

# Sarbanes-Oxley Act

COMPLIANCE BRIEF



*In March 2004, there were 28 disclosures of weaknesses in internal controls. 10 of those disclosures specifically mentioned deficiencies in user access controls or segregation of duties.*

—Compliance Week, April 6, 2004

## The Challenges of Sarbanes-Oxley Section 404 Compliance

One of the most critical laws passed in recent years is the Sarbanes-Oxley Act of 2002 (SOA) enacted by Congress on July 30, 2002. SOA is designed to ensure proper financial reporting and disclosure in an effort to rebuild public trust in corporate business reporting. One of the key pieces of SOA is Section 404, which specifically covers internal control activities over the creation of financial reports. Most companies that will report financial results in the US after November 15, 2004 will be required to obtain an attestation from an outside auditor. As a result, Section 404 compliance has risen to the top of many corporate agendas.

Many companies are now well into their compliance activities, and certain key issues are arising as the most common and pressing weaknesses. As it turns out, many of these key issues are related to user authorization and access to systems, and to the proper segregation of duties amongst roles in systems. With the development of Identity and Access Management products over the past few years, the solution to these internal control issues may be close at hand.

Section 404 compliance, provides a checklist of questions to test your company's level of preparedness, and discusses how Identity and Access Management products can solve many of these problems.

### ■ Common Problems in Sarbanes-Oxley Section 404 Compliance >>

Section 404 is inherently vague about what internal controls are sufficient to “pass” Sarbanes-Oxley, or more specifically to “receive an unqualified attestation with regard to the effectiveness of one’s internal controls” from an outside auditor. Since many companies are in the midst of their compliance activities, many IT auditors have found that there is a common set of issues that are often discovered during the compliance analysis and testing process. The following list<sup>1</sup>, given by a Big 4 IT audit partner at a symposium on Sarbanes-Oxley compliance hosted by the International Systems Audit and Control Association (ISACA), illustrates these common compliance failures:

#### 1. System documentation does not match actual process

In many cases, documentation of internal controls exists but is hopelessly out of date and does not reflect the current processes and controls.

#### 2. Procedures for manual processes do not exist or are not followed

Many procedures and “controls” are simply ingrained in the normal operation of an IT organization. They often are not documented, and if there is documentation, it often is not followed. The result is a process that is not only unclear, but almost totally non-auditable.

#### 3. Custom programs, tables, and interfaces are not secured

Many home-grown applications and the data that they reference are not secured adequately to protect them against unauthorized access or use.

#### 4. Posting periods not restricted within the GL application

Since timeliness of financial reporting is critical, assuring that financial transactions cannot be posted to an improper reporting period is a key control.

#### 5. Terminated employees or departed consultants still have access

Some studies have shown that approximately 25-30% of user accounts represent departed individuals. These orphan accounts represent a huge security vulnerability, and controls need to be in place to ensure that these accounts are terminated immediately.

#### 6. Large number of user with access to “super user” transactions in production

This problem is often the result of the view that a limited set of people ought to be able to perform any function within the IT infrastructure. This problem creates a set of people who have no restrictions on their actions, and sometimes even can perform non-audited operations. All users (even the highest-level Administrators) need to have a specific role that they perform, with a set of access rights that is explicitly associated with that role. And, all such access must be logged and audited periodically to ensure proper use of those access rights.

#### 7. Development staff can run business transactions in production

Development staff often need extra privileges in order to allow them to test applications and transactions before they go live. However, those access rights should generally not be granted to them for production transactions, and any such authorization must be carefully audited to guard against improper use.

#### 8. Databases supporting corporate Financial Applications are not secure

Critical data used by applications such as PeopleSoft, SAP, etc, often are not adequately secured. Data can often be accessed directly by users without going through the appropriate level of access control mechanisms.

#### 9. Operating systems supporting corporate Financial Applications or Portal are not secure

A similar issue to the previous, but in this case with regard to operating system access.

<sup>1</sup>Information Systems Audit and Control Association (ISACA) Conference, April 2004, presentation by K. Vander Wal, CISA.

## 10. Unidentified or unresolved segregation of duties issues

Many times, financial fraud could be controlled or eliminated with a satisfactory segregation of duties in system and transaction access rights. Often, certain people (for example, Administrators) have authorization to approve access requests that they themselves have made. By doing so, they can grant access to themselves beyond what was intended. Segregation of duties problems must be identified quickly, and controls instituted to ensure that they are corrected, and that appropriate approvals are required for any access to sensitive resources. In the words of one Big 4 IT auditor, if a firm has not found any segregation of duties violations in their processes, then they just haven't looked hard enough.

An interesting thing to note in this list is that seven of the ten issues are related to user access controls. (The exceptions are #1, #2 and #4.)

## ■ An Identity and Access Management Section 404 Compliance Questionnaire >>

Although Section 404 compliance requires a detailed analysis of each specific environment, some general guidelines can help you identify the most critical areas of security to consider in your compliance efforts.

### 1. Do you have sensitive applications on the network?

- If so, then access to those applications needs to be controlled through an access management infrastructure.

### 2. Do you have procedures defined to authenticate all users of the system?

- Is it impossible to gain system or application access without proper authentication?
- Are there a variety of authentication methods used (for greater security)?
- Can someone authenticate using one method (e.g., passwords) but gain access to a resource protected by a different type of authentication (e.g., biometrics)?
- Do user sessions time-out after a predefined period of time?
- Do they time-out after a certain period of user inactivity?
- Do you have a "3 strikes and you're out" policy for failed login attempts?
- Do you have a policy about concurrent logins to the same user account?
- Are your user IDs sufficiently difficult-to-guess to prevent outside attacks on those accounts?

### 3. Do you have regular procedures defined to maintain the ongoing effectiveness of the authentication mechanisms?

- Do you have specific policies that ensure that all passwords are "strong" (not easily guessed)?
- Are passwords at least six characters long? Do they require at least one special character?
- Do you have a way of ensuring that users can't choose any of their profile attributes as their password?
- Are there policies that ensure passwords will change regularly?
- Do you have an effective forgotten password policy?
- Do you have procedures for ensuring strong authentication for dial-up access? (eg, callback)

### 4. Do you have procedures in place to ensure timely action relating to requesting, issuing, suspending, and closing user accounts?

- Is system and application access removed "immediately" from users who are terminated?
- Are attempts to gain unauthorized access to systems logged, and followed up on a timely basis?
- Are there periodic reports (in addition to "alerts") that summarize the total unauthorized access attempts, as well as administrative actions related to security?

*"If you haven't found user access control and segregation of duties violations yet, you just haven't looked hard enough."*

—Senior Manager,  
Big 4 Audit Firm;  
ISACA Sarbanes-Oxley Conference,  
April 6, 2004

- Are there appropriate management approvals required for certain requests for system access?
- Is the access that is granted to all your users appropriate based on the role and function of each user?

## 5. Do you have a process to periodically review and confirm the access rights of all users?

- Does this process include a review of access rights for each defined role?
- Are these roles periodically reviewed so that conflicts or inappropriate overlaps can be identified quickly?
- Are these reviews conducted in conjunction with the owners of each application or data, so that someone who understands the sensitivity of the application can review all of its users?
- Are reports available of all access rights currently granted?
- Are these reports periodically generated and reviewed by management?
- Are exceptions handled quickly so that improper access is terminated?

## 6. Are there adequate controls in place to safeguard the data within a corporate directory?

- Are users granted access only to the data that they require, so that they cannot access any information higher in the directory tree?
- Are there controls to prevent users from being able to bind anonymously to directories?

## 7. Do you have controls in place relating to segregation of duties over requesting and granting access to systems?

- Do you have policies and controls in place to ensure that there is no person within your environment that can request as well as grant access to specific resources (i.e., no person can grant their own access request)?
- Are physical signatures required for all requests for broad access rights (however that is defined for your specific environment)?
- Have you analyzed all your users and their roles and access rights, to ensure that there are no examples of incompatible rights granted to any user?

“**My Two Biggest Issues are User Access Controls and Segregation of Duties.**”

—CIO, Finance;  
Fortune 70 Manufacturer

## ■ The Role of Identity and Access Management in Section 404 Compliance >>

Compliance with Sarbanes-Oxley can be a difficult, time-consuming, and expensive effort. Many firms will attempt their initial compliance within the framework of their existing procedures and technology. They will “muddle through”, in an attempt to meet the initial compliance deadlines without adding the risk of new technology acquisition. However, the pain of initial compliance will cause most firms to investigate major changes in their business processes and procedures, as well as adoption of certain technologies that can help facilitate their future compliance efforts.

One of the most beneficial of these technologies for Sarbanes-Oxley compliance is Identity and Access Management products such as those available from Netegrity. Netegrity’s products represent an integrated platform of services that provide user administration, access management, and resource provisioning for Enterprises of all types and sizes. When deployed together, these integrated products not only reduce costs, and increase security, but make compliance with governmental regulations easier and more demonstrable.

The Netegrity product line provides comprehensive identity and access management functionality with an integrated administration model. It offers a flexible, open architecture that fits into your environment, no matter how complex, and handles the specific challenges of emerging service-oriented architectures.

Netegrity products include:

- **SiteMinder®**—the market-leading access management solution for Web-based and enterprise applications, creating a secure foundation for identity and access management.
- **TransactionMinder®**—the industry's first policy-based solution to protect access to Web services.
- **IdentityMinder® Web Edition**—a flexible, role-based user administration and access management solution for Web-based applications.
- **IdentityMinder® eProvision**—a comprehensive provisioning solution for automating the process of managing access to valuable enterprise resources for employees, contractors, and partners.

Netegrity's identity management platform can greatly aid your Sarbanes-Oxley compliance in the following areas:

Product	User Account Management	User Authentication and Authorization	Flexible Password Services	User Access Rights Termination	Activity Monitoring and Auditing	User Self-Service Account Management	Segregation of Duties Prevention
IdentityMinder eProvision	Yes		Yes	Yes	Yes	Yes	Yes
IdentityMinder Web Edition	Yes		Yes	Yes	Yes	Yes	
SiteMinder		Yes	Yes		Yes		
TransactionMinder		Yes			Yes		

**1. User account management**

IdentityMinder eProvision and IdentityMinder Web Edition are designed specifically to address the challenges of user management (requesting, establishing, issuing, suspending, and closing of user accounts). These products provide identity creation and management services through delegated user administration, user self-service, integrated workflow, and a structured administrative model to enable role-based access control thus providing an effective mechanism for managing user's access to protected resources.

Both IdentityMinder eProvision and IdentityMinder Web Edition provide an integrated workflow capability that is used to manage user access requests through a formal and efficient approval process. They also provide a flexible, role-based, delegated user administration capability that is used to more efficiently manage changes, suspensions and terminations to user access.

**2. User authentication and authorization**

SiteMinder and TransactionMinder provide control over what type of authentication method is used to protect a resource and how that authentication method is deployed and managed. By centrally managing all authentication systems and using advanced authentication policy management capabilities, companies can deploy mixed authentication methods based on resource value and business needs, thus providing the right level of resource protection for a given resource.

SiteMinder and TransactionMinder also provide a rich policy model, so that user access to protected resources and applications can be easily controlled as well as monitored.

Centralized controls and processes can be established to manage the creation and management of identities and the creation and management of fine-grained access management using powerful concepts such as role-based access control (RBAC). Centralized identity management and access control provides both greater efficiency and greater security.

### 3. Flexible password services

One of the key requirements of compliance is a set of flexible password policies that ensure that user passwords are not only strong (not easily guessable), but also are changed regularly. IdentityMinder eProvision, IdentityMinder Web Edition and SiteMinder provide a rich set of capabilities that allow user passwords to be easily controlled through flexible password policies that are enforced for all users.

### 4. User access rights termination

IdentityMinder eProvision and IdentityMinder Web Edition allow the access rights of terminated employees or contractors to be ended immediately, thereby dramatically reducing the risk of a security breach by a departed individual. This alone greatly strengthens the internal controls on user access that Sarbanes-Oxley demands.

### 5. Activity monitoring and auditing

All of Netegrity's IAM suite provide in-depth auditing and reporting capabilities to support granular information collection and analysis on access and user entitlements. Activity, intrusion, and audit information are provided to enable the tracking of imminent and past security violations.

As an example, SiteMinder tracks user sessions so administrators can monitor the resources being accessed, how often users attempt access to particular resources, and how many users are accessing certain applications.

### 6. User self-service account management

Through the user self-service capability and the detailed reporting in IdentityMinder eProvision and IdentityMinder Web Edition, users have the ability to exercise their responsibilities to ensure they are aware of what systems and data they have access to and whether their identities and authentication have been compromised. Furthermore, administrators can also be alerted to any unusual behavior concerning protected resources.

### 7. Segregation of duties prevention

With the addition of an optional add-on module, IdentityMinder eProvision's self-service module can identify segregation of duties violations in ERP role requests, and flag those violations to managers. Managers have the option of approving the request only with the implementation of a mitigating control.

## ■ Summary >>

Sarbanes-Oxley requires substantial changes to the way that most firms' internal controls over financial information are implemented. One of the most promising technologies that can greatly streamline compliance is an identity management solution such as the integrated platform offered by Netegrity.

The Netegrity identity management platform greatly reduces administration as well as application development costs, strengthens internal controls through stronger security, and provides a centralized model for managing all user identities and access to protected data and applications.

### About Netegrity

Netegrity, Inc. is a leading provider of security software solutions that securely manage identities and their access to enterprise information assets, letting business in while keeping risk out. Netegrity provides a comprehensive identity and access management product line for continuously evolving computing environments, including legacy, Web, and service oriented architectures. Netegrity's flexible, standards-based offerings increase security, reduce administrative costs and enable revenue enhancement. Supported by a vast network of over 1,200 trained integration consultants and 200 technology partners, Netegrity solutions are licensed to more than 350 million users at over 870 organizations worldwide, including more than half of the Fortune 100. For more information, visit [www.netegrity.com](http://www.netegrity.com).

© 2004 Netegrity, Inc. All rights reserved. Netegrity®, SiteMinder®, IdentityMinder® and TransactionMinder® are registered trademarks or trademarks of Netegrity, Inc. All other product names, service marks, and trademarks mentioned herein are trademarks of their respective owners.

bf-1101-1004-a