Achieving Sarbanes-Oxley Compliance with Oracle Identity Management

An Oracle White Paper
September 2005

INTRODUCTION

The Sarbanes-Oxley Act of 2002 requires corporate executives to provide and ensure an increased level of financial and operational discipline. To comply with this law, most large corporations are now implementing a variety of new measures that cross financial reporting and processes, as well as internal business operations. This short paper describes how Oracle Identity Management can help ensure compliance with Sarbanes-Oxley (as well as other regulations) while increasing ability to monitor and audit compliance on an ongoing basis.

INTERNAL OPERATIONAL CONTROLS

Section 404 of Sarbanes-Oxley requires companies to define and enforce effective internal controls over business operations. While the Act does not define these controls in any detail, significant effort has been made to guide organizations as they create and deploy these controls. Operational controls span the entire business, beyond the purely financial transactions. While information technology is not a cure-all, IT can certainly help enforce and audit many internal controls.

At the core of many controls is the notion of rights; what are the rights a particular manager has, and are those rights in line with new internal controls? One common internal control relates to separation of duties. For example, a corporate manager who has rights to create a new purchasing order might be required not to have rights to create a new approved vendor. By separating these two duties, the desired effect is to prevent any manager from diverting business to a friend's company.

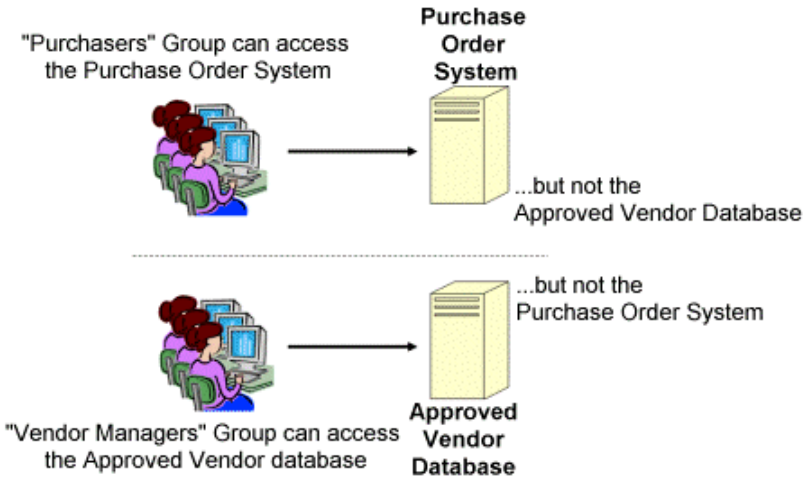
However, while many of these controls are straightforward to define in abstract, enforcing and auditing these becomes difficult in practice. Most corporations struggle to govern interactions between people and applications effectively, to enforce internal controls and to audit rights and responsibilities.

INTERNAL CONTROLS AND PEOPLE

Controls Affecting Employees

Of course, the most common view of Sarbanes-Oxley compliance relates to people: Who can access which systems and data, what can they do with those systems, what happens when I grant Person X this right, and what happens when Person Z is transferred? To further match internal controls with actual business operations, many companies deploy an identity management system. By defining roles and groups, then assigning or revoking rights to those roles and groups, companies can show and enforce internal controls and separation of duties in practice.

For example, a firm might create a dynamic group called ***Purchasers***, with the rights to access the Purchase Order Management system. The firm might also create a group called ***Vendor Managers***, with the rights to access the database and system that controls corporate approved vendors. Most importantly, by next defining an access policy in the identity management system that prevents any member of the ***Purchasers*** group from being in the ***Vendor Managers*** group, and vice versa, the firm can execute its separation of duties control. The benefit of using the identity management system for this purpose is that as any one employee is promoted or reassigned, the identity management system will automatically manage that employee's membership in the above two groups. Any attempt by an employee in the ***Purchasers*** group to access the Vendor Management system will be not only blocked by the identity management system, but also logged and flagged for later audit purposes.



Additional tools for enforcing employee-facing controls come from user provisioning technologies. These can enforce rules relating to employee rights, to ensure that new user accounts are created with correct rights.

Controls Affecting Business Partners

So far, we have looked at internal controls as they relate to internal people, i.e. employees. However, operational controls might also be applied to external people, such as employees of a supplier, a distributor, or corporate customer. These external parties are tied into a corporation more tightly than ever before, and this integration may create compliance issues.

In many cases, a corporation might store and manage information about its partners' employees as well as its own. This information is used to grant partners' access to internal applications. Often, responsibility for managing this information is delegated to the partners themselves, even though the data and access rights live within the corporation. This creates an additional set of holes, not only concerning rights and separation of duties regarding partner employees, but also audited controls when one of those employees leaves the partner organization. If the partner neglects to update the corporation's systems, a rogue ex-employee will still have rights to access internal systems at the corporation. New forms of identity management systems, typically known as "federated access systems," can provide automatic enforcement of controls against partner employees accessing corporate systems, thereby increasing compliance in additional areas.

INTERNAL CONTROLS AND APPLICATIONS

While applying internal financial and operational controls to people is most common, many corporations are starting to worry about applying these controls to the interactions between two back-end corporate systems. That is, as technologies such as web services proliferate, it is much easier for systems to connect and access each other's data directly, without people involved. This increases business agility and efficiency, but open up a new set of compliance holes. What corporation wants to spend significant time and money to implement regulatory controls on its people, only to find that automated interactions between back office systems are completely avoiding these controls?

Because of this scenario, many firms are looking to apply IT solutions to automated systems operations in a similar manner to operations involving people. This makes sense, as many concepts, such as rights control, separation of duties (in the form of business logic) and auditing/reporting apply equally well to business systems and applications as people.

Firms that are examining Service Oriented Architectures as a way of increasing business agility should prepare to apply operational controls to these architectures and applications. Products such as web services management solutions are available to automate enforcement of internal controls within back office and inter-company data processing.

COMPLIANCE AUDITING AND REPORTING

Effective design and deployment of internal controls is only half of the burden imposed by Sarbanes-Oxley. Firms must also be able to demonstrate the workings of these controls. As a result, comprehensive auditing and reporting of controls are as important as the controls themselves. Otherwise, the firm cannot show compliance, thereby wasting the effort.

Earlier, we discussed one of the main benefits of identity management and web services management solutions for compliance—these technologies automate the enforcement of internal controls. However, there is a second important benefit. As these products enforce controls, they also gather the data necessary to audit transactions and demonstrate proper operations of these controls.

Firms that are considering IT solutions to enforce internal controls across corporate applications should examine these solutions' ability to track and report on enforcement and potential violations.

ORACLE IDENTITY MANAGEMENT AND SARBANES-OXLEY

As a leading provider of technology for managing interactions between people and corporate applications, Oracle provides a full suite of identity and web services management solutions. For example, Oracle COREid Access and Identity ensure enforcement of rights for both internal employee and business partner access. Oracle Web Services Manager applies these same controls to back-office system-to-system interactions, for example between an accounting and order processing application.

Sarbanes-Related Features

Oracle has found that customers typically use several key features as they complete their compliance initiatives. These include: strong policy enforcement, automatic group management, and centralized reporting.

Strong Policy Enforcement. Many compliance controls require specific and often complex policies related to access and application rights. Oracle COREid Access and Identity provide extremely flexible policy definition, so that customers can build IT controls that match real-world business requirements.

Automatic Group Management. Enforcing separation of duties requires effective and up-to-date group membership. Without automatic group management, the firm cannot ensure that a particular employee is locked out of a particular system. Oracle COREid Access and Identity provides automatic group management and membership, based on employee attributes, so that policies are enforced correctly.

Centralized Reporting. Defining and enforcing controls is only half the battle; reporting on these controls is equally important. Oracle COREid Access and Identity provides a centralized reporting facility that gathers information from many decentralized systems, collates the data, and generates compliance reports on the fly. As a result, Oracle customers can ensure not only enforcement, but also demonstration of all necessary IT controls.

CONCLUSION

The result of the Oracle Identity Management solutions is more effective internal controls, tighter auditing and improved reporting, and greatly improved compliance with a host of regulations, including Sarbanes-Oxley.

ORACLE FUSION MIDDLEWARE

Achieving Sarbanes-Oxley Compliance with Oracle Identity Management
September 2005
Author: Rick Caccia

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com