



*PROACTIVE SOA SECURITY AND COMPLIANCE*

## **FIVE THINGS YOU SHOULD KNOW ABOUT COMPLIANCE, SECURITY, AND WEB SERVICES**

**A White Paper**

2208 Plaza Drive  
Suite 120  
Rocklin, CA  
95765-4404

**P** 916.783.6960

**F** 916.783.6970



## INTRODUCTION

In a growing number of industries, businesses are under increasing pressure to comply with regulations mandating data security and network integrity. Accounting scandals and well-publicized security breaches have angered consumers and legislators. As a result, businesses find themselves legally compelled to put in place rigorous enforcement and monitoring processes for access control, financial reporting, and permission marketing. Security regulations are continuing to multiply, and audits are becoming more frequent. As CIO Magazine recently noted, “Companies now view spending for compliance as part of the cost of doing business.”

At the same time that regulations are mandating tighter security and improved IT oversight, software architects, IT managers, and business managers are exploring new technologies, such as Web services and Service-Oriented Architectures (SOA). These technologies promise to increase business agility, to accelerate time-to-market, and to reduce IT and operational costs. An SOA solution replaces large, monolithic applications with configurations of smaller, re-usable software components that are designed and quickly assembled to meet the specific needs of a business offering or service. While an SOA can be implemented without Web services, in fact most SOA implementations today use Web services based on XML and HTTP. In large enterprises, Web services are most likely standards-compliant, SOAP-based Web services protected by technologies that comply with the OASIS WS-Security standard.

Are these two trends—increasing regulatory pressure and the migration to SOAs—related in any way? Do SOA security vulnerabilities make regulatory compliance more difficult? Or is the unfolding SOA revolution a golden opportunity for businesses to tighten controls over business processes and online services?

If you’re an IT manager, security professional, software developer, or QA tester working with Web services and SOAs, here are five things you should know about compliance, security, and Web services.

<sup>1</sup>“Sox Compliance Now Business as Usual,” Edward Prewitt, CIO Magazine, July 1, 2005.



**#1. Because Web services are loosely coupled and granular, they provide a better infrastructure for protecting confidential data and securing business processes than traditional, application-centric security approaches.**

A major West Coast financial services firm recently replaced its traditional LDAP-based identify management system with a new SOA-based identity management system. Why? Because the company recognized that the security landscape is changing. New business models, Internet applications, and mobile computing have effectively eliminated the network perimeter. To provide comprehensive security — security that is robust enough to withstand increased regulatory scrutiny — every application and every information asset must be identity-enabled. The best way to implement identity management on this grander scale was to adopt an architecture based on end-to-end business processes. As the company put it, they needed “to get identity out of the apps, into the business process.”

The company replaced its LDAP directory and update scripts with a new set of internally developed Web services, including a meta-directory service that manages updates. This new SOA-based solution decidedly improved the coverage and the accuracy of the company’s identity management functions. “Web services really work,” the company reported, surprised by the short learning curve and the easy integration offered by Web services technology. Since January 2004, the service has achieved 99.95% uptime.

This example offers a valuable lesson for other businesses, such as financial services companies, telecommunications companies, and healthcare organizations, that are facing the challenge of increased regulatory scrutiny. For these organizations, too, the best approach for strengthening security and reducing regulatory risks is use SOA to build security and compliance “into the business process.” Designing solutions for end-to-end business processes, rather than for intermediary client-server transactions, is the best way to ensure that data is always secure, wherever it happens to be in the course of a business transaction.

Organizations like financial services firms require a flexible software architecture, like that possible through SOA, in order to keep pace with growing lists of regulations. The analyst firm RedMonk notes:

*Enterprises are developing more and more software in house generally, and decreasing their reliance on packaged software or custom solutions.*



*“Leading with siloed applications may be adequate for initial, tactical compliance, but that approach introduces significant complexity and limitations over the longer term. The sheer variety and scope of compliance challenges require that IT organizations address compliance issues at an architectural level, using a fluid, adoptive approach. Organizations should deploy a services-based architecture that can deliver compliance specific services as necessary, based on specific acts and regulations.”*

Instead of taking the costly and cumbersome approach of addressing regulations in isolation, enterprises should deploy enterprise-wide security capabilities that can be applied to meet the compliance requirements of each department and division. The same authentication capabilities, for example, can ensure compliance with both Sarbanes-Oxley and Gramm-Leach-Bliley. Enterprises do not need to invest in regulation-specific solutions; rather, they can invest once in security building blocks that can be deployed and redeployed as necessary to comply with whatever regulatory requirements are in force.

Creating these building blocks within an SOA makes eminent sense, as the goal of an SOA is to deliver common, re-usable services that can be applied wherever they are needed. The SOA model is ideal for implementing broadly accessible components designed to ensure compliance in a cost-effective manner.

**#2. The best way to ensure that Web services are secure and compliant is to build security and compliance into Web services components and verify security and compliance during the QA process, before the services are deployed.**

Rather than relying on XML firewalls and other data center technologies to plug all the security holes in an SOA application, enterprises would do better to build security into their applications during the development phase. By systematically applying security policies and best practices and testing for the presence of common vulnerabilities, enterprise IT departments can ensure that the Web services deployed in the data center are already reasonably secure and policy-compliant. Production-stage technologies, such as XML firewalls, simply become an additional layer of security, rather than the sole bulwark against all attacks.

<sup>2</sup>“SOA Meets Compliance: Compliance Oriented Architecture,” RedMonk Study, Stephen O’Grady, August 12, 2004.



This proactive approach minimizes risks for four reasons. First, it minimizes the dependency upon firewalls and other defensive products; the software is protected, even if these products fail to block every intrusion or attack. Second, it makes Web services running within the network perimeter less vulnerable to attack from insiders—users who might not be blocked by outward-facing defenses such as firewalls. (Insiders are now responsible for 70-80% of attacks on enterprise networks.) Third, if the Web service is going to be shared with partners, customers, or other sites outside the control of the corporate IT department, built-in security minimizes exposures to risks caused by oversights and omissions in the data center security of those other organizations. Finally, by incorporating security and compliance testing into the standard testing and release process, enterprises can make security a reliable feature of every Web services release.

This proactive approach has one other major advantage: cost. According to Gartner, fixing a vulnerability in development costs only 2% of what it costs to fix that same vulnerability in production. That's a 50x savings for each vulnerability found.

To improve security while lowering costs, enterprises should test for security during development.

**#3. To test for security and compliance, QA teams and development teams need an automated software solution with built-in policy knowledge.**

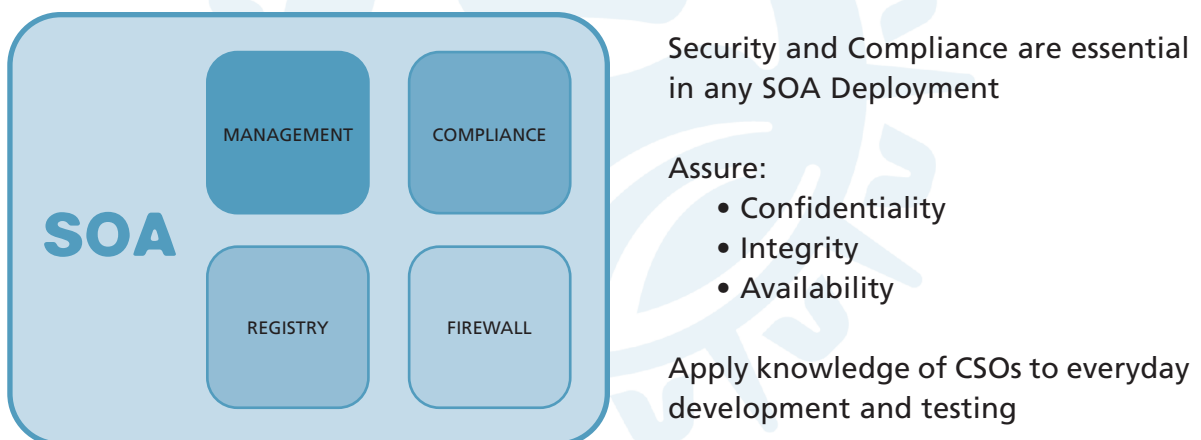
Any enterprise interested in promoting a security and compliance testing practice within its IT organization is going to face several challenges—challenges that can be overcome through automation and knowledge sharing.

What are these challenges? First, software developers and QA testers are not security experts, and enterprises cannot afford to train them to become security experts. Second, the security experts in the organization, such as the CSO, CISO, and his or her security team, have no way of systematically transferring their knowledge of software vulnerabilities and security best practices to the development team. Security policies may be scattered across written documents and email messages, but they are not encoded in a way in which they can be systematically applied and monitored in development and testing.



Enterprises need an automated framework that enables security experts to encode their knowledge in policies and rules that can be passed to development and QA teams in a reliable, usable format. This automated framework should take advantage of the domain knowledge of each group—security, QA, and development—without requiring security experts to become developers or developers to become security experts.

Automation offers several benefits. It makes it practical for IT engineers to take on new security and compliance testing processes without jeopardizing their commitments to other projects. It eliminates the errors and redundancies commonly found in manual processes. It scales to accommodating growing SOA implementations, supporting growth that hand-written testing scripts would be unable to accommodate. And, by minimizing manual work, it ensures that lack of manual resources doesn't become an excuse for companies deferring the adoption of a rigorous security and compliance testing methodology.



*Figure 1: Key components of any SOA deployment. In today's regulatory environment, security and compliance testing are essential as other SOA basics, such as Web services management products and registries.*

**#4. A security and compliance testing solution should be able to assess the effectiveness of the security building blocks required to keep information confidential and secure.**

While regulatory requirements vary from industry to industry and legislative act to legislative act, a few common security building blocks are common to just about all major industry regulations. For example, these capabilities are common to almost any security solution to achieve compliance:



- a. Authentication
- b. Encryption
- c. Resilience to attack

For example, the Gramm-Leach-Bliley (GLB) Act compels financial institutions to implement security measures to protect the confidentiality of consumer data. At any financial institution, these security measures will involve access control measures involving authentication, authorization, and data encryption. Only users who present valid IDs should gain access to consumer data, and consumer data should be encrypted whenever it's exposed to public networks or other potentially hostile environments.

The Health Information Portability and Accountability Act (HIPAA) compels all health care organizations (HCOs), including payers such as insurance companies and providers such as hospitals, to protect patient data through a variety of security measures, including authentication and encryption.

GLB pertains only to financial services companies, and HIPAA pertains only to HCOs, but, in each industry, organizations are likely to turn to the same security technologies to achieve compliance. Top-down security policies, authentication controls for networks and applications, identity management, and encryption are the obvious solutions for compliance in both these industries.

To a large degree, the success of any compliance technology is going to depend on its ability to implement and assure these core, building-block security measures.

Any compliance assessment solution for SOA, then, should include tools for testing these building blocks. Is consumer data encrypted when it traverses the network? If a specific business service requires authentication, are authentication measures being enforced? Does a portal withstand common attacks? By enabling developers, QA testers, and compliance officers to answer questions like these, a Vulnerability Assessment and Policy Compliance solution provides the visibility that organizations need to assess their risk exposures and measure their compliance efforts.



## **#5. Once Web services are deployed in production, test for security and compliance again, using the same policies and automated test solution.**

It's most cost-effective to test for security and compliance while Web services are still being developed. But to ensure that no new vulnerabilities are introduced by gaps in change management or on-the-fly configuration changes, enterprises should regularly test Web services in the production stage, as well.

The automated security and policy compliance testing solution used for development-stage testing should support production-stage testing, as well. Obviously, when a CSO or other security professional defines a security policy to be followed in development, that same security policy should be applied in production. Vulnerability profiles and other test metrics used in development should also be applied in production-stage testing.

Using the same testing solution for both development-stage testing and production-stage testing saves money by eliminating the need for an IT organization to invest in parallel but separate security and policy compliance testing solutions.

But there's another advantage, as well. Administrators and compliance officers can more quickly discover vulnerabilities and exposures if they can compare test results across lifecycle stages. If security tests that passed during development suddenly fail in production, the IT department knows that a potentially serious change has occurred. They can then use the knowledge they gained from their development-stage testing to find and fix the problem quickly.

## **CONCLUSION**

We're at a turning point for Web services. Analyst firms agree that over 75% of enterprises now have Web services projects under way. Web services have become essential business technology for companies such as Amazon.com and eBay, and organizations such as banks are busy rewriting their online applications to run as Web services. We can expect to see Web services gain even more momentum in 2006. Bill Gates' recent endorsement of Web services business models is simply one more spark for the kindling.



We can also expect to see regulatory enforcement organizations, such as the SEC and the FTC, continue to scrutinize corporate operations and punish wrong-doers. Regulatory oversight is not going away by any means. Many regulations require organizations to monitor their own progress and to continually improve their performance. It's likely that in 2006 and 2007 auditors will look for tangible signs of improvement. Putting compliance and monitoring practices in place might suffice for Year 1. But by Year 2 or 3, progress should be able to be measured. Auditors will be looking for reports and quantifiable results.

Enterprises can take advantage of SOA to make themselves more nimble while rising to these regulatory challenges. SOA enables enterprises to invest once in compliance and to have that investment pay dividends for every regulatory challenge they face.

At the same time, enterprises need to recognize that the public interfaces and new technologies of SOA pose serious threats to network security. Gartner estimates that Web services will re-open roughly 70% of the security holes that firewalls and other security products have closed over the past decade. So, enterprises must take SOA security shortcomings seriously and build security and compliance into every Web services component they deploy.

Even Web services pilot projects should be built with security in mind. It's a mistake to assume that services deployed within the firewall are safe. The majority of security attacks now originate with insiders, including disgruntled employees. Pilot projects need to be safe from these "trusted" users.

Pilot projects also provide an opportunity for enterprise IT teams to test and to develop the security and compliance mechanisms they will deploy along with their production Web services. Rather than assuming that mature, foolproof security and compliance mechanisms can be developed on the spot when Web services are ready to deploy, IT teams should design, implement, and assess these mechanisms along with the Web services they are designed to protect.

New SOA security and compliance solutions offer enterprises the tantalizing opportunity to finally apply the knowledge of CSOs to the daily work of developers and testers, without overburdening developers and testers with the rote learning of policies and enforcement busywork.



What can developers do to lead in these efforts?

- If your development team isn't already exploring SOA, start now. The technology is mature enough to offer real benefits. Survey results make it clear that your partners and customers will likely expect you to be delivering Web services soon.
- Work with your organization's CSO and security team to identify the common security requirements of the industry regulations that apply to your organization.
- Design and implement Web services that act as "security building blocks," providing these common security services, such as authentication, encryption, and so on.
- Ensure that all new business services and SOA applications incorporate these "security building blocks."
- Invest in an automated testing framework that enables CSOs and security professionals to define policies (using assertions such as those in the WS-Policy standard), which can be automatically translated into test suites for use in development and QA.
- Make security assessment and compliance testing part of development. End users want to buy products and services that are secure out-of-the-box. The best way to create these products and services is to make security an intrinsic part of software design and development.

Through SOA, developers have an opportunity to play an important role not just in creating new applications for end users, but also in helping their organizations meet their regulatory requirements. It's an exciting opportunity and one that developers should be sure not to overlook.



## ABOUT KENAI SYSTEMS, INC.

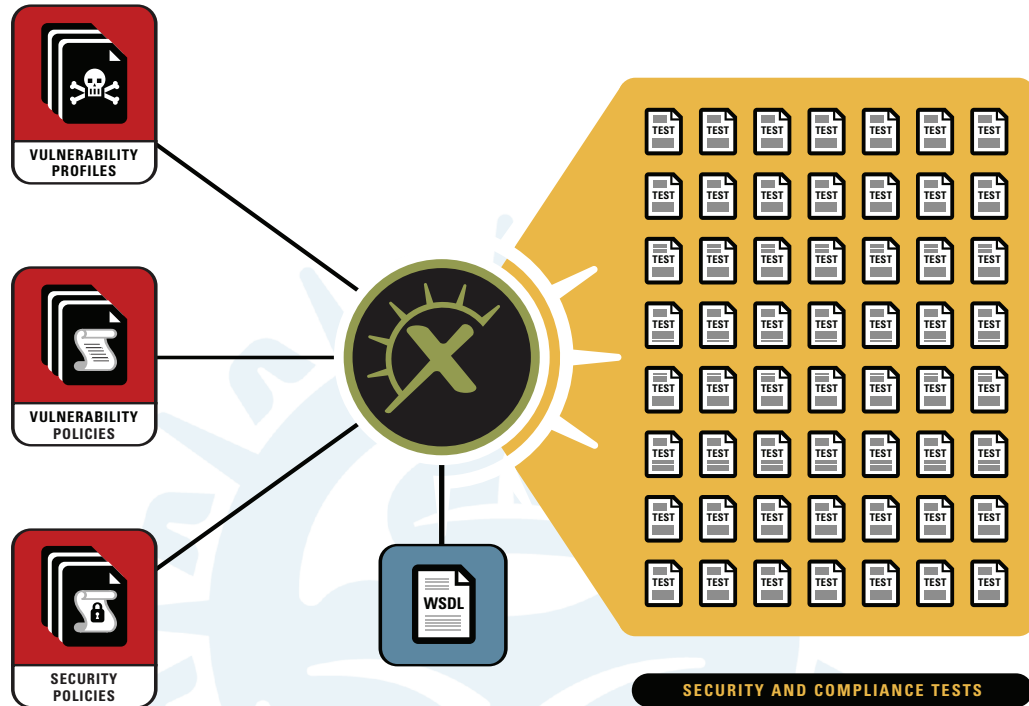


Figure 2: The Kenai eXamine solution automatically generates security and compliance tests based on vulnerability profiles, vulnerability policies, security policies, and WSDLs.

Kenai Systems is a leading provider of vulnerability assessment and policy compliance solutions for Web services and SOA. Kenai's solutions enable businesses to identify and to mitigate security vulnerabilities and compliance failures before they jeopardize mission-critical operations.

**Kenai's flagship product, eXamineSOA Enterprise, delivers proactive SOA security and compliance in a cost-effective, easy-to-use solution that fits into the development and testing environments enterprises have already deployed.** A cross-departmental solution, eXamineSOA Enterprise leverages the expertise of security professionals, QA engineers, and development teams, and systematically applies the domain knowledge of each group to the assessment and elimination of SOA vulnerabilities. CSOs and security professionals use eXamineSOA Enterprise to define security policies and best practices and associate them with specific SOAP-based Web services. QA engineers and development teams use eXamineSOA Enterprise to automatically generate and run tests for security and compliance while SOA components are still



in development, pre-empting vulnerabilities that can jeopardize IT security and trigger policy violations. eXamineSOA Enterprise's reporting capabilities provide IT departments and management teams with unprecedented visibility into the state of the organization's SOA security and compliance. With Kenai eXamineSOA Enterprise, IT departments and security teams gain centralized control over and visibility into SOA security and compliance practices, enterprise-wide.

For more information about Kenai Systems' eXamine product family, call +1 (916) 783-6960 or visit [www.kenaisystems.com](http://www.kenaisystems.com).



*Copyright 2005 Kenai Systems, Inc. All rights reserved. Kenai, Kenai eXamine, Kenai eXamineSOA Enterprise, and the Kenai Systems logo are trademarks of Kenai Systems, Inc. All other trademarks are the property of their respective holders.*