



Sarbanes-Oxley (404) Network Assessment and Compliance

360 GRC
Whitepaper



Audit IT, Trend IT, Solve IT

SOX Compliance

What is the history behind Sarbanes-Oxley Act (SOX)?

In 2002, the U.S. Senate added the Sarbanes-Oxley Act (SOX) to the network of securities regulations in order to keep corporate America in check. It was named after its sponsors - U.S. Senator Paul Sarbanes (D-MD) and U.S. Representative Michael G. Oxley (R-OH). This Act was created to protect investors and the U.S. economy from the threat of scandal and corruption by publicly traded companies. That legislation became effective after a series of accounting scandals led to the failure of several major corporations (Enron, WorldCom, Tyco International, Adelphia), the conviction and imprisonment of multiple key executives, and the failure of a major public accounting firm (Arthur Andersen).

SOX -- What is it?

Essentially, SOX requires that every publicly traded company's executive members evaluate and maintain responsibility for the accuracy and completeness of all financial information that is released to the public. This Act also requires that companies release information regarding those controls that are in place in order to ensure the accuracy of their financial information.

SOX contains 11 titles that describe specific mandates and requirements for financial reporting. Each title consists of several sections.

Title I consists of nine sections and establishes a new regulatory authority to set public accounting auditing standards. The Public Company Accounting Oversight Board (PCAOB), which essentially replaced the American Institute of Certified Public Accountants' (AICPA's) self-regulated auditing rule-setting authority, provides independent oversight of public accounting firms that are performing audit services ("auditors"). It also creates a central oversight board tasked with registering auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

SOX changes many of the processes that public companies had used for their own governance, to report their financial results to the Securities and Exchange Commission (SEC) in the United States, and to their investors. These SOX initiated changes touch boards of directors, senior management practices, and the adequacy of the internal controls used to support their financial and other processes.

The most important sections of SOX for the senior managers, the board, internal audit, and other key members of the management team are:

- **Section 302:** Corporate Responsibility for Financial Report
- **Section 404:** Management Assessment of Internal Controls
- **Section 409:** Real Time Issuer Disclosures

While many portions of SOX may require changes and adjustments, Section 404 rules on internal controls have caused management and internal auditors the greatest level of pain and suffering. Strictly interpreted, the legislation laid out some very tight internal control compliance rules.

SOX Compliance

SOX Section 404: What does it mean to you?

In compliance with SOX Section 404, each annual report must include a statement by executive officers to the effect that they are responsible for the establishment and maintenance of the internal control structure and other procedures for financial reporting. In addition, the Internal Control Report must also include an assessment of all internal controls related to the financial information that has been released. This assessment is required to inform investors not only about the structure of the controls, but also about their efficacy.

What is at stake if you don't follow the rules?

SOX was created to address the accounting deficiencies and hold senior managers – specifically the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) – criminally and civilly accountable for the financial reports and internal controls of their company.

Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. Section 304 requires that if an enterprise is required to restate its earnings due to some material violation of securities laws, the CEO and CFO must reimburse the company for any bonuses or incentives received on the basis of the original, incorrect statements issued during the past 12 months. The same applies for any profits received from the sale of enterprise securities during that same period.

Title IX increases criminal penalties for white-collar crimes and also contains the legal penalties for executives who do not certify the accuracy of the company's financial reports or who certify reports that do not meet SOX compliance standards.

In addition to civil lawsuits and damage their image in the marketplace, CEOs and CFOs of companies that are non-compliant with SOX are subject to financial penalties and potential incarceration.

Situations where willful deceit can be proven carry fines of up to \$1 million and 10 years in prison. However, in the event that wrongful certification has been submitted intentionally, the maximum penalty rises to \$5 million and 20 years in prison.

So what are you required to do to comply with SOX mandates?

Information Technology (IT) controls are specific activities performed by persons or systems designed to ensure that business objectives are met. They are a subset of an enterprise's internal control. IT control objectives relate to the confidentiality, integrity, and availability of data and the overall management of the IT function of the business enterprise.

IT controls are often described in two categories: IT general controls and IT application controls. IT general controls include controls over the IT environment, computer operations, access to programs and data, program development and program changes. IT application controls refer to transaction processing controls, sometimes called "input-processing-output" controls. IT controls have been given increased prominence in corporations listed in the SOX Section 404.

Below are four key network compliance capabilities that are required by IT Risk Professionals (IRP):

- Access Control – ensure only authorized personnel have access to your network infrastructure. Produce audit reports that document and verify this. Any user authentication should be configured

SOX Compliance

to meet best practices and ensure adherence to institutional policy. If there is an attempt to gain access to the network infrastructure, you should be able to detect it and alert the appropriate personnel.

- Track and report user activities – who made what changes and when and where did they make the change(s) to the network infrastructure? A managed enforcement process must be in place in order to insure and verify uniform and compliant configurations when network operators import, edit, update and restore configurations to the network.
- Inventory Management – Clearly document your network infrastructure’s configurations, including device name, IP address, access method, vendor and model, and physical location. You must be able to document current network status, as well as provide historical reports that verify consistent internal auditing.
- Configuration Management – Track and report every configuration change to network equipment.

Can an audit be performed on the network to ensure SOX compliance?

Unfortunately, most SOX regulated entities are not placing any emphasis in complying with SOX on the network. A minority of covered entities are trying to comply by manually auditing their network configurations or using a home grown script to inspect individual device settings. To ensure 100% compliance, the Information Risk Professional should review each line of every network device’s configuration file and try to ensure that it matches the applicable PCI mandates.

There are several potential risks and problems with this approach:

- The process can be tedious and time consuming, even in small IT environments. Therefore audits are not performed or only in a minimum number of network devices. This can expose non-compliance with the remaining devices.
- The process leaves much room for error, as it’s easy to overlook a device or setting due to the technical nature of the review.
- Performing routine audits can be costly and difficult, especially in large environments in which changes are frequent and thousands of devices must be examined.

Summary

Although some vital differences exist among the various regulations, all share one unifying factor: they all deal with fundamental issues of data security and privacy. In IT, an optimal way to address regulations is first to understand the potential threats and vulnerabilities of the data and the network then create an effective and secure technology solution built on a well-designed infrastructure.

This approach enables an organization to easily deal with any new regulations that become law. Many organizations have invested in well-designed network infrastructures, but they still need an upgrade or a technology refresh to achieve a comprehensive solution to meet their regulatory compliance challenges.

About 360 GRC

360 GRC is headquartered in Manhattan, New York. 360 GRC’s management team includes over 100+ years in global enterprise Architecture and over 50+ years in IT Audit and IT Security field in top global organizations.

To learn more, visit www.360grc.com

© 2010, 360 GRC Inc.

The information contained herein is subject to change without notice. The only warranties for 360 GRC products and services are forth in the express warranty statement accompanying such products and services. 360 GRC shall not be liable for technical or editorial errors or omissions contained