SYS-CON

THE WORLD'S LEADING MAGAZINE DEDICATED TO WEB SERVICES TECHNOLOGIES

SOA Web Services JOURNAL

JULY 2006 / VOLUME: 6 ISSUE 7

Managing SOX in the Age of SOA

Policy-Based Version Control for SOA Services

Formalizing Middle-Tier Data Management

The Performance Woe of Binary XML

XML Compression and its Role in SOA Performance

PLEASE DISPLAY UNTIL SEPTEMBER 30, 2006

$6.99US $7.99CAN

07>

0 71486 03420 9

Managing SOX in the Age of SOA

Rethinking internal controls

WRITTEN BY **HUGH TAYLOR**

Service Oriented Architecture (SOA) is at the heart of many major IT initiatives and vendor offerings. However, while SOA has the potential to deliver business value through streamlined application integration, as well as integration with partners and suppliers, the open nature of SOA has the potential to cause problems with Sarbanes-Oxley compliance. This article will look at compliance issues inherent in developing an SOA. Using a practical example, we'll examine COSO Control Objectives, Risks, and their supporting IT systems from the perspective of Sarbanes-Oxley compliance.

This article is meant to help IT professionals, corporate managers, and auditors understand two complex and interconnected sets of activity in the world of corporate computing: Sarbanes-Oxley (SOX) and SOA. Both SOX and SOA are emerging as major areas of focus – some might say distraction – for a growing number of people involved in information technology, management, and audit.

Familiarity with the origins and intent of the law will help you understand why the Sarbanes-Oxley Act is relevant to IT professionals at a public company. Congress passed SOX in 2002 to calm the financial markets after Enron, Adelphia, and Worldcom. To assure investors that the financial statements that public companies make are accurate, SOX expanded the reporting and disclosure requirements concerning their internal financial controls, the process, practice, or structure designed to provide a reasonable assurance of the reliability of financial reports.

Internal controls can be either *preventive* or *detective*. A preventive control prevents fraud or errors that can result in a misstatement of financial results. A locked cash register is a simple example of a preventive control. A detective control enables an accounting staffer or auditor to check to see if a financial statement, or a supporting piece of data for a financial statement, is correct. Bank statement reconciliation is an example of a detective control.

SOX Sections 302 and 404 mandate that a public company documents and tests its internal controls. Management must then certify that the company's internal controls are effective. Then, an external auditor must also test and certify them.

The Public Company Accounting Oversight Board (PCAOB) has directed public companies to adhere to the internal control framework known as COSO in their SOX 404 compliance. The COSO framework pairs risks with control objectives and control practices to provide a level of confidence in a company's internal controls. If they are not effective, the company must disclose the deficiency, which can cause problems with the SEC and others.

If you're involved in IT and SOX then you should understand that you're working on showing that IT supports the COSO control objectives intended to mitigate the risk of financial misstatement. The purpose of your work is to help the company comply with SOX 404 and 302 by establishing, documenting, and testing the effectiveness of IT systems that support COSO Control Objectives.

IT's Place in Internal Controls

Because so much of business today is done using computers and software, IT plays a prominent role in internal controls. Underscoring that point, Gartner reports that 97% of the material weaknesses in internal controls can be mitigated through IT. In practice, there are two essential ways that IT finds a place in internal controls:

1) The IT General Controls as recommended by COSO
2) IT as a component of a non-technological internal control over financial reporting (often an application-level control)

Now we'll look at each of these categories using the example found in Figure 1, which depicts the IT architecture used by a public company. It shows the systems and software applications necessary to process inbound, revenue-producing transactions. While the corporate general ledger system is responsible for financial reporting, much of the supporting data regarding the transactions and inventory comes from two connected systems: A mainframe-based warehouse management application and a customer portal.

IT General Controls

There are numerous IT General Controls. To stay focused, we'll only look at one example – "Control Objective: Controls provide reasonable assurance that financial reporting systems and sub-systems are appropriately secured to prevent unauthorized use, disclosure, modification, damage, or loss of data."

With regard to this control objective, in the context of the architecture shown in Figure 1, the internal auditor would have to document and test the effectiveness of the internal controls that secured that architecture. Specifically, the internal controls would have to prevent unauthorized access to the General Ledger system, the Warehouse system, and the Customer Portal. The internal control would have to establish rigorous password protections, firewalls, hardening guidelines, and so on to assure the auditor that the systems in question were "appropriately secured." We'll return to this point later when we introduce the idea of Service Oriented Architecture.

IT Supporting Non-Technological Controls

Many internal controls over financial reporting are not technological in nature. For instance, subjective valuation of some balance sheet assets usually involves manual processes. However, many of them rely on IT for their effectiveness. Using the COSO framework, an internal control for the company depicted in Figure 1 might look like the pairing of control objective, risk, and control practice shown in Table 1.

Following the COSO framework virtually all internal controls are expressed in the format shown in Table 1. Of course, in reality the details might be different or more specific in any given situation, but the principles apply. Internal controls over financial reporting set out a control objective intended to mitigate a risk using a control practice.

Although the internal control described in Table 1 is procedural in nature, and may in fact be entirely manual, it's likely rooted in IT. In our Figure 1 example, there must be a reasonable level of certainty that the general ledger system is receiving accurate, timely data from the warehouse system and the customer portal. The IT department may be called on to document and test these technological factors that support this procedural control.

Problem Scenarios

If the control isn't effective, the company faces a risk that the control objective, "Accurately record invoices from all authorized shipments" won't be met. If this control is deficient to the point that it could cause a material misstatement of financial results – a "material weakness" in internal controls – then the company could be in real trouble. If a public company discloses a material weakness in internal controls under SOX and fails to remedy it, consequences can include SEC investigations, sanctions, and even delisting from exchanges.

Let's look at an example of what could go wrong. Material weaknesses usually manifest themselves in fraud. Consider the practice known as "channel stuffing." Channel stuffing involves creating bogus revenue by colluding with customers. To earn a high bonus, an executive might ask a customer to place a large order on December 28. The revenue is booked for the year, but on January 2, the goods are returned. This device might seem obvious, but it happens all the time and it can be quite hard to detect or prevent in a large, complex organization.

If the company doesn't have effective internal controls over invoicing and inventory and the IT systems that support those controls then it's more vulnerable to the risk of channel stuffing than it would be if it had robust controls. The channel-stuffing example also highlights one of the key principles of internal controls over financial reporting, which is the segregation of roles. It's usually required that one individual, such as a salesperson, can't be able to book a sale, take possession of the merchandise, request shipping, and book the revenue into the general ledger. A fraud such as channel stuffing is much harder to prevent or detect if role segregation isn't practiced as one of the internal controls.

Consider then, what happens, when the architecture is opened up as an SOA.

Internal Controls in a Transition to SOA

If the company described in Figure 1 transitioned to a Service Oriented Architecture (SOA), its IT architecture would resemble the one shown in Figure 2. What's different? Well, where before the company relied on a proprietary interface to connect its systems with one another, they can now exchange data and operating instructions using the open standard of Web Services. The company has also taken advantage of the universal "machine to machine" interoperation capability of SOA and enabled its customers to have direct programmatic access to its ordering systems. Instead of a portal, the company now has a Customer Web Service hub to which customers can connect directly using their ERP systems.

Control Objective	Risk	Control Practice
Accurately record invoices from all authorized shipments.	Missing documents or incorrect information.	Invoiced amounts are properly recorded as to account, amount, and period.

Table 1: Control objective/risk/control practice pairing

SOURCE: INTERNAL CONTROLS PRIMER. KARL NAGEL & CO.

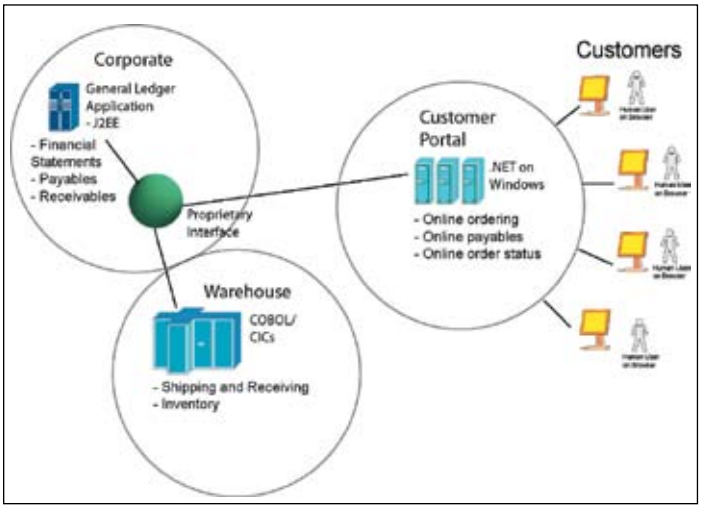

Figure 1: A public company's enterprise architecture for outbound transactions (revenue)

SOA's Impact on Internal Controls

While SOA may be a boon to business executives owing to its inherently flexible nature, this new architectural paradigm can cause difficulties for the IT side of SOX-mandated internal controls. There are several major areas of concern outlined below.

A New Level of Openness

Because an SOA is built on open standards, it can expose critical data and application functionality to a vast new array of users. Any effective set of internal controls over financial reporting that relate to applications in an SOA must take this new level of openness into account. In the example shown in Figure 2, the internal controls must consider the risks inherent in exposing the data in the warehouse system, general ledger, and customer hub to unauthorized access. For example, a SOX auditor may want to test the controls over the integrity of inventory documents that support the inventory asset figures in the company's balance sheet. To certify that the control is effective, the auditor will probably want to see documented evidence that access to the software that generates these inventory reports is restricted to authorized personnel. The open nature of SOA creates the added challenge of establishing and testing this kind of internal control.

Machine-to-Machine Security

The fact that Web Services, the fundamental building blocks of most SOAs, are based on machine-to-machine interactions creates another internal control hurdle for IT professionals involved in SOX compliance. While not a revolutionary shift, the machine-to-machine nature of SOA changes the nature of many existing internal controls that assume that the user of a given application is a person.

Many standard internal controls in place today involve the authorization and authentication of specific individuals and their right to access financial applications and modify the data in those applications. In the age of SOA, the focus has to change to accommodate the reality that many of the new "users" of financial applications are in fact other applications that can't be authenticated or authorized using a traditional identity store or access management system.

In the example shown in Figure 2, the shift to SOA has changed the nature of the customer's interactions with the company. Before, specific individuals could log onto the customer portal and transact business with the company. Internal controls related to revenue recognition, as depicted in Table 1, were based on a process of authenticating and authorizing those individual users against an identity store that was under the company's control. In the new SOA, the "users" of the customer hub are actually the customers' ERP systems. There are people using those ERP systems, of course, but there has to be a way for the company to authenticate and authorize those users before granting access to financial applications that have been exposed as Web Services. If there is no such authentication or authorization going on, then the open access to financial systems by unknown persons working through an ERP system at another company would probably result in an internal control deficiency.

Segregation of Roles

Segregation of roles is a core technique of internal controls over financial reporting. Continuing with the machine-to-machine authorization issue described in the previous section, note that it may be impossible to establish clear role segregation in an SOA. Why? If the "user" of a Web Service-exposed financial application is actually another application, but the internal controls use role-based authorization for a human user, then the control will be deficient.

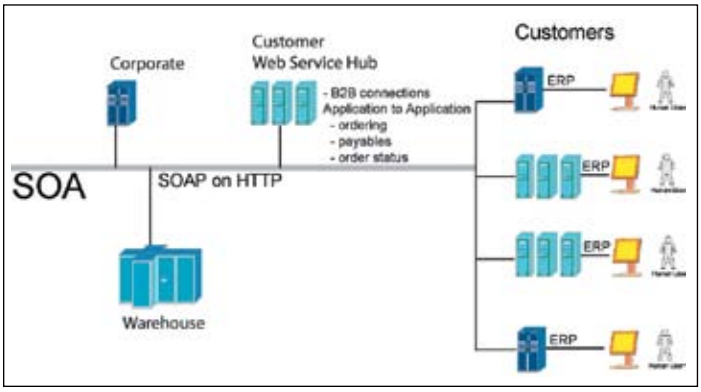

Figure 2: Transition to a Service Oriented Architecture

For example, in Figure 2 a sales rep shouldn't be able to access the general ledger and create a sale that would give him a bonus or access the warehouse system and move inventory around. The potential results of such role-based control lapses are error and fraud. If the sales rep can access those systems using a Web Service-consuming application on the SOA that doesn't authorize him directly, then there can be trouble. In the transition to SOA, those responsible for internal controls involving financial systems need to evaluate whether or not they are addressing the potential for deficient control over authorization and role segregation.

No Perimeter Emphasizes Application Controls

Overall, the move to SOA puts greater emphasis on application level controls than may have been required in a conventional IT architecture. While many of the IT general controls focus on the perimeter – firewalls, network access, passwords, baseline standards, and so on – the SOA renders much of perimeter security irrelevant. If access to critical financial applications is open to direct use by virtually any application in the world, then the perimeter is necessarily less significant as a component of an internal control practice.

Conclusion

Service Oriented Architecture requires some rethinking of internal controls over financial reporting. In terms of IT general controls, SOA changes some of the underlying assumptions that exist today, including the importance of the perimeter and the role of individual users versus machine users of critical applications. For IT systems that support non-technological internal controls, the transition to SOA should stimulate analysis regarding access rights, segregation of roles, and integrity of data.

The good news is that SOA represents an incremental shift in the IT aspects of internal controls and Sarbanes-Oxley compliance. SOA is not a categorical revolution in technology that shatters previously understood notions of internal controls.

However, one thing should be clear: A poorly governed SOA could easily result in deficient internal controls and problems with Sarbanes-Oxley compliance. ■

About the Author

Hugh Taylor is vice president of marketing communications at SOA Software, the provider of management and security solutions for enterprise Service Oriented Architecture. He is the co-author, along with Eric Pulier, of Understanding Enterprise SOA *(Manning, 2005) and* The Joy of SOX *(Wiley 2006). The author of more than a dozen articles and papers on the subject of Web Services and Service Oriented Architecture, Hugh is an authority on business process management, SOA, and compliance issues. He got his BA, magna cum laude, from Harvard in 1988 and his MBA from Harvard Business School in 1992. He lives in Los Angeles.*
hugh.taylor@soa.com