ManageEngine
Password Manager Pro

Ensuring Compliance to Sarbanes-Oxley through Privileged Identity & Information Management

White Paper

V Balasubramanian
ZOHO Corp.

Disclaimer: This document is not intended to be a complete guide or legal advice to Sarbanes-Oxley. This is just to propose a solution for SOX-compliance. If you have a real-situation, satisfy yourself about the effectiveness of the solution through proper evaluation.

Abstract

Enterprises dealing with public funds are required to comply to Sarbanes-Oxley (SOX) Act. Organizations are looking for a single, complete, low-cost, enterprise-wide solution that could take care of all their SOX-compliance needs. This White Paper discusses the SOX compliance challenges and the problems faced by the IT administrators, who are mandated with the task of ensuring compliance to SOX. It explains how Privileged Identity and Information Management (PIIM) solutions could ensure effective internal controls and serve the enterprise-wide SOX-compliance needs. The vital ingredients that one should expect in a PIIM solution and the factors to ponder before zeroing-in on a PIIM solution, have also been dealt with.

Contents

Ensuring Compliance to SOX – The Challenge

The Public Company Accounting Reform and Investor Protection Act of 2002, popularly known as the Sarbanes-Oxley Act, enacted in the U.S in the wake of unprecedented, large-scale financial scandals, mandates the top management of public finance companies to incorporate strong internal controls and ensure accuracy and transparency in public financial disclosures.

Perhaps, the biggest challenge with SOX Act is that it just asks the companies to ensure accuracy and transparency in financial disclosure and establish internal controls without prescribing anything like 'best practices' or other specific details.

The objective of SOX Act is straight-forward: Assuring that the information, which the investing public rely on to make investment decisions are trustworthy, accurate and complete. But, ensuring compliance to this objective is indeed a daunting task as there are numerous factors that could lead to inaccurate financial reporting.

Auditors and analysts have listed out some of the prime factors that dampen the accuracy of financial disclosure:

> The biggest challenge with SOX Act is that it just asks the companies to ensure accuracy and transparency in financial disclosure and establish internal controls without prescribing anything like 'best practices' or other specific details.

- As laid down in SOX Act itself, lack of proper internal control – specifically, lack of an effective mechanism to restrict access to sensitive financial information, is often the key for malpractices in organizations
- The internal control mechanism should be capable of detecting and preventing the malpractices/frauds in organizations. If there are rooms for fraud, the financial disclosures will be inaccurate
- Lack of informative reports that depict information on 'who' has access to 'what' information in the organization
- Each and every activity of a privileged user should be monitored in the organization. Lack of such a monitoring capability is a potential cause for mis-appropriation of funds
- Whenever a security breach occurs, the organization should be capable of detecting that quickly. Lack of such a mechanism will lead to holes in fraud prevention

From the foregoing, it is clear that effective internal control forms the backbone of SOX.

Though SOX Act targets the top-brass like the CEOs, CFOs and Board of Directors of the organizations by holding them directly responsible for mal-practices, the implementation part for compliance largely rests with the staff at the lower level.

The administrators and IT Managers, in particular, are responsible for defining SOX compliance policies and also demonstrate that the organization complies to the policies defined.

The administrators mandated with the task of ensuring compliance to SOX are bogged by several questions:

- How to select an IT solution that can help in ensuring compliance to SOX? What to look for in the solution?
- Our financial data are spread across diverse systems, applications, databases and servers. How to generate a unified, enterprise-wide SOX compliance report?
- What are all the reports that SOX auditors expect?
- When the data pertaining to several clients are being managed, how to generate separate SOX compliance reports for each client separately?
- Where to store the audit trails related to SOX?
- How to generate reports for SOX compliance from the audit trails?
- How to detect and prevent misuse of data by privileged users?

Scenario Today

Today, organizations are looking for a complete solution that could take care of all their SOX-compliance headaches. But, such solutions are prohibitively expensive. Industry researchers have estimated that SOX and other financial governance spending in the U.S will reach $6.2B in 2008, up by nearly 2 per cent from 2007.

The SOX compliance costs for smaller organizations, in particular is very disproportionate. The U.S. Securities and Exchange

What does SOX Mandate?

Of the 11 sections of SOX, section 404 lays the foundation on how IT can aid SOX compliance. Section 302 and 802 are also relevant to some extent.

Section 404 - Management Assessment of Internal Controls

This section pertains to the guidelines laid down by the Securities and Exchange Commission on what SOX demands. According to the SEC, companies must: "Include in their annual reports a report of management on the company's internal control over financial reporting".

The control report must include:

1. "A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting."
2. "Management's assessment of the effectiveness of the company's internal control over financial reporting."
3. "A statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting."
4. "A statement that the registered public accounting firm that audited the company's financial statements”

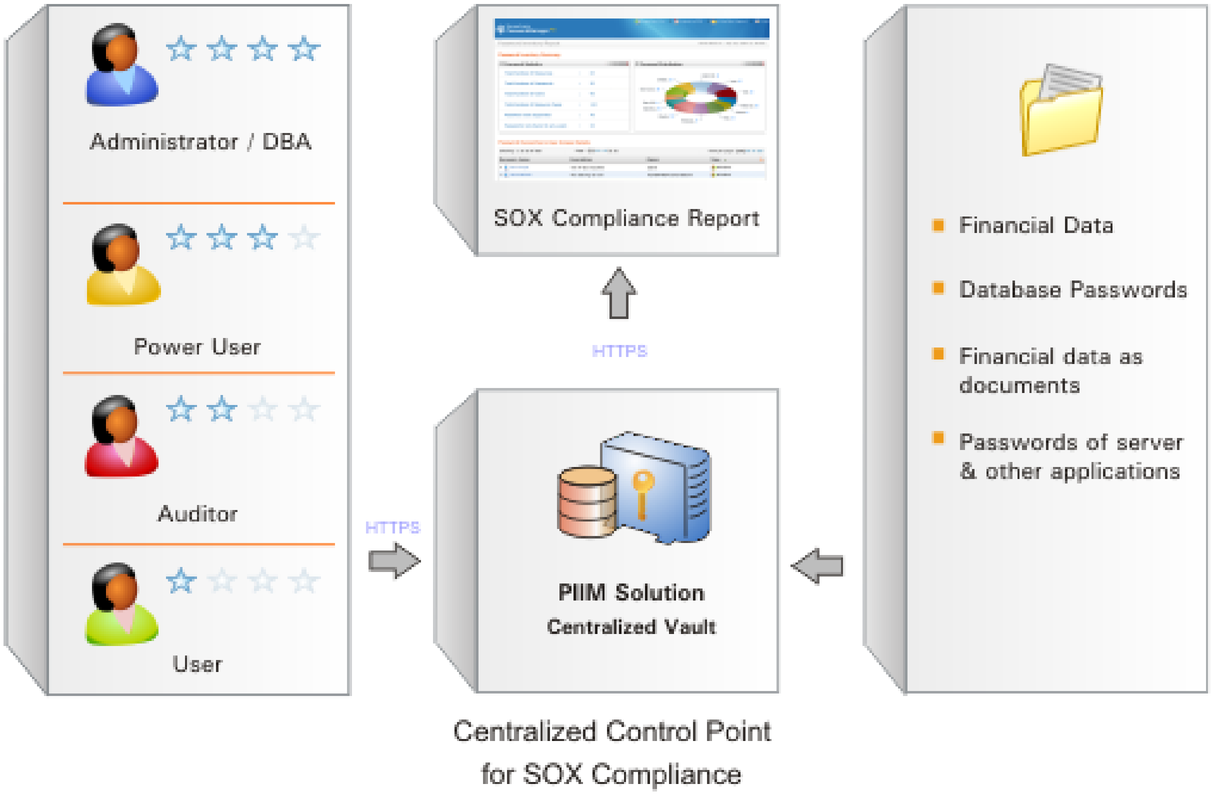
Commission has predicted compliance costs of $91,000 for smaller public companies, technically those with less than $75 million in market capitalization.

Therefore, organizations are caught in a fix. They are required to comply to SOX, but not in a position to spend huge money. It is equally difficult to find a single solution that could take care of all their SOX compliance needs.

The Way out

SOX lays stress on internal controls on access to privileged information, resources and applications. Deploying a Privileged Identity and Information Management (PIIM) Solution is one of the ways to achieve effective internal control in organizations.

All the documents, spreadsheets and reports containing sensitive financial data could be stored in a repository, which would serve as a secure, central vault. Ownership for the documents/data could be clearly-defined and the documents could be shared with the privileged users on need basis.



Similarly, the privileged identities, whose passwords are typically shared to gain access to databases, servers and other IT resources containing financial data, could be stored in the central vault. This would help in restricting access to these resources to a few privileged users alone.

Thus, PIIM solution will become the centralized repository for all sensitive data. It will act as the 'centralized control point' for the entire organization from the standpoint of SOX. The reports generated by the PIIM solution, with special emphasis on SOX related details, will provide a unified view of the happenings in the organization.

A single PIIM solution could serve almost the entire SOX compliance requirements of organizations. With the availability of affordable PIIM solutions in the market, the cost of deploying and maintaining such a solution would be very less, in fact, just a fraction of the cost involved in deploying many compliance management solutions.

What to look for in the Privileged Identity & Information Management (PIIM) Solution from SOX Compliance Perspective?

Document Vault

The solution should be capable of securely storing documents containing sensitive financial data, in addition to storing privileged identities / passwords. This is a pre-requisite for SOX compliance.

Ownership & Sharing Model

There should be provision for establishing clear-cut ownership for the passwords and documents. Only the owner should have exclusive privileges to access, view and change the document/password. Optionally, there should be provision to share the documents/passwords with other users on need basis, with fine-grained access restrictions. SOX emphasizes on '**segregation of duties**'. The ownership and sharing model is essential to achieve segregation with respect to SOX related information in the organization.

Section 302 - Corporate Responsibility for Financial Reports

For each company filing periodic statutory financial reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 it is required to include certifications that:

1. The signing officers have reviewed the report.
2. The report does not contain any material untrue statements or material omission to make the statements considered misleading.
3. The financial statements and other related financial information fairly present the financial condition and the results of operations in all material respects.
4. The signing officers are (a) responsible for internal controls (b) designed such internal controls (c) have evaluated these internal controls within the previous ninety days and (d) have reported on their findings.
5. The signing officers have disclosed (a) all deficiencies in the design or operation of internal controls and (b) any information on any fraud that involves employees who are involved with internal activities.
6. The signing officers have indicated any significant changes in internal controls or related factors that could have a negative impact on the internal controls.

Section 802: Corporate and Criminal Fraud Accountability

1. This section mandates that records be maintained for seven years after the auditor concludes the audit

2. Also, specifies the criminal penalties for altering records

Secure Data Storage & Communication

All sensitive data stored in the PIIM application such as passwords, files, digital keys, account names, IP addresses etc should be encrypted using government approved and industry standard encryption algorithms like AES and stored in the database. All data communication between the user interface and database should be encrypted. In the case of web interfaces, the communication should be through secure http.

Account Activity Monitoring

Maintaining the passwords of sensitive resources in the centralized control point alone may not be sufficient for completely tracking the activities performed by the privileged users on the resources. In such cases, the PIIM application should have the provision for monitoring the user activities in resources through detailed access logs.

Periodic Password Rotation

One of the important ways to protect IT resources from unauthorized access is to rotate the passwords of the resources at periodic intervals. Manually carrying out the password rotation would prove to be cumbersome. The PIIM solution should have provision to carry out periodic, automatic password rotation. Also, the solution should provide reports showing the frequency of password rotation as part of SOX compliance reports to be submitted to the auditors.

Comprehensive Audit Trails

All activities happening in the system should be accurately captured as audit trails. Comprehensive auditing is, in fact, the cornerstone of SOX. When SOX-related information is stored in the PIIM application, all activities performed by the privileged user should be audited. Document/password access, changes done, login/logout events, failed login attempts, changes to user privileges and all other operations performed should be audited. Details on 'who', 'what' and 'when' of user actions recorded chronologically would help in fixing accountability issues.

Tamper-proof Audit Trails

Audit trails recorded by the central vault should not only be accurate, but also tamper-proof. Otherwise, malicious users would delete the records to conceal their actions. Audit trails will then be of no use to fix accountability issues. There should be no provision to delete the audit trails as Section 802 of SOX mandates that audit records be maintained for seven years after the auditor concludes the audit. Besides, alarms should be generated when an attempt is made to delete the trails.

Request-Release Mechanism

The application should have provision for some sort of dual control when it comes to providing access to sensitive documents/passwords stored in the central vault. When a user needs access to the document/password, a request for authorization would be sent to the administrator, who would validate the request and authorize access.

Risk Analysis and Management

Despite all the policies, standards, controls and precautions, the organizations might have to face innumerable threats to security. SOX mandates the presence of a sound risk analysis and management system in the organization to protect the financial data. Therefore, the application should have provisions for analyzing and managing various risks to the data.

> SOX mandates the presence of a sound risk analysis and management system in the organization to protect the financial data.

For example, inactive users/resources are vulnerable to hacking and attacks. The application should provide a report on the inactive users/resources. Such users and resources need to be isolated and monitored. Failed login attempts are another indication of potential hacking attempts and they also need to be monitored. Frequently accessed data, passwords and resources and records should be isolated and monitored.

Out-of-the-box SOX Compliance Reports

When the very purpose of deploying a PIIM solution is for managing the SOX-related information, it should have provision for generating out-of-the-box reports depicting compliance to SOX. Particularly, the report should clearly depict who has access to what resources in the organization. This is the most basic requirement of SOX and automatic generation of such report would save a great deal of time for the administrators.

SOX auditors are required to certify the assessment of the effectiveness of internal controls established in the organization. So, apart from showing 'who' has access to 'what', there must be provision for proving other security measures such as periodic password rotation, enforcement of strong password policies, ensuring access is removed when an employee leaves the organization, eliminating need to share passwords to access systems and automating password reset process to eliminate human error.

Custom Reports

Apart from the ready-to-use reports, the application should have provision for generating custom reports to prove compliance to SOX. For example, financial organization may be dealing with the data pertaining to different clients. Some of the clients may be big companies and would require SOX compliance report pertaining to their data alone. In that case, the administrators in the financial company will have the need to generate multiple SOX compliance reports. The PIIM solution should essentially have provision for easily filtering out the required data and generate SOX compliance reports based on that.

Real-time Alerts & Notifications

For detecting and preventing frauds in organizations, SOX lays stress on real-time notifications on access to sensitive data. To facilitate this, the application should have provision for sending alerts to the owners of documents/resources on various actions such as data/password access, change in access permissions, change in user roles, password expiry, automatic password reset etc.

> For detecting and preventing frauds in organizations, SOX lays stress on real-time notifications on access to sensitive data.

Backup & Disaster Recovery

SOX mandates organizations to have provision for disaster recovery. When all sensitive financial data are stored in the application, it should have a robust disaster recovery mechanism. The data should be backedup as and when there occurs a change in the data. There should also be provision for recovering the data quickly after a disaster.

Continuous Availability of Information

Financial data stored in the application should be available for access at anytime as desired by the users. Once the application is deployed in production with all data, administrators would be heavily dependent on the application availability for retrieving documents/passwords. Continuous availability of the PIIM solution would be crucial in such scenarios. Otherwise, at the most wanted time, users would end up in not getting the required document/password and it may lead to problems, including security issues.

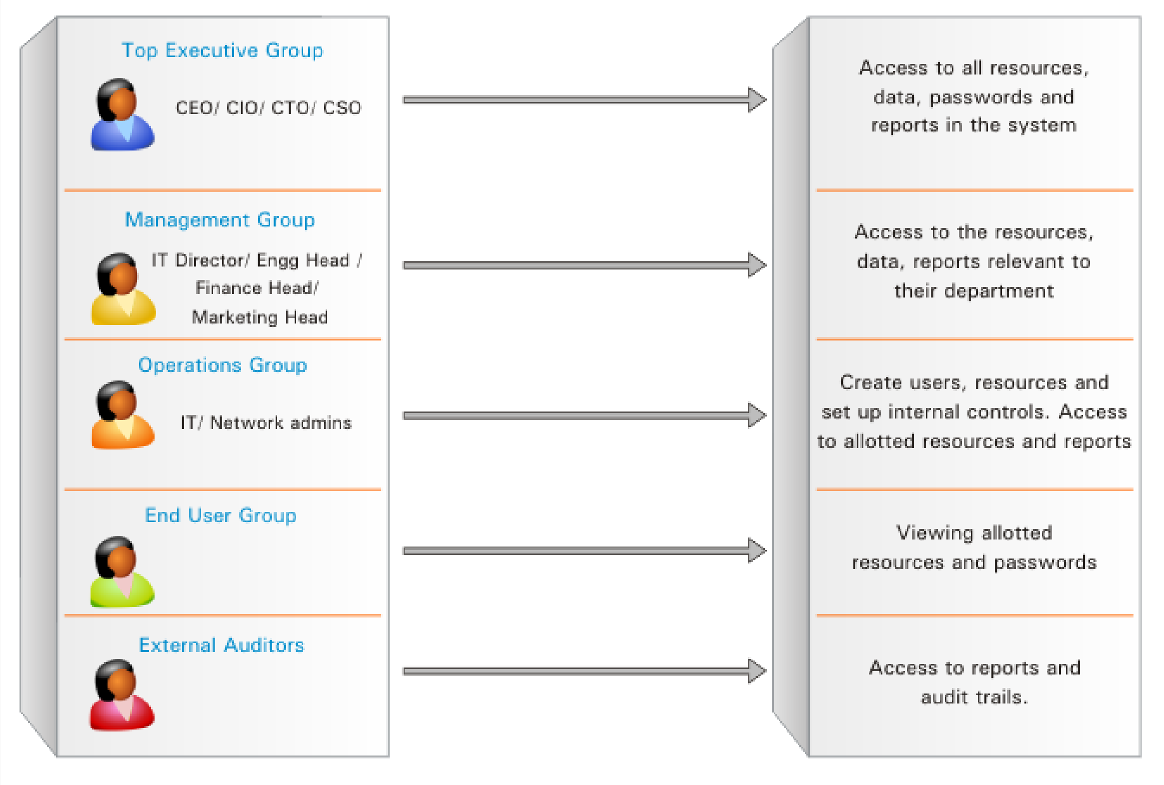
Affordable Price

Though PIIM applications would provide high value for your buck by simplifying the compliance initiatives, the cost of the solution should not be too high to damage your pockets. The price of the solution should suit your IT budget and should be capable of providing rapid Return On Investment (ROI).

A typical business environment requiring ways to ensure SOX Compliance…

Consider a financial enterprise having critical financial data stored in 500 documents and 300 spreadsheets in diverse systems. Besides, other sensitive data are maintained in 100 file servers and databases. About 200 users, with different roles would require access to specific data. Information pertaining to different clients is stored.

This is how the PIIM Solution will help: All the 200 users will get accounts in PIIM solution with well-defined access permissions and roles. The users will be grouped based on departments/divisions. The 500 documents and 300 spreadsheets will be stored in the PIIM application and specific ownership will be defined. The passwords of 100 file servers and databases will be stored in the PIIM solution and access permissions will be defined. The resources will be grouped for carrying out operations in bulk.


Top Executive Group
CEO/ CIO/ CTO/ CSO
Access to all resources, data, passwords and reports in the system
Management Group
IT Director/ Engg Head / Finance Head/ Marketing Head
Access to the resources, data, reports relevant to their department
Operations Group
IT/ Network admins
Create users, resources and set up internal controls. Access to allotted resources and reports
End User Group
Viewing allotted resources and passwords
External Auditors
Access to reports and audit trails.

The resources/resource groups would be shared with users/usergroups on need basis. PIIM solution will become the central control point and all the users will have to access it first to get the data / access other resources. Reports on user activities can be generated based on different user roles. Thus, a centralized management environment will be in place.

Conclusion

Protection of sensitive financial data by establishing robust internal control processes and demonstrating the effectiveness of the controls through reports, form the crux of the SOX.

Deployment of a PIIM solution to manage critical financial data would prove to be cost effective and highly productive as it could act as the 'centralized control point' for information access. For ensuring SOX compliance, the application would act as an enterprise-wide solution.
With a central vault, most of your SOX-related information protection activities could be automated.

Highly-skilled IT Managers and administrators need not have to spend their time generating SOX compliance reports. They can cash-in on the automation capabilities of PIIM application and meet the SOX Compliance requirements with ease and face the SOX audits with comfort.

Introducing ManageEngine Password Manager Pro

Password Manager Pro (PMP) is a web-based **Privileged Identity and Information Management Solution** for enterprises to control the access to shared administrative / privileged passwords of any 'enterprise resource' such as servers, databases, network devices, applications etc. PMP enables IT managers to enforce standard password management practices such as maintaining a central repository of all passwords, usage of strong passwords, frequent changing of sensitive passwords and controlling user access to shared passwords across the enterprise. PMP could ensure effective internal controls and prove as a potential solution for SOX compliance. It is available at costs affordable to SMBs.

For more details on PMP, visit http://www.passwordmanagerpro.com

ManageEngine

ZOHO Corp. (formerly AdventNet Inc.)
4900 Hopyard Rd., Suite 310, Pleasanton, CA 94588, USA
Phone: +1-925-924-9500 **Fax**: +1-925-924-9600
Website: http://www.passwordmanagerpro.com
For Queries: passwordmanagerpro-support@manageengine.com