



SentryAccess for Sarbanes-Oxley Compliance

© 2004 Nenix Corporation. All Rights Reserved. Nenix, Nenix Corporation, SentryAccess, Smart And Secure, Simple Smart & Secure, and all SentryAccess logos, are pending trademarks, registered trademarks, or service marks of Nenix Corp. All other products, services, and/or company names mentioned within this document are trademarks and/or trade names of the respective owners.

Nenix Corporation
2310 Walsh Ave.
Santa Clara, CA 95051
408.970.9242
www.nenix.com

Introduction

The Sarbanes-Oxley Act of 2002 mandates corporate responsibility for financial reporting and calls for a documented system for the management of internal controls. Effectively, Sarbanes-Oxley places the responsibility for accuracy in financial reporting onto a corporation's executive officers. Companies failing to comply with the provisions set forth by Sarbanes-Oxley (commonly referred to as "SOX") will be subjected to penalties.

This paper will show that firms implementing an identity and access management (IAM) solution will be best positioned to efficiently comply with SOX stipulations. A comprehensive IAM solution, such as that delivered by Nenix, will enable executives to confidently vouch for the data used in reporting activities.

An Overview of Sarbanes-Oxley Regulation

SOX is federal legislation affecting how corporations conduct business. It came into being as a result of several highly-publicized accounting scandals, which impacted Wall Street and overall investor confidence. Its purpose is to provide standards that ensure truth and disclosure in financial reporting for relevant corporations.¹

There are 11 sections to the Sarbanes-Oxley Act. Out of these titles, sections 302 and 404 affect how organizations perform their financial reporting, and the internal controls that are in place to ensure that such information remains private, confidential, and otherwise secure.

Section 302: Corporate Responsibility for Financial Reporting

This section assigns responsibility for accurate financial reporting to the Chief Executive Office (CEO) and the Chief Financial Officer (CFO). Both executives must assert that all information concerning financial reporting is complete and accurate, or face criminal penalties.

Section 404: Management Assessment of Internal Controls

This section states that employees signing off on financial reporting documents are responsible for a yearly report to the SEC concerning their firm's "internal controls." In this case, internal controls means access to systems that contain information of a financial nature, or that pertain to the financial operations of the organization. Organizational executives must be able to demonstrate that there are policies and controls in place that preserve the integrity of the data they use in their reporting.

How SOX Compliance Affects IT Departments

In order to comply with SOX accounting regulations, senior executives must be able to assert that financial reports are accurate. They must also be able to demonstrate auditing and reporting of internal controls. The most effective way for them to do this is to ensure the protection of the information used for reporting. The best way to protect data integrity is by implementing a system of internal controls where administrators are able to:

- Manage who has access to the system
- Assign which information, applications, systems (called "resources") to protect
- Configure alarms to sound when suspicious events occur
- Store and maintain system logs for use when reporting on internal controls

¹ Affected companies include public U.S. companies, private companies with public debt, and foreign companies trading in the U.S. market (i.e., any company listed on U.S. stock exchanges)

Identity and Access Management Systems Ease IT Burden

Deploying a robust IAM solution would ease the burden placed on IT departments. Such systems will aid the organization with regulatory requirements, as they work to enhance overall IT effectiveness.

A comprehensive IAM system should allow IT administrators to define user roles or user groups, and to assign access principles accordingly. The system should also be comprehensive enough to permit a variety of user authentication methods beyond the standard username and password. Lastly, the system should have the appropriate tools and utilities to monitor, audit, log and create system reports.

Sophisticated IAM solutions create more effective IT departments. They aggregate resources and deliver single sign-on capabilities. They provide for decentralized administration, so that multiple administrators may manage different aspects of the system. The challenge facing most organizations when deploying an IAM solution, however, is that these systems are typically very costly, and extremely complex (and therefore difficult to install).

SentryAccess: Bridging the IT-SOX Compliance Gap

SentryAccess (SA) is a comprehensive identity and access management system that enables the configuration and enforcement of authorization rules to protect corporate resources. It efficiently manages multiple user types as it applies application usage rules from internal networks to intranets, extranets, and the Web. SentryAccess requires very little modification to existing Web applications and system environments.

SentryAccess software is designed to seamlessly integrate with existing applications, resources, and firewalls. Moreover, it has been designed with an intuitive interface that makes it is easy to manage and use.

Functionality for Compliance

SentryAccess is a powerful utility that enables organizations to securely and effectively manage users, resources, access control, and system policies, thereby assuring Sarbanes-Oxley compliance. Several SentryAccess features relevant for SOX compliance are:

- **Access Control to Applications and Resources**
SentryAccess prevents unauthorized users from obtaining, viewing, or otherwise accessing protected applications and resources. It provides a way to uniquely identify users and to manage each user's privileges so that they are granted access only to those applications and resources for which they have been authorized.
- **Centralized Control over Access Management**
Administrators can use the SentryAccess Manager to centrally create and administer system policies. Many of these policies concern how to manage user requests for resources. Policies are linked by different components such as individual users, user groups, resources, or actions associated with resources. In addition, system reactions that are triggered by these policies may be defined.
- **Support for a Variety of Authentication Methods**
SentryAccess supports multiple authentication methods and levels. This is a useful feature, since not all resources have the same level of sensitivity (i.e., a public earnings statement is less sensitive than employee payroll information), and not all users have the same access rights (i.e., accounting intern should not be able to have access to the same resources as the CFO).

Functionality for Compliance, continued

- **Strong Monitoring and Reporting Tool**

SentryAccess includes powerful, real-time system monitoring tools. These tools record information such as system status (system configuration, CPU and memory usage, network connection, and Services status), user session information, and intrusion detection. Alarms for login information or failed login attempts may be monitored here. All of these are efficient tools for demonstrating effective internal controls.
- **Delegated Administration**

Large corporate portals often have so many internal and external users, and their networks are so complex, that it makes it very difficult for one administrator to manage the entire network. For fine-grained control of the corporate network, SentryAccess provides delegated administration, which makes managing corporate resources easier and more efficient. Delegated Administration grants an individual limited responsibility for maintaining identity information (such as a person's title, phone number, etc.) and security policy information (such as different access rights). The delegated administrator's control over identity attributes (view, create, modify, delete, or notification of change), is based on data sensitivity.
- **Single Sign-On**

Once a user has been authenticated to a system, SentryAccess handles the user's session information and keeps track of his/her information. The user will not need to be re-authenticated for resources with equal or lesser level of authentication. SentryAccess grants the user access to applications and resources across multiple domains without re-authentication, which makes access appear transparent to the user.
- **Web-Standards Based**

SentryAccess was created using only Web services technology. The philosophy behind this simple fact was to create a product that would be easily deployed into a myriad of diverse environments. The result is a product that is remarkably easy to integrate and deploy, even in the most diverse environments. Because it was built upon industry standards, there is a high degree of interoperability with legacy and other systems. SentryAccess supports a broad range of platforms. But the fact that it's based on standards means less customization effort is required, saving both time and money. Further, there aren't any additional hardware or software requirements.

Conclusion

The combination of functionality and web standards technology makes SentryAccess an ideal strategic component in every organization's compliance program. SentryAccess helps to assure effective, ongoing compliance by providing for secure internal controls, thereby enabling corporate executives to assert the accuracy of their financial reporting with certainty.

About Nenix Corporation

Nenix delivers Smart and Secure Web Access Management (WAM) software solutions to customers in a variety of industries. Nenix's solutions enable customers to securely deploy e-Business environments, where audiences can converse and conduct business efficiently, without worrying that sensitive information is being compromised. International corporations have chosen Nenix for its easy-to-install solution that is simple to manage, yet extremely secure. Nenix supplies WAM solutions and technology to customers through a rapidly growing worldwide channel distribution network. To meet customer demands, Nenix offers turnkey solutions through qualified business partners. With offices in North America and Asia, Nenix has the expertise and authority to address all your global e-Business security needs. You can trust in Nenix. For more information, please visit us at www.nenix.com or email us at info@nenix.com.