Chapter 11

SOA Governance

In This Chapter

- Governing by the people, for the people
- Figuring out IT governance
- Governing SOA
- Getting ready for SOA governance

While a lot of organizations are starting to understand that service oriented architectures have the potential to transform the value of their IT assets, the ability to make SOA work comes down to governance. What do we mean by this? Well, in a broad sense, *governance* is just like it sounds — putting a consistent process in place to make sure there are checks and balances that ensure that the expected results happen. In the case of SOA, we're talking about keeping checks and balances between business and IT, between the business and government regulations, and between service and performance. Governance applies to human processes as well as software processes, and the consequences of failure are high.

The overarching principle behind governance is trust. All parties involved (the line of business managers, IT managers, software developers, business partners, and suppliers) must be able to trust that each party will execute its function to make the whole organization work according to established laws. Without governance, your SOA implementation will be a wild, untamed frontier. That isn't a very comforting thought, is it?

What Is Governance?

There are many ways to define *governance.* Governance comprises the organizing principles and rules that determine how an organization should behave. It is also interesting to note that *governance* derives from the Latin word for "steering." The idea of a process that focuses on steering is appropriate for

our discussion of IT and SOA governance. SOA is dynamic, changing constantly. Therefore, you never really get to the end of the road. You simply keep steering your company in the right direction. All the policies and procedures — as well as the tools and programs that enforce policies and procedures — form governance.

Governance gives organizations — whether they are countries, towns, or corporations — a structure to make sure the rules of conduct between constituents are followed for the good of everyone. Country, city, and state laws and regulations keep civilization moving in the right direction. Without a set of laws, countries would slide into chaos. Needless to say, governance is a necessary fact of life.

To understand SOA governance, think about the general notion of how a government works. In essence, governments operate on a variety of levels. Local governments, for example, handle issues that concern the town or city, whereas national governments deal with matters of concern to the nation as a whole. In concrete terms, this means that policies related to how often garbage is collected are handled at the local city or town level, while policies related to national defense are handled at the country level.

Likewise, within a corporation, some governance issues are handled at the departmental level, while other issues require the attention of the corporate management team. Governance defines who is responsible for what and who is allowed to take action to fix whatever needs fixing. Governance also sets down what policies people are responsible for and puts in place means by which one can determine whether the responsible person or group has, in fact, acted responsibly and done the right thing.

We didn't write this book to discuss your local, state, or federal government, so we're going to focus on governance within companies. Working under the assumption that a good question or two (or three or four) is as good a way as any to wriggle one's way into a topic, here are a few questions (and example answers) to ponder when trying to imagine how SOA governance issues affect your organization:

- **What are the core values that define your business?** *"Our company is devoted to transforming the way critical medicines are made available without refrigeration to developing countries."*
- **How does your business deal with its customers?** *"Our goal is to make each customer a reference. We aim to solve a customer issue within 24 hours of notification."*
- **How does your business deal with partners?** *"Partners are a critical part of our company's strategy. We treat partners as an extension of our own brand. We do not compete with our partners."*

- **How does the company ensure that it treats shareholders fairly?** *"Our objective is to make shareholders successful by empowering every employee to help keep the stock price as high as possible."*
- **How do you structure your company so that the business principles and rules put in place by management are followed?** *"Management will articulate to every individual in the company what our company's principles and rules are. There will be ongoing meetings and interactions to make sure these principles and rules are well understood by everyone."*

Clearly, every company has a philosophy for conducting business and a set of rules for how employees within that organization are supposed to act within that philosophical structure. Therefore, the idea of corporate governance is a complicated combination of rules and regulations. In recent years, governments across the globe have passed laws to make sure corporations comply with binding legal notions of correct corporate conduct.

Governing IT

This whole governance business is all good in theory, but how do you put these ideas into practice? Can you say "IT"? There isn't a company in the industrialized world that doesn't use software as part of the process of automating aspects of how it deals with customers, partners, and suppliers. Efficient companies have gone to great lengths to automate as many routine (and some not-so-routine) processes as possible. Therefore, corporate governance is tied directly to IT governance.

IT governance is the way people make decisions and tie business practices to IT systems. IT governance includes the techniques and policies used to measure and control the way IT departments make decisions about their systems and the way those decisions are implemented and controlled. But IT is not monolithic. Like its counterparts in government, some IT systems are centralized and controlled directly by the IT department, while other systems are designed and controlled by individual business units. Still other systems are designed and controlled by business partners. One of the big issues businesses face is the need to have consistency across the company in terms of the business principles and rules that are implemented. This is a very difficult task if each department works in isolation.

The SOA wrinkle in IT governance

When organizations begin to move away from easily governed fiefdoms of separate software toward creating reusable business services that will be

used by various constituents across an entire organization (and potentially beyond), it has a big impact on IT and corporate governance. Some rules and regulations apply in all circumstances, others don't.

Before you even start implementing SOA, you really need a SOA governance strategy. For example, say that you create a business service that calculates the commission structure for one product line. Just for fun, call this business service the *Sales Commission Calculation Service*. Your company now mandates that any time someone calculates a sales commission, he or she must use the *Sales Commission Calculation Service*. Within that business service are the business policies regarding commission rules, and it includes the process of paying big bucks that will have a major impact on the bottom line. It also must include any local, regional, national, or international regulations for appropriate business action (tax liabilities that are dependent on location, for example). As you can see from our little example, what is required here is more than a simple piece of code — it is the codification of business policy. The nature of IT governance changes as we move from coding to building services.

With SOA, organizations begin to change IT's focus from creating a single codified application to developing a set of business services that are loosely linked together. Therefore, *governance* takes on a whole different meaning. In essence, organizations must tie the integrity of those business services to corporate governance. As organizations create these services, they cannot be managed in isolation. For example, you can now combine the *Sales Commission Calculation* business service with a service that calculates the bonus for a salesperson based on seniority and performance level. In so doing, you suddenly find yourself in the brave new world of SOA governance.

Understanding SOA Governance

The previous sections in this chapter illustrate that SOA governance has a clear impact on overall IT governance. From an implementation perspective, SOA governance is a combination of policy, process, and metadata (data that defines the source of the component, the owner of the component, and who can change it). In many situations, an organization stores its definitions of rules within a registry so that everyone knows where to locate this important information. A SOA repository is a place where the organization stores information about what is inside each service. While the registry and repository are two separate SOA components, they are used in conjunction with each other.

Organizations that are experimenting might not put a lot of investment into their registry and repository. However, as companies begin to move from a pilot stage of SOA into real implementations across many different business

units, the registry and repository become important factors in both scalability and control of the environment.

At this stage, organizations need to look at both SOA governance and IT governance. SOA governance is about looking at a holistic view of the processes and rules for creating a business-services-driven approach to business. SOA governance is as much about organizational issues and how people work together to achieve business goals as it is about any technology.

In contrast, IT governance is about the details of building business services, ensuring that the rules and processes are implemented correctly, ensuring that each service meets technical standards, as well as ensuring that the right interfaces have been implemented in the right way. It looks at the tools and processes at every stage from the creation of business services through their use and transformations over time. IT is building services to be reused in many different situations. Therefore, the SOA technical environment must be dynamic; there will be constant change. New business services that codify the way the business operates will be created, and new rules will be applied. These reusable business services are linked together to create brand-new applications called *composite applications.* These services and rules will have to be tested and designed according to processes within the company. The environment must be designed to easily deal with changes, such as new business services, new security requirements, new partner-generated services, and new innovative processes.

Moving to the reuse of business services is the heart of SOA. Therefore, it's important to think about the business implications of managing those services. If you use a service once and it's incorrect (for example, the calculation of a commission is written as 7% rather than 5%), the company could lose some money, but someone probably will catch the mistake (hopefully sooner rather than later). Now, if 20 different departments use that same service, that 2% mistake compounds quickly. The loss will have a major impact on the bottom line. Now, add another ten business services to the commission business service and link them together. The consequences of a mistake are even greater. If the company is public and tells the market to expect a profit and the company loses money instead because of a bad business service, well, the consequences aren't pretty or nice.

To avoid this type of business disaster, SOA governance has to be a part of overall corporate decision-making process. You must have a method in place to define and verify each business service. You must have a process for both business and technical professionals at the corporate, departmental, and IT level to be involved. You must also have a process in place to measure how effective each service is in delivering value to the business. Later in this chapter, we give you some help in how to set about putting SOA governance in place. Just hold tight.

SOA, What's Different?

In the past, business units and IT took very different views of what governance was all about. Business unit management looked at its customer requirements, its business practices, and its strategies and then established policies and guidelines for its staff to follow. Likewise, the IT department created policies and guidelines for everything from programming techniques to security requirements. While both organizations may have been working on the same issues, they acted as though they were autonomous organizations. And then there was a whole different layer of governance at the corporate level, hovering above the individual business units and IT. With SOA, such parallel universes are no longer an option — policies and business practices that impact the entire company need to be decided at the same level.

In a traditional scenario, the business unit certifies a new business policy, getting the necessary sign-offs from upper management. It then approaches the IT department and asks that a certain application be developed or an existing application be changed to implement that new policy. At this point, the IT department takes over and applies its own processes to writing the necessary code. Often, that application is designed in isolation from other applications. In addition, the IT department is responsible for its own development, testing, and certification of the code. The IT department turns to the business organization for "acceptance testing." Often, this type of testing involves a group of users sitting at a system and trying the application. When business management signs off on the finished product, the contractual obligation of the IT department has ended.

With SOA, life gets a little more complicated. By moving away from isolated, self-contained applications and data, SOA makes it possible to reuse existing IT assets. So, a truly effective SOA governance must be put in place so that organizations have real control over these business services. You must let everyone involved know the status of those services, within both the IT department and the business units.

As a SOA implementation begins to mature, hundreds of business services will be reused across many different departments. Because so many organizations will depend on the validity and quality of a service, a process has to be put in place to keep track of changes to services. For example, there might be a business service that calculates a 30-year mortgage. Suddenly, the governance committee has decided that the technique for calculating the 30-year mortgage must be changed. If there are only a few reusable business services, someone can possibly pick up the phone and call the departments that need to know about the change. (Not necessarily the wisest way to go, but still feasible.) However, if there are hundreds of business services, picking up the

phone is a really bad idea. An organization needs a repeatable, documented process for keeping track of changes and informing all interested parties.

Remember that SOA requires a high level of trust. Each service needs to be so well constructed that anyone who needs to use that service can be confident that it will deliver the expected results. To reach this level of trust, there are a series of SOA governance steps you will need to put in place:

- **Establish a business services policy board made up of representatives of corporate, departmental, and IT management.** This board will certify that a service is the correct business practice and that it has been implemented in software correctly. For example, it will answer questions like these:
  - Is this the right way to process an order based on corporate practices?
  - Is this the way to calculate sales commissions?
  - Is this the way to calculate taxes on different products in different regions of the world?
  - Does the resulting code match the business practice?
- **Establish a programming standards board within the IT organization.** Many developers within IT organizations like to focus their attention on technique and cool new languages. Although mastering new skills and techniques is important, the IT department needs to focus on the use of SOA standards and the techniques for creating reusable business services. You need a peer review process so that IT serves the business in the most effective and predictable way.
- **Establish IT SOA governance best practices.** This is a combination of best practices and reality testing. For example, who is allowed to change a service? Who needs to be alerted if a service is changed? If a service is changed, does it have an impact on another service? How do you name a service so that its function is well understood by the business? Who decides which piece of code should become the standard service? How does the organization check the service for quality and performance? What is the process if something goes wrong? Who gets notified and how do problems get fixed? Without these checks and balances, SOA will not work.
- **Monitor the life cycle of services.** Because business services cut across technology, people, and processes, they require strong coordination between business and IT. Both business and IT must constantly monitor these services and their architecture to make sure that corporate governance standards are met.

The folks in IT are going to have their own (quite specific) set of obligations that they need to meet under SOA — obligations we summarize for you in this handy list:

- **Ensure the proper design of a service.** By *proper,* we mean insisting on a modular design process, consistent naming conventions, and standard usage of Web services interfaces.
- **Identify key implementation issues.** What do we mean by *key* here? First and foremost, IT needs to be vigilant when it comes to documenting how services are dependent on each other. IT also needs to create a reliable process so that an approved service is sure to be registered. It needs to create a consistent process for verifying the quality and integrity of a service, and it needs to come up with a consistent process for putting a service into operation. Finally, IT needs to implement a security strategy for ensuring that only the appropriate people and applications actually end up accessing services.
- **Monitor SOA services from a business perspective.** This is where all that talk about turning over a new leaf and working as *partners* gets tested. IT needs to create a consistent contract between itself and the business, and it has to establish an agreed-upon way to measure how successful the SOA implementation has been. In other words, IT needs to effectively track and report on results in a fashion that is comprehensible to the business side of things. And, after things are running (relatively) smoothly, IT needs to create a joint business/IT task force to implement a process for service improvement. (No more resting on one's laurels.)
- **Correlate your SOA strategy with regulatory requirements.** Regulations are as certain as death and taxes, so IT had better take on the responsibility of educating others on the way regulations are implemented in software. IT also needs to create a management process to monitor how software helps the company meet regulations. Finally, IT needs to put in place a well-documented process for ensuring that the right steps are followed throughout the lifetime of the software services.

It's very easy to get caught up in the technical details of implementing a SOA plan. SOA governance brings the focus back to the importance of the partnership between business and technology. Remember, the focus and objective of SOA governance is to identify the services that the business needs to conduct predictable and accurate business processes. When these are identified, it is the joint responsibility of the business and the IT organizations to meet the implementation goals. Therefore, you must have a centralized committee that focuses on the way the SOA life cycle works for the business. This committee needs to establish strategies for how IT policies are designed. It

determines how SOA components are managed and maintained and how to achieve quality of service. This is the foundation for the governance strategy.

When organizations move to SOA, they are creating a dynamic and heterogeneous world across many different constituents. Without SOA governance, SOA will not be trusted as a business computing model. Without SOA governance, SOA actually introduces risk to the business.

Therefore, if you intend to create a SOA strategy, begin with your SOA governance strategy. The first task force you set up should be around governance. This will be time and money well spent. With successful SOA governance, you will create quality, trustworthy services that will make the company more efficient and effective. It will also ensure that you meet corporate- and government-mandated standards.