



How Enterprise Single Sign-on Can Help You Survive a Sarbanes-Oxley Audit

(without losing your compliance, your freedom, or your shirt)

A resource guide compile and edited by:
Gregg LaRoche, Director of Product Management, Imprivata, Inc.

The Sarbanes-Oxley Act

Written in the wake of major corporate financial scandals and passed by a near-unanimous vote of Congress, the Sarbanes-Oxley Act of 2002 was designed to restore confidence in the equity markets and in the integrity of corporate financial reporting. Among several sections of the Act intended to improve the quality of financial reporting, Section 404 has the most direct impact on IT organizations and their operations.

Section 404 governs “management assessment of internal controls.” It mandates that a corporation must state the internal controls it has in place to protect the integrity of the financial reporting mechanism, and attest to the quality of those controls. These statements must be signed by officers of the company and their accuracy confirmed by external auditors.

According to a recent Computerworld article¹, “Expert estimates range from a low of 5% to between 20% and 25% of the 4,000 companies filing reports this year will reveal ‘material weaknesses’ in their financial controls. Moreover, some experts predict that more than 200 publicly held companies will disclose material weaknesses this year because of IT-related control deficiencies, such as security gaps and segregation of duties among applications.”

If a corporation misstates the status of its internal controls, its officers face the same consequences they would face had they filed incorrect information: possible civil or criminal penalties ranging anywhere from a costly fine to a prison sentence. However, no matter how harsh the individual penalties might be, the corporate repercussions from any allegation of non-compliance would be all but certain: negative publicity and a resulting loss of reputation, investor confidence, customers, and revenue.

Meeting the requirements of Sarbanes-Oxley is proving to be a challenge for companies of all sizes. Many larger corporations are spending millions of dollars to ensure compliance. For smaller public companies with fewer resources, even the recent one-year extension granted by the Securities and Exchange Commission (SEC) does little to ease the burden.

However, many organizations are now discovering that an Enterprise Single Sign-on (ESSO) solution can offer a means of fulfilling requirements of a Sarbanes-Oxley compliance audit while also strengthening application and database security enterprise-wide.

ESSO gives companies the ability to:

- Ensure enterprise-wide adherence to a strong password policy, thereby minimizing unauthorized access to critical financial applications and databases;
- Set compliance levels for those policies with strong authentication to control which users can access which applications;
- Self-audit the policy compliance process with full reporting capabilities to monitor which users are sharing passwords, which users are accessing financial applications from which devices/locations, and more.

1 “IT role in Sarb-Ox problems is unclear,” Computerworld, February 7, 2005

ESSO and Sarbanes-Oxley compliance requirements

To achieve SOX compliance, organizations need to adopt and enforce a range of policies, processes and procedures. ESSO solutions can help ensure the success of these initiatives. In order to select the right ESSO solution, companies should look for products that address key aspects of SOX access control requirements.

The following tables detail the SOX requirements that a proper ESSO solution must address:

SOX SECURITY STANDARDS *Administrative Safeguard Requirements*

Security Management Process	ESSO should support:
Information System Activity Review	Enabling the review of system activity via logs that show user time in and time out. Works in conjunction with application logs to doubly-verify user activity.
Workforce Security	ESSO should support:
Authorization and/or Supervision	Enforcing network-level authorization.
Workforce Clearance Procedures	Providing a mechanism for enforcing network-level authorization.
Termination Procedures	Simplifying the Authorization, Authentication, and Accountability aspects of network security policies and procedures.
Information Access Management	ESSO should support:
Access Authorization	Enabling a single point of control for access, authorization and authentication.
Access Establishment and Modification	Providing a gateway to role- or policy-based systems. Establishing a single point of control for denying network systems and application access.
Security Awareness and Training	ESSO should support:
Logon Monitoring	Monitoring of logon attempts (success and failure) for training assessment. Demonstrating of trends for awareness assessment, e.g., is a user or department more likely to have failed logon attempts? Are accounts being used multiple times when they shouldn't be? How many times did a person fail to logon correctly?
Password Management	Assisting the management of password policies via implementation of strong passwords at one central point. Allowing uniform password standard across organization, even if the application doesn't support it. Results in better management and greater security.

SOX SECURITY STANDARDS
Physical Safeguards Standards

	ESSO should support:
Workstation Use	Providing a single point of control for access, authorization and authentication
Workstation Security	Providing a mechanism for enforcing network-level authorization

SOX SECURITY STANDARDS
Technical Safeguards Standards

Access Control	ESSO should support:
Unique User Identification	Assigning one set of unique user credentials for each individual that will allow access to all appropriate applications on the network (including legacy). Enables sharing of workstations without compromising security.
Automatic Logoff	Providing uniform automatic logoff across applications.
Person or Entity Authentication	Enabling of positive verification of system use via biometric, smart card and token authentication. Supports non-repudiation
Transmission Security	Providing the security measures to guard against inappropriate access. No user can access the network without being tracked.

The IT challenges of Sarbanes-Oxley compliance

When Section 404 of the Sarbanes-Oxley Act refers to "internal controls," it means having processes in place that provide reasonable assurance that financial reporting and the preparation of financial statements for external purposes are in accordance with generally accepted accounting principles (GAAP).

While many internal controls relate to accounting practices and the handling of assets, other controls involve the recording of financial transactions and the maintenance of transaction records. These latter controls can only provide "reasonable assurance" that they are in accordance with GAAP principles if pervasive IT security is in place, because pervasive IT security is necessary to ensure the integrity of the information reported in financial statements.

The most essential form of IT security for Sarbanes-Oxley compliance is access control. If organizations cannot control access to applications and databases, they have no way of providing reasonable assurance that the information they report has not been tampered with or corrupted.

Ensuring access control is a challenge for many organizations, for a number of reasons, including:

Complex IT environments:

Most companies' IT environments include a diverse assortment of legacy, PC and Web applications, both internal and external. Any access control methods they employ must address all relevant applications and platforms in their environments.

Complex legacy applications:

Many finance departments still rely heavily on legacy systems for which the software code has grown increasingly complex over time. Often, organizations lack the resources to modify application code written years or decades earlier.

Weak or poorly-enforced password policies:

A strong password policy – requiring complex passwords and regular password changes – can be very effective in preventing unauthorized access to critical applications. However, without mechanisms in place to enforce them, strong password policies often fail due to a lack of user cooperation.

Time and cost:

Development and deployment of enterprise-wide access control mechanisms can be costly and require months or years of effort, thus precluding the possibility of meeting the Section 404 compliance deadline.

The proper ESSO solution should enable you to put policies in place, ensure that employees are following procedures, and monitor compliance internally. As a result, when the Sarbanes-Oxley auditors arrive, you will have what you need to answer their questions and prove compliance with the provisions of Section 404.

However, with compliance deadlines looming, time and money can become major stumbling blocks to the implementation of some ESSO solutions. Imprivata OneSign is different.

The advantages of Imprivata OneSign technology for Sarbanes-Oxley compliance

Two major ways in which organizations can support Sarbanes-Oxley requirements are by strengthening application password security and establishing a log of user application access data. An enterprise SSO solution can fulfill these needs, but some SSO solutions are costly, difficult and time-consuming to deploy.

Imprivata OneSign is an affordable network appliance that enables organizations to implement enterprise SSO for Web, client/server and legacy applications. Through a unique, centralized approach to password management, OneSign makes secure SSO services quick to deploy, convenient to use and easy to administer. OneSign makes it simple and practical for companies of all sizes to adopt and enforce password policies that support SOX compliance.

“To be Sarbanes-Oxley compliant when you have backend legacy systems is very difficult, because application vendors must be forced into authentication and authorization compliance. We need a password authentication scheme that proxies -- that is, comes between -- all the legacy systems and the user interface. OneSign provides exactly that service, allowing organizations to jumpstart Sarbanes-Oxley compliance. With OneSign, the IS department can bring everyone to a common organizational and compliance standard of strong passwords, and eventually move to biometric, smart card and/or to token authentication.”

~ OneSign customer

Imprivata OneSign's superiority as an ESSO solution rests on several key distinguishing features:

Password Policy Automation

OneSign is tightly integrated with the Windows Domain authentication, allowing administrators to implement a clear and straightforward password policy across all applications based on users' primary authentication. For additional security measures, OneSign has the ability to change complex application passwords behind-the-scenes on users' behalf, enabling realistic enforcement of a strong password policy from one central location. Enterprise-wide adherence to strong password policies provides additional assurances to auditors that proper security measures are being followed.

Client-Side Monitoring and Reporting

Imprivata OneSign records and captures all user and application events in log files, providing a trail accessible to the administrator and, in turn, to Sarbanes-Oxley auditors. Client-side events pertaining to SSO services - including data on which users accessed which applications and when - are collected and consolidated by the OneSign appliance for centralized viewing and reporting. In addition, event logs capture information on user switching and password changes with time stamps that verify authentication and lockout incidents. These capabilities provide objective proof to Sarbanes-Oxley auditors that IT security measures are in place and being adhered to.

The image displays three overlapping screenshots of the Imprivata OneSign web interface, illustrating its reporting capabilities.

The top screenshot shows the 'Reports' section with a table of 'Administrator Activities between Apr-12-2005 and Apr-12-2005'. The table includes columns for Date, User, and Activity. The data rows are as follows:

Date	User	Activity
Apr-12-05 4:10:54 PM	Administrator	Deployed application 2-80
Apr-12-05 3:57:42 PM	Administrator	Deployed application 2-80
Apr-12-05 3:53:30 PM	Administrator	Deployed application 3MCT
Apr-12-05 3:53:11 PM	Administrator	Modified application profile
Apr-12-05 3:43:39 PM	Administrator	Deployed application 2-80
Apr-12-05 3:40:57 PM	Administrator	Modified application profile
Apr-12-05 3:40:53 PM	Administrator	Modified application profile
Apr-12-05 3:33:19 PM	Administrator	Modified application profile
Apr-12-05 3:33:16 PM	Administrator	Modified application profile
Apr-12-05 3:27:40 PM	Administrator	Modified application profile
Apr-12-05 3:27:37 PM	Administrator	Modified application profile
Apr-12-05 3:13:20 PM	Administrator	Modified application profile
Apr-12-05 3:13:16 PM	Administrator	Modified application profile

The bottom-left screenshot shows the 'Administrator Activity Report Setup' form. It includes a 'Date Range' section with 'Start Date' and 'End Date' fields, both set to 04/12/2005. There are 'Go' and 'Cancel' buttons at the bottom.

The bottom-right screenshot shows the 'User Reports' section. It lists several reports with their descriptions:

- Login Activity:** The Login Activity Report lets you see all the user login activities into Domain that occurred over a specified period.
- User Lockouts:** The Lockout Report lets you see all the user lockouts that occurred over a specified period of time. Lockouts occur after a specific number of login attempts are exceeded. This threshold is managed by the OneSign Security Policy.
- Enrollment:** The Enrollment Report lets you see all the enrollments to OneSign that occurred over a specified period.
- User Activity:** The User Activity Report lets you see all the user activities using OneSign over a specified period of time.
- Administrator Activity:** The Administrator Activity Report lets you see all the administrative tasks that were performed using OneSign over a specified period.
- Username Correlation:** The Username Correlation Report shows you all the OneSign users who are sharing the same username to log into one or more applications.

The bottom-right screenshot also shows the 'Application Reports' section with two reports:

- Application Credential Capture:** The Application Credential Capture Report lets you see application credential captures by OneSign that occurred over a specified period.
- Application Credential Proxy:** The Application Credential Proxy Report lets you see all the application credential proxies by OneSign that occurred over a specified period.

Imprivata OneSign's superiority as an ESSO solution rests on several key distinguishing features (cont.):

Application Profile Generator (APG)

The OneSign APG enables secure and seamless SSO to all enterprise applications - without requiring any modifications to existing code. With OneSign APG, the arduous task of building connectors to each application in order to enable SSO is completely eliminated.

OneSign's APG "learns" the behavior of any application's authentication process and then generates an SSO application profile that stores these attributes in XML. These profiles are automatically uploaded to the OneSign appliance by APG and are ready for deployment and distribution to users at runtime.

With OneSign APG, even the most challenging of application password behaviors and authentication processes can be learned. The powerful technology can capture and proxy the attributes of a logon process for applications like custom TEs, SAP, Oracle Forms, and JAVA applets – all of which have complex or hidden controls that have previously required IT staff to write "workarounds" or custom scripts to successfully configure SSO. As a result, companies of all sizes can have OneSign up and running well in advance of Sarbanes-Oxley compliance audits.



Shared Workstation SSO

Imprivata OneSign's support for shared workstation environments allows a single computer to serve unique and secure access to multiple users, a major benefit in any business setting where several people might use the same computer, such as in a retail store, or on the floor of a manufacturing facility where employees are accessing inventory applications.

The OneSign appliance makes it easy for every user to start a secure SSO session with proper authentication. Individual users no longer need to leave their terminals logged on all day with one name and password – they can easily sign on themselves. In addition, OneSign's shared workstation support features a one button lock/unlock via a globally defined keyboard key. With single sign on/off, users can automatically terminate a session or re-access a suite of existing SSO enabled applications by re-authenticating to the OneSign appliance. For Sarbanes-Oxley purposes, these capabilities also ensure the accuracy of OneSign log files that identify the users accessing critical financial applications.

Beyond Sarbanes-Oxley

While the current focus on IT security is largely being driven by the Sarbanes-Oxley Section 404 deadline, the advantages of ESSO extend far beyond that initial need. Besides supporting Sarbanes-Oxley compliance, OneSign delivers an array of valuable benefits, including:

Stronger security

By relieving users of the need to memorize multiple passwords, OneSign makes it easier for organizations to implement – and enjoy the increased protection afforded by – strong password policies. OneSign also strengthens security by making it practical for organizations to change passwords more frequently.

Simplified password administration

With OneSign, administrators can implement a straightforward password policy across all applications based on users' primary authentication. To increase password security, OneSign can cycle application passwords behind the scenes and disable any user with a single mouse-click.

Reduced help desk costs

When users have multiple application passwords to remember, they often forget them – leading them to call their IT help desks for assistance. According to industry analysts, more than 30% of help desk calls are password-related. With a single help desk call costing an estimated \$25, the annual cost of password problems can be considerable. OneSign can reduce the number of help desk calls and the resource costs associated with them.

Increased user productivity

With SSO, users can gain more immediate access to the applications they need to do their work, and spend less time tracking down forgotten passwords.

Organizations can also enhance their OneSign investment by easily adding cognitive security (strong passwords), token security (RSA SecureID, swipe cards), and biometric security (retina scans, fingerprints). Once OneSign is deployed and in use, companies can strengthen security further by adopting more stringent standards of their own.

For more details on OneSign, please visit: <http://www.imprivata.com> or contact Imprivata at: **877-ONESIGN.**