SOX

Compliance White Paper

February 2018

Published by: Janco Associates Inc.
Park City, UT 84060
435 940-9300
E-mail - support@e-janco.com

The publisher cannot in any way guarantee the procedures and approaches presented in this book are being used for the purposes intended and therefore assumes no responsibility for their proper and correct use.

Table of Contents

Sarbanes Oxley Compliance White Paper

Sarbanes-Oxley Act (SOX) requires the certification of the accuracy of the periodic reports and financial statements of ENTERPRISE by the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) of ENTERPRISE. In addition, it adds the requirement that the CEO and CFO on a “rapid and current basis” disclose information that can or does materially change the financial condition of a publicly traded ENTERPRISE.

Companies face the task of ensuring their accounting operations are in compliance with the Sarbanes Oxley Act. Auditing departments typically first have a comprehensive external audit by a Sarbanes-Oxley compliance specialist performed to identify areas of risk. Next, specialized software is installed that provides the "electronic paper trails" necessary to ensure Sarbanes-Oxley compliance.

The summary highlights of the most important Sarbanes-Oxley sections for compliance are listed below. Note that certification and specific public actions are now required by companies to remain in SOX compliance.

Overview

The audit spotlight now shines on IT. After years of regulation and embarrassing data breaches, the highest levels of management now comfortably discuss IT controls and audit results. However, their quality expectations are rising. Where IT once performed audits annually, many now support quarterly, monthly, and ad hoc exercises. Each audit expands the scope of the technologies assessed, measured, and proven compliant. Broader scope means more complexity and more work. With the Sarbanes Oxley Compliance Kit, you can increase timeliness and accuracy of audit data while reducing IT audit effort, disruption, and cost.

Sarbanes-Oxley Section 404 requires that:

- Enterprises have an enterprise-wide security policy;
- Enterprises have enterprise-wide classification of data for security, risk, and business impact;
- Enterprises have security-related standards and procedures;
- Enterprises have formal security based documentation, auditing, and testing in place;
- Enterprise enforce separation of duties; and
- Enterprises have policies and procedures in place for Change Management, Help Desk, Service Requests, and changes to applications, policies, and procedures.

SOX adopted the COSO model of controls, which is the same model that SAS 70 audits have utilized since inception. SOX heightened the focus placed on understanding the controls over financial reporting and identified a type II SAS 70 report as the only acceptable method of obtaining third-party assurance regarding the controls at a service organization. Security "certifications" are excluded as acceptable substitutes for a type II SAS 70 audit report.

In addition, the ISO 27000 standard is used in SAS 70 reports. The Security Manual Template contains an ISO 27000 Security Process Audit Checklist. These two items directly address a service organization's descriptions of controls. The auditor can use these to help them in the evaluation of the service organization's control framework.

Preparation for Disaster Recovery / Business continuation in light of SOX has two primary parts. The first is putting systems in place to completely protect all financial and other data required to meet the reporting regulations and to archive the data to meet future requests for clarification of those reports. The second is to clearly and expressly document all these procedures so that in the event of a SOX audit, the auditors clearly see that the DR plan exists and will appropriately protect the data.

SOX Section 302 - Corporate Responsibility for Financial Reports

Defines several mandates including:

- **Establish safeguards to prevent data tampering** - SOX requires that the signing officer must attest to the validity of reported information. Safeguards must exist to prevent tampering with data so that data is verifiably true.
- **Establish safeguards to establish timelines** - SOX requires that the signing officer attests to the fact that reported information is fairly presented, including accurate reporting for the time periods. Safeguards must exist that the data relates to a verifiable time period.
- **Establish verifiable controls to track data access** - SOX requires internal controls over data so that officers are aware of all relevant data. Data must exist in an internally controlled and verifiably secure framework.
- **Ensure that safeguards are operational** - SOX requires that officers have evaluated the effectiveness of the internal controls as of a date within 90 days prior to the report. The security framework must be periodically reviewed and verified.
- **Periodically report the effectiveness of safeguards** - SOX requires officers to generate a report on the effectiveness of the security system, and state their conclusions. The security framework should report its effectiveness to auditors and officers of the enterprise.
- **Detect Security Breaches** - Similar to Section 404 A&B, and require that security breaches (either due to flaws in the control system, the security system or due to fraud) be detected.

This translates to the following specific responsibilities and accountabilities:

- CEO and CFO must review all financial reports.
- Financial report does not contain any misrepresentations.
- Information in the financial report is "fairly presented".
- CEO and CFO are responsible for the internal accounting controls.
- CEO and CFO must report any deficiencies in internal accounting controls, or any fraud involving the management of the audit committee.
- CEO and CFO must indicate any material changes in internal accounting controls.

SOX Section 404: Management Assessment of Internal Controls

All annual financial reports must include an Internal Control Report stating that management is responsible for an "adequate" internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these controls must also be reported. In addition, registered external auditors must attest to the accuracy of the company management's assertion that internal accounting controls are in place, operational and effective.

SOX Section 409 - Real Time Issuer Disclosures

Companies are required to disclose on an almost real-time basis information concerning material changes in its financial condition or operations.

SOX Section 902 - Attempts & Conspiracies to Commit Fraud Offenses

It is a crime for any person to corruptly alter, destroy, mutilate, or conceal any document with the intent to impair the object's integrity or availability for use in an official proceeding.

Sarbanes-Oxley Compliance Kit Options

To meet these needs the Sarbanes Oxley Compliance Resource Kit, which comes in four editions (Standard, Silver, Gold, and Platinum) contains:

- Security Policies (all editions);
- Threat & Vulnerability Assessment Tool (all editions);
- Business & IT Impact Questionnaire Risk Assessment Tool (all editions);
- Safety Program Template (all editions);
- Disaster Recovery Template (all editions);
- Outsourcing guide update to reflect what you vendors need to do (all editions);
- Internet and IT Job Descriptions (Silver, Gold, and Platinum Editions) and;
- IT Service Management Template (Platinum Edition) includes
  - Service Request Policy and Standard
  - Help Desk Policy, Procedure, Standard, and Service Level Agreement
  - Change Control Standard, Quality Assurance Standard, and Management Workbook
  - Documentation Standard
  - Version Control Policy and Standard
  - Sensitive Information Standard
  - Blog and Personal Web Site Policy
  - Travel and Off-Site Meetings Security Policy
  - Internet, e-mail and electronic communication Policy

Implementing Compliance

Closing the loop on data management

Getting started with an enterprise-wide strategy for compliance requires an understanding of the requirements particular to your industry and business. Then, policies must be put in place for collecting, alerting, reporting on, storing, searching and sharing data from all systems, applications, and network elements. This creates a closed-loop process that governs the lifecycle of enterprise data and ensures your compliance program is successful.

Here are the 10 essential steps for implementing a successful enterprise-wide compliance program:

- Understand the requirements
- Understand the IT controls that affect your business
- Define the compliance processes and success criteria
- Identify all in-scope IT components
- Collect fine-grain user and system activities
- Store all logs centrally for the required time period
- Implement regular tasks
- Implement and verify continuous monitoring
- Demonstrate compliance status to auditors
- Substantiate reports and alerts

Understand the requirements

The first step is to understand the requirements of the regulations you must meet in your industry. No matter what industry your company plays in, there are numerous mandates and regulations that apply, as well as frameworks and controls that help various business units within an organization maintain security and risk management policies. Failing to follow certain controls can result in lost customers or lost jobs, whereas failure to meet industry regulations and legal mandates could result in more serious ramifications, such as fines or even imprisonment. A thorough understanding of the requirements applicable to your industry can prevent unnecessary problems.

Understand the IT controls that affect your business

Putting in place the IT controls and frameworks for meeting compliance helps to govern compliance tasks and keep companies on track for complying with legal mandates and industry regulations. However, this requires an understanding of the specific language within those frameworks regarding log data management. The most common frameworks—COBIT 4, ISO17799, NIST 800-53/FISMA, and PCI—all have specific language pertaining to log data collection and retention. For example, requirement 10 within the PCI standard states that companies must log and track user activities, automate and secure audit trails, review logs daily and retain the audit trail for at least a year. Other frameworks have similar requirements for log data collection and retention. It's important that companies not only implement the frameworks but really understand what they're asking for.

Define the compliance processes and success criteria

Once you understand the requirements of a given regulation or mandate, determine the scope, configuration, and mechanism for collecting, alerting on, reporting on and retaining the data necessary to meet satisfy auditors. This step by step process allows you to define goals and key tasks for successful compliance. For example, when you determine the scope, your goal should be to identify all system components that are subject to a given regulation. Then you can define key tasks related to that goal. Once those tasks are complete, you can move to configuring network elements, systems and applications to generate the required log messages. After configuration, you can move to defining key tasks for important compliance activities, including the collection and retention of data and setting up automated alerts and reporting on that data.

Identify all in-scope IT components

It’s a misconception that only hardware should be monitored for compliance. In addition to network elements, servers, applications, and homegrown systems should also be monitored. The specific components that need monitoring will depend on the mandates and regulations that apply to your industry. For example, if PCI applies to your business, all components that transmit, process or store financial information are in-scope.

Collect fine-grain user and system activities

Log data from IT components across the enterprise provide a fingerprint of user activity. This information includes failed login attempts, security breaches, file uploads and downloads, credit card data access, information leaks, user and system activity, privileges assigned and changed, runaway applications, customer transactions, and email data. This is the information that auditors will expect you monitor on a daily basis. Log data contains a wealth of information that provides insight into the health and security of the network; hence, it’s critical to collect, store and have access to all of it.

Store all logs centrally for the required time period

All information from network components (hardware, servers, application and homegrown systems) should be collected over geographically distributed locations and placed in a central archive. This archive should be stored long-term for regulatory compliance. Most regulations specify that log data should be stored for 1-7 years:

- 7 years for long-term archival
- 1 to 3 years for immediate forensics and compliance access
- 90 days online for operational use

Implement regular tasks

Although some tasks, such as user activity monitoring, must be completed on a daily basis, others are required on a weekly, monthly or even as-needed basis. It's important to determine ahead of time how often to perform critical tasks. IT controls frameworks and best practices provide recommendations for the frequency of specific tasks. Automated alerts are helpful for as-needed tasks such as monitoring excessive failed user logins or IDS attacks, or reviewing change management requests. Automated reports ease the hassle of daily and weekly tasks like reviewing user access logs or configuration changes, or ensuring backups are conducted properly. Ten Steps to Continuous Compliance: Putting in Place an Enterprise-Wide Compliance Strategy.

Implement and verify continuous monitoring

Alerting mechanisms and scheduled reporting let IT personnel know when a component, system or application is not complying with set policies. During an audit, auditors will want specific information about incidents that occurred and what was done to mitigate or resolve the incident. Questions may include:

- What active alerts are set to monitor these controls?
- What was the actual alert you received?
- Where is the evidence that you acknowledged the alert?
- Where is the evidence that you investigated the incident?
- Where is the evidence that you are periodically reviewing user logs?
- Where is the evidence that you have removed terminated employee accounts?

Demonstrate compliance status to auditors

Using alerts and scheduled reports, you can also demonstrate compliance status to auditors. Alerts should be set based on compliance with SOX, PCI, ISO17799, HIPAA or whatever regulation or best practice you are implementing. Then, reporting can be used to demonstrate compliance. An auditor might want to see the actual report that you are using for demonstrating the segregation of duties, for example. Log Management and Intelligence solutions provide report templates that map to common IT control frameworks to simplify compliance reporting.

Substantiate reports and alerts

Alerting and reporting on logs must be substantiated with immutable log archives. It's critical to store logs centrally with a long-term archival solution that preserves the integrity of the data. Immutable logs require time stamps, digital signature, encryption and other precautions to prevent tampering, both during transit of the data from the logging device to the storage device, as well as during archival.

A cross-functional effort

Compliance is no longer an isolated IT project; it’s an enterprise-wide endeavor that requires cooperation between business units and a deep understanding of the requirements, regulations, mandates and IT controls necessary for your particular industry and business. Compliance must be looked upon as a business issue that requires a cross-functional approach, involving people, processes, and technology across the enterprise. Taking the steps necessary to understand, define and implement the appropriate IT controls and frameworks for your business will simplify compliance and reduce the costs and resources involved in completing compliance related tasks.