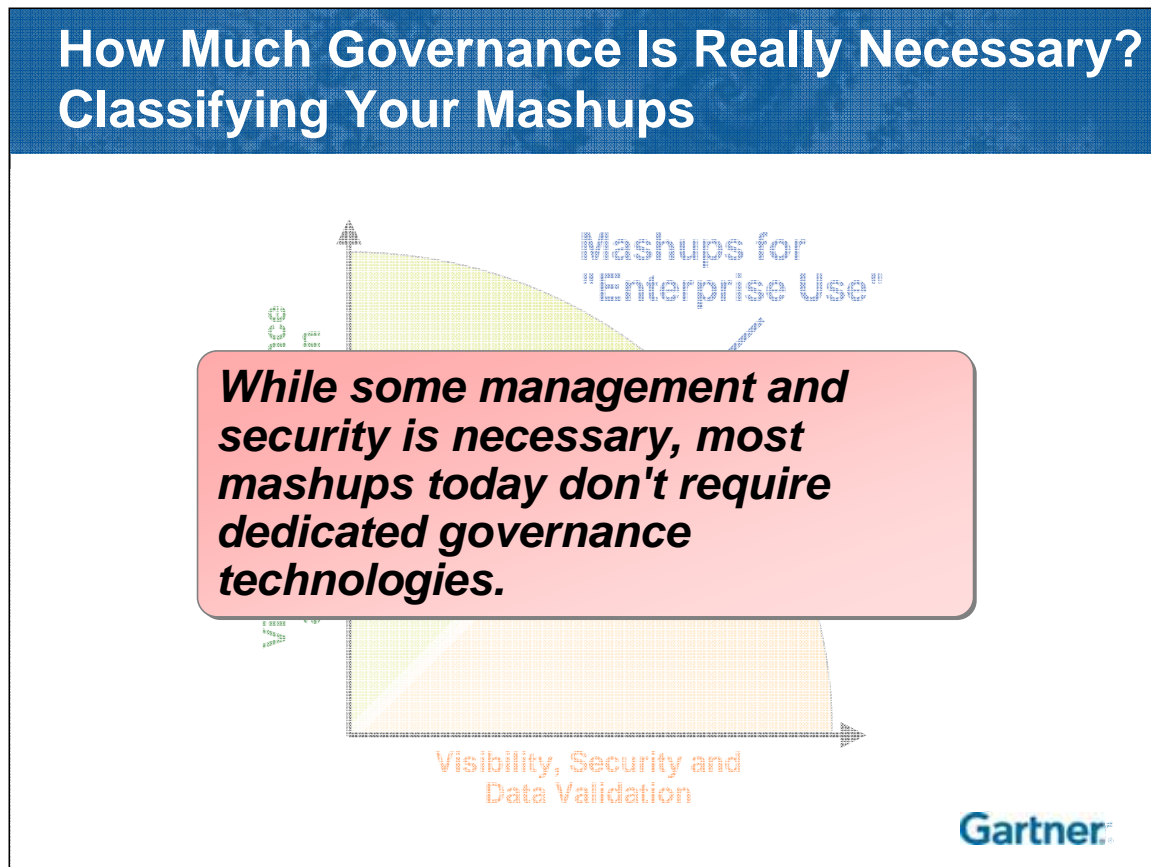
**... terrifying developers, system administrators,
architects and security analysts.**



Gartner

As IT moves into the next wave of Internet-based technologies and business models, the nontraditional IT user will have more of an effect on which products and services are offered by the enterprise. These users will be responsible for many ad hoc "on the fly" projects using both Web 2.0 technologies and valuable, sometimes critical and confidential, corporate business services. What is important, however, is that Gartner sees that many companies will become more forgiving of these non-IT users — in many cases demanding that the IT organization support the efforts, applications and interfaces of these ad hoc developers. IT will be forced to formally define the life cycle of these artifacts and ensure that they are "certified" for enterprise consumption.

Strategic Imperative: The more you depend on mashups for your critical business services, the more you need to use SOA and Web 2.0 validation technologies to ensure user satisfaction and met expectations.



Key Issue: What effect will Web 2.0 technologies have on underlying SOA infrastructures, and why?

Having a governance strategy that is rooted in reality is often overlooked as over 100 policies are defined and enforced on only a handful of resources and artifacts that, in reality, have low strategic importance to the organization. For example, many end users are quite forgiving if the information on a Google Map is incomplete or if the service is underperforming. Many just refresh the screen, and the experience is still an enjoyable one. At the other extreme, however, the data sources need to be correct and the service needs to be available if an organization or individual has created a business model around the mashup. Visibility, performance, security and data validation all have their importance, but should be considered within the context of who is the consuming entity and what is the value they put on the service.

Tactical Guideline: RSS feeds and reader software are no less secure than Web browser software; instead, it is somewhat more secure, depending on the RSS package and the browser with which it is being compared.

Governing Syndication

- The majority (if not all) of RSS feeds are XML over HTTP
- Authentication, encryption and access control in combination with HTTP are well-known and understood
- When higher levels of security and management are needed, virtualization extensions such as Greasemonkey work well enough

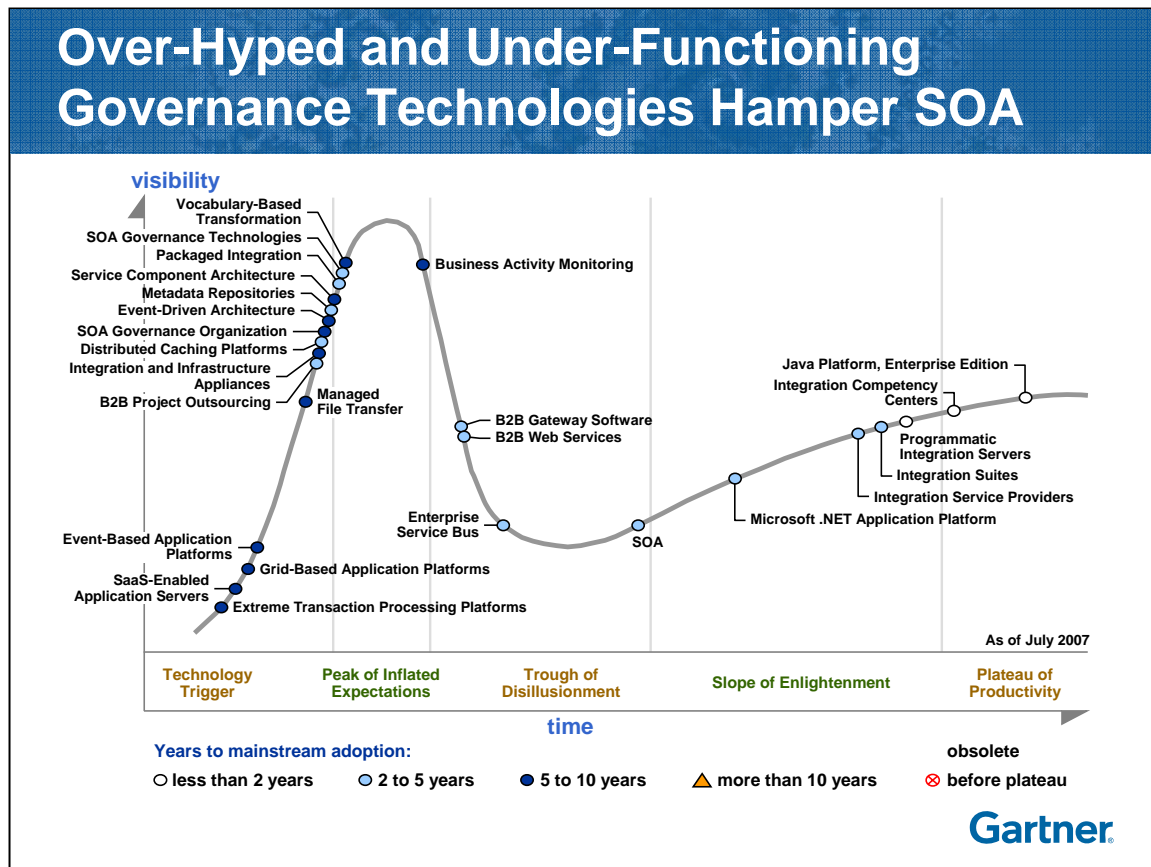
No need for new technologies... yet.

Gartner

Key Issue: What effect will Web 2.0 technologies have on underlying SOA infrastructures, and why?

In the case of RSS reader software, discussions of security vulnerabilities are mostly theoretical because this software has not been targeted by hackers and crackers in the same way that Web browsers and e-mail software have been. However, in general, a user accessing content from a Web site via RSS is no less secure than a user accessing content from the same site via a Web browser. As RSS readership grows and different usage scenarios for RSS proliferate, this situation may change; therefore, it is useful to understand the factors that affect security in RSS readers — some of these factors favor security, while others hinder it. One factor that favors security is the inherent simplicity of RSS software and protocols compared with broader-scope and more-complex Web and e-mail systems. RSS client software is more narrow in scope and, therefore, the programs are smaller and simpler (easier to code). This reduction in code volume and complexity tends to reduce security vulnerabilities. However, this will change as RSS usage scenarios broaden in scope and the software expands to meet extended requirements. RSS reader software will increasingly rely on full-featured browser engines (such as those in Internet Explorer, Firefox and Safari browsers), inheriting their security strengths and weaknesses.

Key Issue: What technologies and methodologies should you have in place to ensure continued governance of SOA and Web 2.0 initiatives?



The use of SOA is accelerating in response to escalating business requirements, the emergence of Web and Web services standards (such as WSDL and SOAP), and the improving availability of SOA-capable development tools and applications. The growing use of BPM and business activity monitoring (BAM) is also causing companies to use more SOA, because BPM and BAM are more-effective and easier to develop when using SOA. SOA governance technologies, specifically the service registry, and SOA policy enforcement (service management and service security) have been hyped by vendors and end users; many end users are deploying these technologies without credible SOA governance organizational processes and strategies. As a result, service registries and policy enforcement tools are often underused today (only for cataloging and XML security). With more vendors entering into OEM agreements and partnerships with best-of-breed vendors, these technologies will reach the Peak of Inflated Expectations within 12 months. However, because most SOA deployments will likely fail without proper governance, enterprises will eventually move to better leverage SOA governance technologies to provide visibility, manageability, monitoring security and quality assurance.

Tactical Guideline: Ensure that governance is part of business management, SOA governance is part of IT governance, and policy management is part of SOA governance.

Attributes Of Technical SOA Governance

1. **Visibility** — Can users find and use my resources?
2. **Security** — Are users allowed to access resources?
3. **Management** — Are my resources behaving as designed and expected?
4. **Audit** — Is the system being used and who used them?
5. **Development** — Are my resources being developed and are they adhering to standards?
6. **Validation** — Are my resources being validated, and are they valid, in the context of the business?
7. **Composition** — Can my resources be composed to create new composite entities?

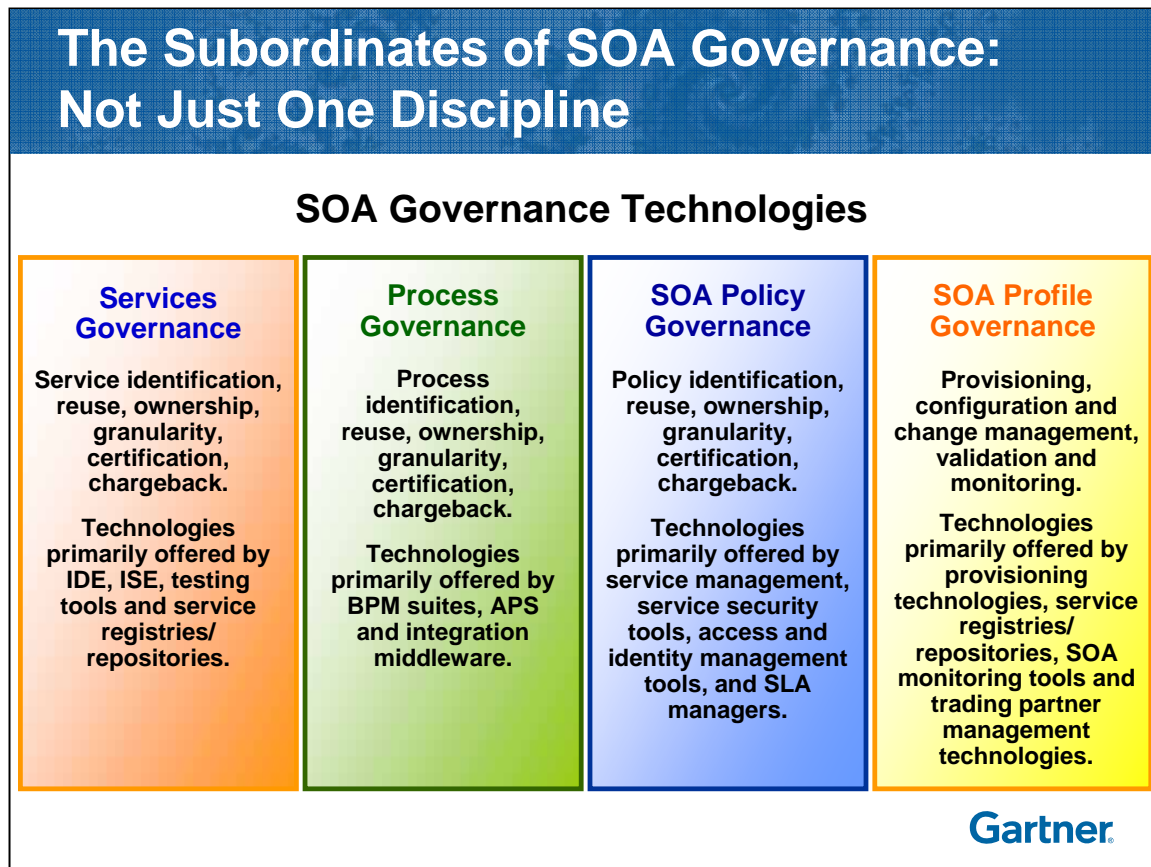
Technical and SOA governance should be part of your larger IT governance strategy.

Gartner

Key Issue: What technologies and methodologies should you have in place to ensure continued governance of SOA and Web 2.0 initiatives?

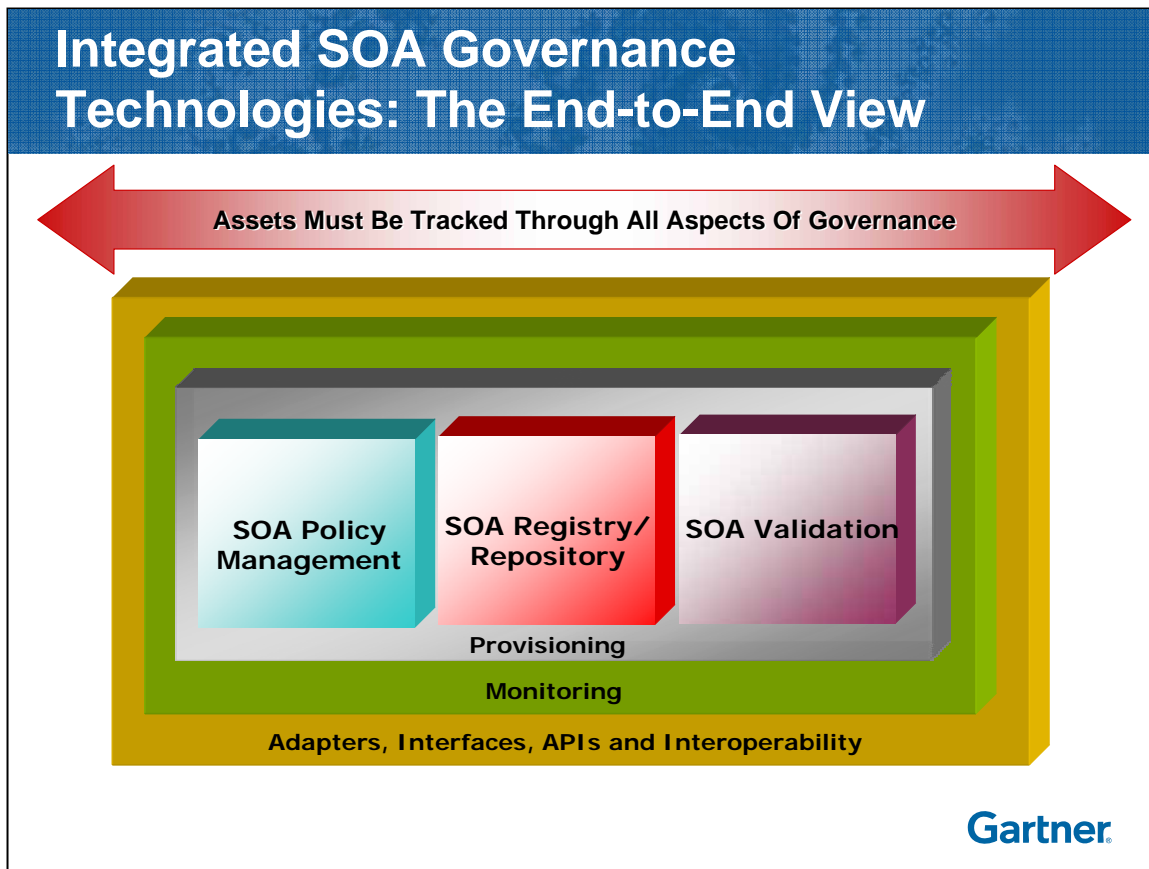
"Fill in the blank" governance continues to be an overloaded term that means various things to different people. Gartner sees governance as two very distinct disciplines around organization and technology. In other words, a company can organize for governance, create a strategy and use technology to enact that governance strategy. Key attributes of a governance strategy should include visibility, security, management (such as performance and availability), auditing, development, validation and composition. Each of these attributes has multiple technologies that can address them, such as registries/repositories, BPM suites, and validation and testing tools. Still, most of this is irrelevant if the organization hasn't formally defined policies to govern.

Tactical Guideline: Ensure that your existing integration and infrastructure technologies, such as BPM, can interoperate with governance technologies so relationships between all SOA artifacts and assets can be mapped and leveraged.



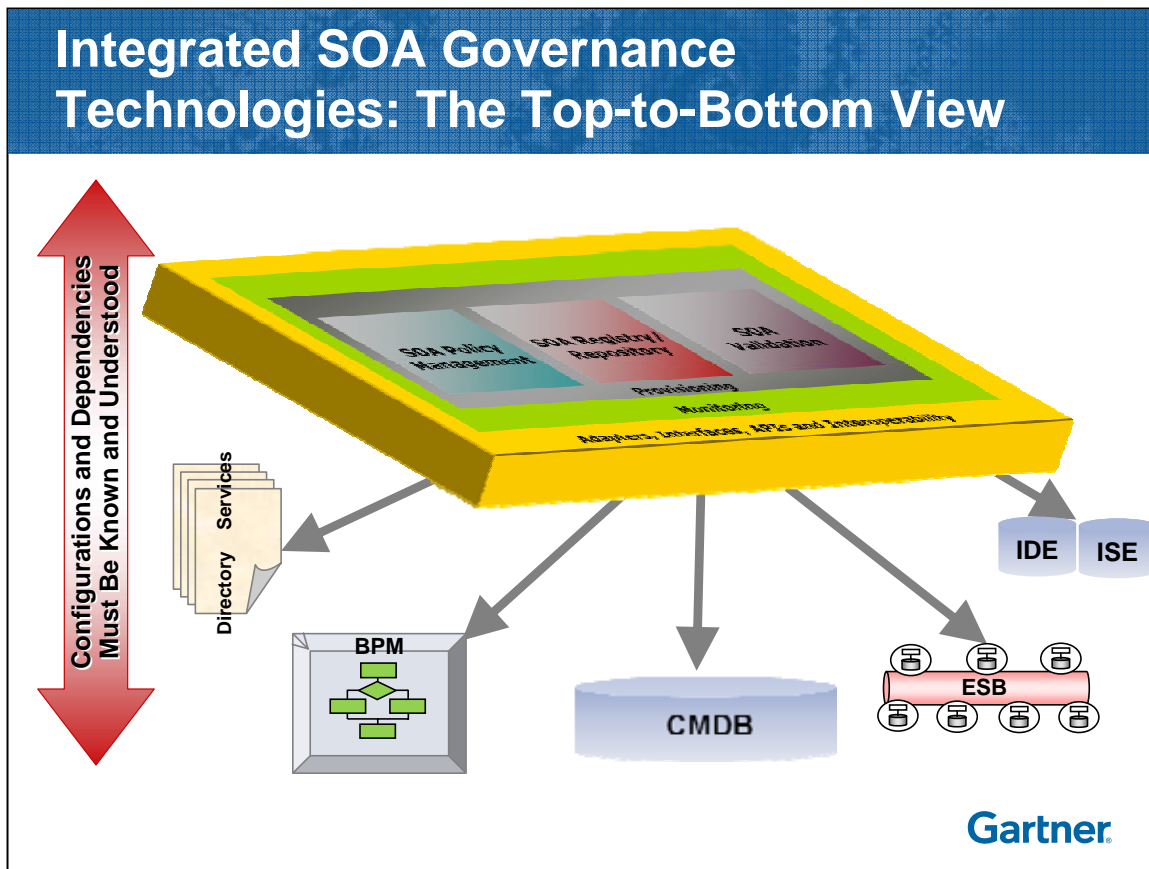
Key Issue: What technologies and methodologies should you have in place to ensure continued governance of SOA and Web 2.0 initiatives?

From a technology perspective — organizational issues regarding SOA governance is a broader subject — SOA governance has four very distinct subordinate disciplines. Each discipline has its own preferred technologies and life cycles that must be used and managed. Unfortunately, because SOA governance has been over-hyped and misinterpreted, many vendors supplying these technologies tend to focus on just one discipline. As a result, many enterprises consider their SOA governance strategies complete when, in reality, they have addressed less than 50% of the real challenge. The vendors can be held accountable as they have frequently ignored the importance of integrating or, at the very least, making their products interoperable with governance technologies such as registry/repositories, policy management and validation technologies.



Key Issue: What technologies and methodologies should you have in place to ensure continued governance of SOA and Web 2.0 initiatives?

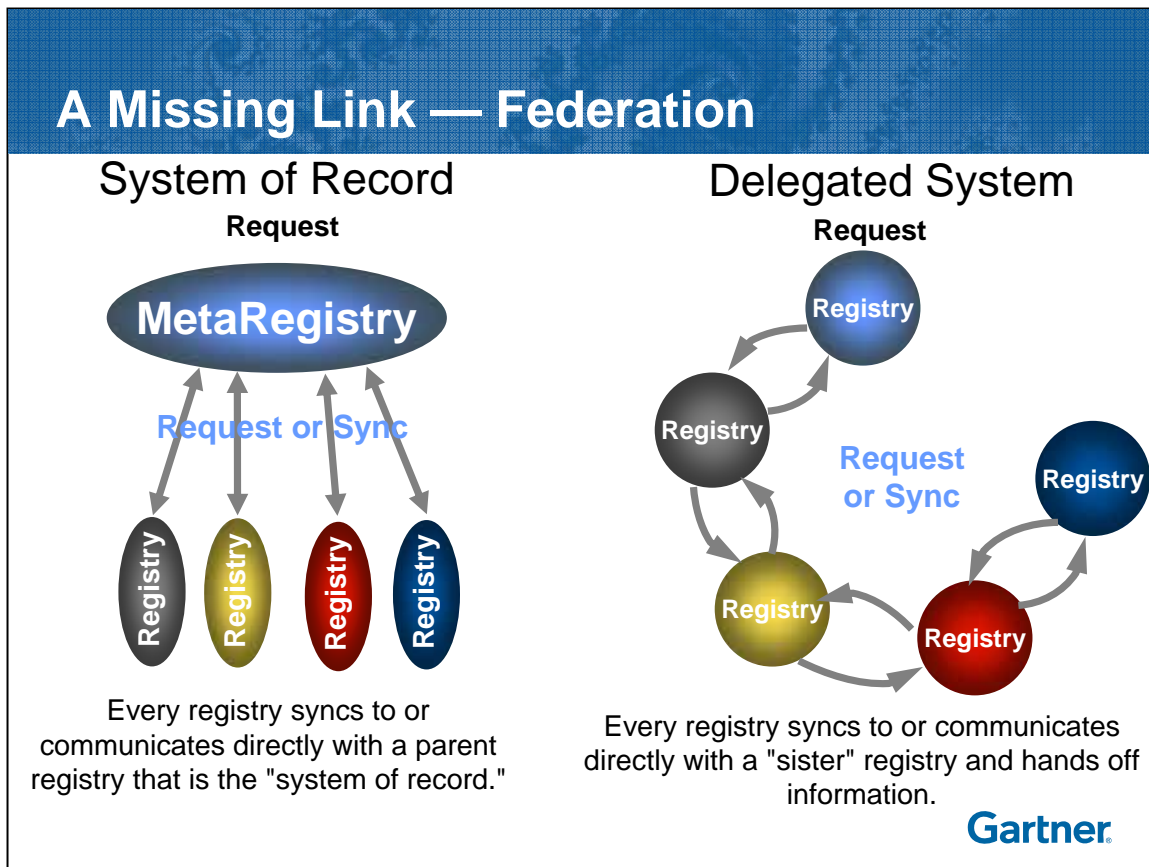
Managing the end-to-end life cycle of any SOA asset requires multiple technologies that are purchased together (in a deeply integrated offering) or separately with the ability to interoperate with additional governance technologies. These technologies include: SOA policy management, SOA registries and repositories, SOA validation technologies, monitoring and adapters, interfaces and APIs. Governance information about the asset, such as access controls and performance, must be shared with all the components, generally allowing the user to have visibility through the registry.



Key Issue: What technologies and methodologies should you have in place to ensure continued governance of SOA and Web 2.0 initiatives?

Consumers and providers of an SOA must understand the dependencies of their assets and resources. Frequently, these dependencies are outside the domain of the SOA and require configuration and dependency information be federated to the registry/repository for user consumption. Most of the major enterprise systems management and operations management vendors have invested heavily in centralized CMDBs, and the SOA should take full advantage of these databases and systems. Additionally, federation and interoperability must be present to operate with directories, metadata repositories associated with integrated development and service environments, as well as existing integration middleware such as ESBs and integration brokers.

Tactical Guideline: In lieu of standards for federation, use data synchronization technologies, such as ETL tools, to integrate metadata registry/repositories.



Key Issue: What technologies and methodologies should you have in place to ensure continued governance of SOA and Web 2.0 initiatives?

Federation is the cooperative agreement between autonomous entities that have committed to giving up some of their autonomy in order to work effectively in supporting a collaborative effort. Autonomy is not eliminated in this cooperation, but the federation requires planned interaction along with independent operation. For example: In a cooperative effort between lending institutions responding to a loan request, each credit agency, realty group and loan office must exchange information, reference each other's accounts and validate approvals. Although each of these entities can work independently of one another (that is, are autonomous) they work together in a planned and coordinated effort to approve or deny the loan. In this case, giving up autonomy means providing access to shared customer data and shared customer accounts. A federated registry is a collection of two or more autonomous registries that cooperate in support of location, design, and execution of software services and their associated metadata. Note that the federated registry is neither a single registry product nor a single database. Instead, it is a collection of registries working together. In order for any registry to participate in registry federation, it must either be reference-able by a registry that supports federation or it must support federation itself.

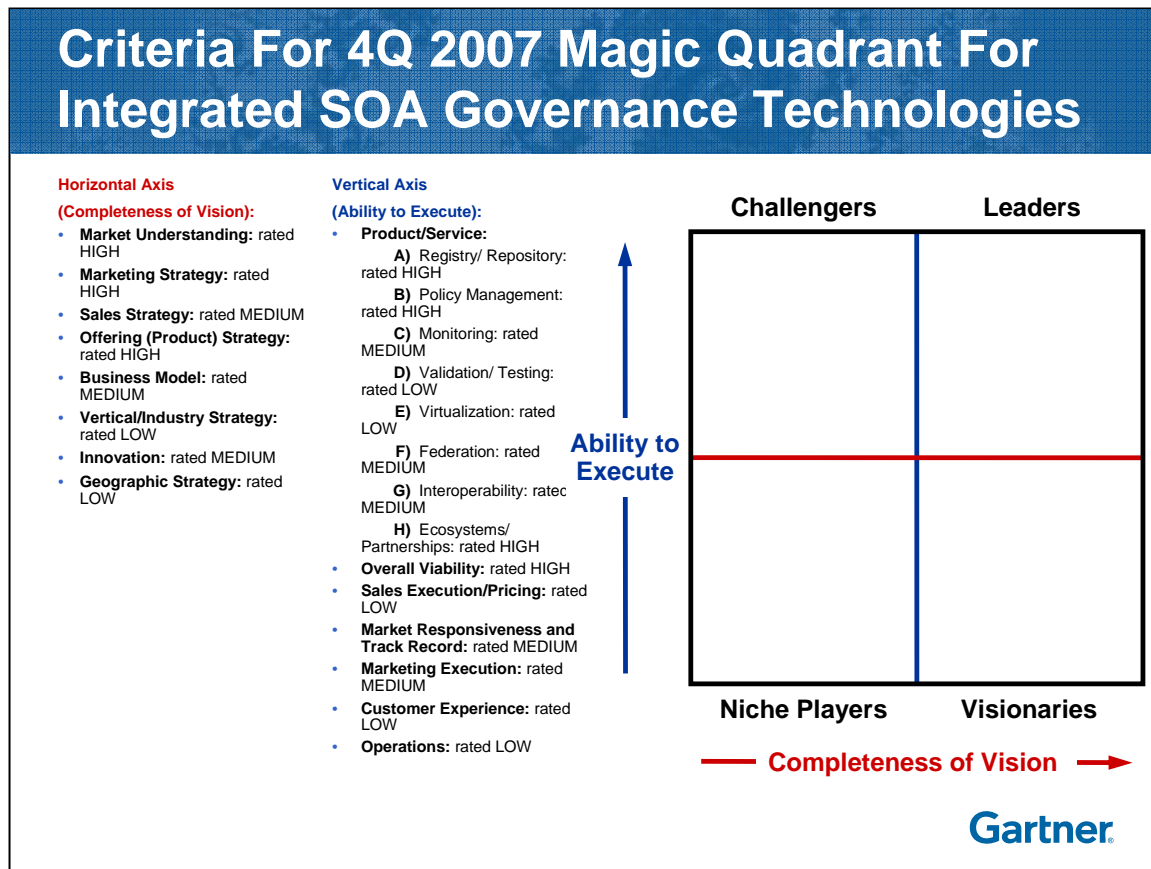
Strategic Planning Assumption: Through 2009, 60% of companies acquiring SOA governance technologies will choose best-of-breed solutions and choose to self-integrate them in house.



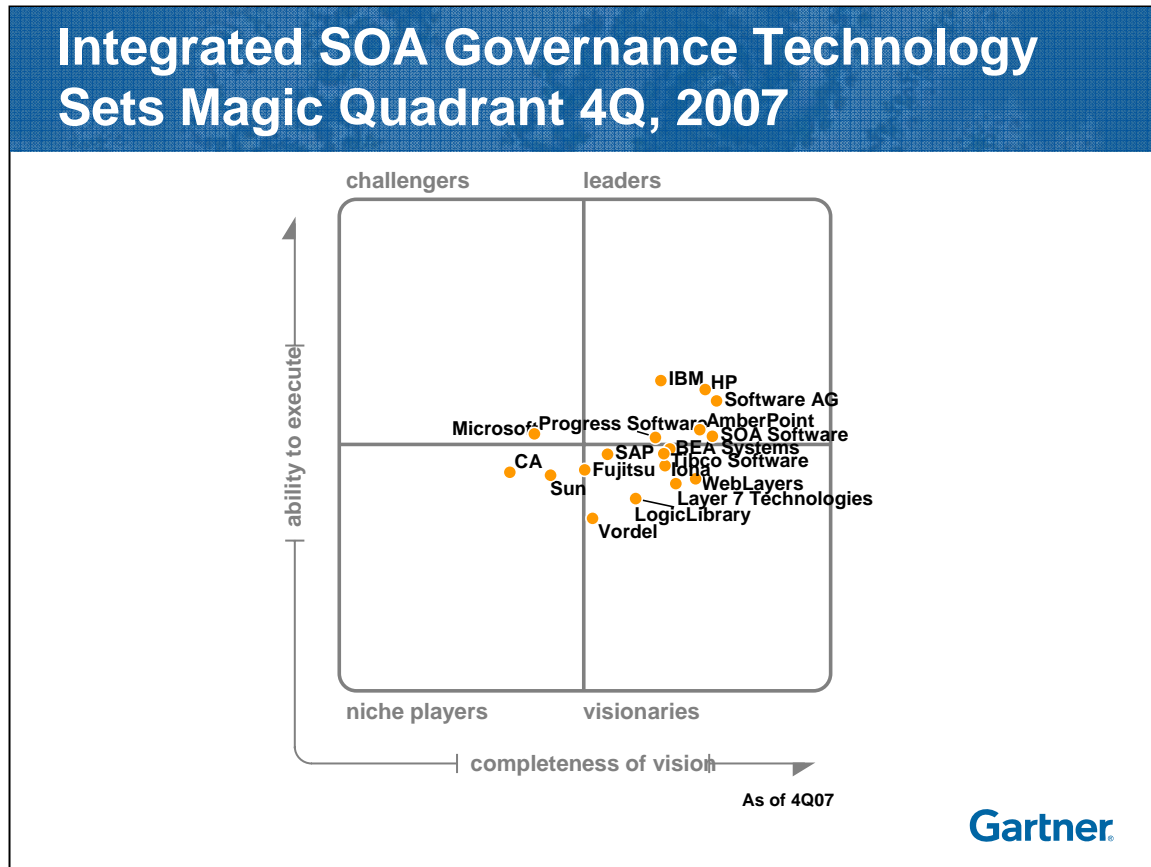
Key Issue: What technologies and methodologies should you have in place to ensure continued governance of SOA and Web 2.0 initiatives?

Adapters, interfaces, APIs and interoperability standards enable all the technical domains to communicate and share information, as well as enable the governance suite to be integrated with existing infrastructure applications, such as business applications, integration middleware or operating systems for optimal policy definition and executions. While it seems that users commonly seek the first three technologies listed above, the latter two are also essential for true end-to-end SOA governance. In fact, most vendors are committed to proprietary interoperability specifications such as: HP/Systinet's Governance Interoperability Framework (GIF), BEA/Flashline's SOA Partner Ecosystem, and Fujitsu and Software AG's joint venture CentraSite Community. It should be noted that in all the major standards around registries and repositories, there are no mechanisms for governance interoperability. Credit should be given to companies that develop and publish their own specifications, and enable any third-party vendor to interoperate, even though these specifications are very proprietary.

Key Issue: What are the vendors' approaches to SOA governance and Web technology governance?



The market for SOA governance is a varied one with many different types of products providing support for governing the behavior of an SOA. In short, SOA governance is about ensuring and validating that services within the architecture are operating as expected, and maintaining a certain level of quality. This Magic Quadrant reduces that market to one set of technologies with strong architectural cohesion (integration) promoting ease of use and interoperability of products. This integration includes the idea that multiple personas will be involved in governing an SOA. Each of these personas will bring a different perspective to the process of performing different kinds of tasks. However, all of these tasks must be part of a single governance effort instead of different, but related, efforts. We avoid use of the term "governance suite" because it is not representative of the actual product sets sold today. The majority of SOA governance technologies are not integrated into a single suite, but are provided from very different technology code bases. Policy management and enforcement engines seldom share the same integrated code base as registries and repositories. In addition, many of the features of SOA governance are being built into other SOA infrastructure offerings (such as Tibco, IBM and BEA) and, as such, do not constitute an independent suite in packaging or product SKU. However, the need to provide a set of governance functions in an integrated fashion, no matter what the original source of the technology feature, is important. Likewise, these technologies are not a platform, but are, rather, part of a larger set of integrated composition technologies designed for creating and deploying an SOA.



Key Issue: What are the vendors' approaches to SOA governance and Web technology governance?

Tactical Guideline: When looking for SOA validation technologies, examine solutions from your current provider of application testing. In some cases, they will partner with existing validation providers or provide a referral to one.

Web 2.0 and SOA Validation Approaches

The image displays three screenshots of SOA validation tools. The first screenshot on the left is for iTKO LISA Suite, showing a bar chart with green bars and a red line graph. The middle screenshot is for HP-Mercury Service Test, showing a complex interface with various panels and a red box highlighting a specific area. The third screenshot on the right is for Mindreef SOAPscope, showing a detailed view of a SOAP message with its headers and body. The Gartner logo is visible in the bottom right corner of the image.

Key Issue: What are the vendors' approaches to SOA governance and Web technology governance?

SOA validation technology is relatively new — in many cases being born from existing application testing suites. The differences between testing and validation are not trivial, however. Validating SOA artifacts by activity monitoring them and understanding their effect to and dependencies on other SOA artifacts and the SOA infrastructure itself will be exponentially more difficult given the increase in availability and use of composite application/service development suites. Vendors such as HP, iTKO and Mindreef all have solutions that address this functionality, but they validate artifacts differently. For instance, iTKO will validate using information from various sources, including policy management, registry and testing tools. HP relies heavily on their BAM, CMDB, registry and testing solutions, and Mindreef will employ third-party repositories and its own testing data to provide real-time validation. These three vendors have heavily partnered with other SOA governance technology vendors to address companies' needs for holistic integrated SOA governance technology sets.

Strategic Imperative: Most companies embarking on an SOA typically have disparate, multiple SOA initiatives, all requiring governance. Work to align the SOA governance strategy.



Key Issue: What are the vendors' approaches to SOA governance and Web technology governance?

Companies deploying an SOA tend to do so from three different approaches:

Process-centric: Companies who are looking to understand and formalize their business processes will tend to use BPM technologies to help them achieve insight in their processes. BPM suites enable users to govern the entire life cycle of the processes created within the suite. Business services become visible at this level and typically are broken down into a more granular set of processes.

Development- and Orchestration-centric: Companies who are looking to identify and reuse common services tend to use IDEs and ISEs along with governance technologies such as registry/repositories.

Application- and SOBA-centric: Companies with applications that have been service-enabled, or have SOBAs within their portfolio, tend to deploy service and security governance technologies along with registry/repositories to create visibility and management/security (particularly during runtime cycles).

Tactical Guideline: Many decision types (architectural, organizational, technical and strategic) are best taken by different groups of people, all linked to the ICC.

How To Pay For All This Technology



Top 5 Reasons To Love Your Architect:

5. They have the \$
4. They have the \$
3. They have the \$
2. They have the \$
- 1. They have the \$**



17

Key Issue: What are the vendors' approaches to SOA governance and Web technology governance?

As one would expect in a market that is maturing, more emphasis is being placed on procuring and deploying strategic solutions that can be used "across" multiple silos of the infrastructure. In many cases, the architect who usually manages the communication between the business and IT, has both visibility into the needs of multiple silos and influence into which technologies are considered and used. While system administrators and security specialists should always be consulted in any governance decision (both parties are integral parts of an SOA Center of Excellence and ICC), service management and service security technologies should be deployed within the context of a larger SOA governance initiative. Architects are increasingly at the head of those initiatives.

Recommendations

- **Today there is little or no need for additional governance technologies to enforce policies on your Web 2.0 deployments.** What you have today for visibility, security and performance will likely be enough.
- ✓ **On Monday morning**, consider your overall business model and ask yourself:
 - Are the consumers of my services getting what they expected from me?
 - How can I measure their satisfaction of what they are getting from me?
 - From the perspective of my consumer, could I be doing what I do better?
- ✓ **Then, on Tuesday morning**, take stock in your SOA and application portfolio. Then ask how many services are really running in your environment.
 - Any successful SOA deployment will need effective SOA governance mechanisms. How will you address:
 - Visibility?
 - "Audit-ability"?
 - Quality Assurance?
 - Manageability?

Gartner