solarwinds

SIMPLIFYING SOX COMPLIANCE FOR IT PROFESSIONALS

SOLARWINDS
WHITEPAPER

SIMPLIFYING SOX COMPLIANCE FOR IT PROFESSIONALS

You've probably heard people discussing the Sarbanes-Oxley (SOX) Act, or have read something about it online, but you may still be wondering how it impacts your work as an IT professional.

It's pretty straightforward: If you work for a U.S.-based, publicly traded organization, a U.S.-based privately held company poised for IPO, or a subsidiary of a foreign company that is based in the U.S., and you are responsible for the IT used to maintain that company's electronic financial records, you are required to comply with SOX.

The Sarbanes-Oxley Act was enacted by Congress in reaction to a number of corporate accounting scandals uncovered in the early 2000s. Its purpose is to force organizations to adopt a level of financial transparency that would prevent future fraudulent activities. The work of maintaining SOX compliance touches every aspect of IT operations involved in the financial and accounting functions within an organization.

Your company must configure the entire IT infrastructure, from IT processes and operations to network and server security to be able to maintain and then demonstrate SOX compliance. Almost every aspect of your IT operations are affected by SOX compliance, which can include any communications relating to finance or accounting that your company transmits via new communication platforms, such as social media, blogs, intranets, or wikis.

This paper offers an overview of the Sarbanes-Oxley Act, the concerns it poses for IT professionals, guidelines for data archiving and storage to meet SOX retention regulations, and the codes of ethics, processes, financial reporting, and procedures of which you need to be aware.

While SOX compliance regulations apply mainly to publicly listed institutions, Section 802 of the Sarbanes-Oxley Act states that anyone who knowingly "…alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence…" a federal investigation can be fined and subject to up to 20 years imprisonment. So, clearly, the stakes are high.

Finally, while you may not currently work for a company that must maintain SOX compliance, if you do business with a public company, you may be required to prove compliance. There are benefits to educating yourself on the Sarbanes-Oxley Act's requirements and working toward compliance, primary among them is improved security for your firm.

A BRIEF OVERVIEW

The Sarbanes-Oxley Act, enacted July 30, 2002, was designed to protect the public and company shareholders from unethical and illegal financial business practices. While the SOX Act's primary purpose is to prevent fraudulent activity by public company executive officers and directors, it impacts company IT practices profoundly. In addition to assisting with the safekeeping of financial data, business processes involved in meeting and maintaining compliance are becoming increasingly reliant on technology for timely, comprehensive, and accurate execution.

Every year, the cost of SOX compliance rises, which affects company budgets, time, and personnel. According to the 2015 Sarbanes-Oxley Compliance Survey, over half of large corporation respondents spent more than $1 million for SOX compliance. Many businesses are paying particularly close attention to the strength of IT controls and high-risk process management.

The IT department, specifically its information security professionals, has a fundamental role in maintaining SOX compliance. Without strong data management practices, companies face penalties, including steep fines, and their top executives can be held liable and face criminal prosecution and imprisonment. This is a grave responsibility for IT professionals, particularly those who handle compliance-related data and data management solutions. Developing a basic understanding of SOX and its broad technical implications is essential.

What is the Sarbanes-Oxley Act?

The Sarbanes-Oxley Act is federal financial reporting compliance legislation that was enacted to protect investors and others from the effects of poor accounting practices and acts of fraud. The SOX Act contains 11 sections, which outline the financial responsibilities of companies and the penalties for noncompliance.

The act's name comes from its two writers, Sen. Paul Sarbanes and Rep. Michael Oxley. It mandates complete disclosure and transparency among board members, executives, and corporate auditors. Today, a CEO or a CFO cannot get away with feigning ignorance about a financial error or suspicious recordkeeping. Every CEO and CFO of a public company must verify the accuracy of all financial reports submitted to external auditors and in Securities and Exchange Commission (SEC) filings.

A Brief History of SOX

The Sarbanes-Oxley Act followed in the wake of some of the worst corporate scandals in American history. Enron, an energy and commodities company, and WorldCom, a telecommunications company, were each involved in financial scandals that eroded investor and stakeholder confidence. Enron failed to record enormous debts in its financial statements, and an insider blew the whistle on the company. WorldCom failed to report certain line costs and fraudulently inflated revenue streams. Arthur Andersen, a large accounting firm, was implicated in the Enron scandal as the organization failed to handle its Enron accounts accurately.

These and several other corporate financial scandals came to light in 2001 and 2002, spurring Congress to take action. In the same timeframe, the stock market took a dive due to the dot-com crash of 2012. The U.S. was in a financial crisis, and so the executive and legislative branches of government decided to take action. Among those actions was the passage of the SOX Act, which was enacted into law with an overwhelming majority in the House and Senate. The SEC was tapped to take responsibility for tracking companies and enforcing the tenets of the act.

Major Elements of the SOX Act

The full text of the Sarbanes-Oxley Act is available on the SEC website and outlines requirements public companies must follow in their financial practices. Here is an overview of its principal elements:

- **Corporate governance:** Section 302 describes the responsibilities of the CEO and the CFO regarding information they must include in financial reports and filings.
- **Audit stipulations:** Section 201 designates activities that auditors may not participate in while performing corporate audits. For example, a financial institution may not engage in bookkeeping, financial records system designs, or actuarial services if the organization also performs auditing services.
- **Internal controls:** Section 404 requires public companies to create and maintain an appropriate internal structure and oversight procedures for financial reporting. Companies must conduct annual internal evaluations and reporting to assess the relevance of existing practices.
- **Financial disclosure:** Section 409 amends section 13 of the Securities Exchange Act of 1934. Under the revised rules, all issuers required to disclose information under section 13(a) or 15(d) of the Securities Exchange Act must also disclose relevant financial information to the public using plain English.
- **Penalties for altering financial documents:** Section 802 outlines the criminal repercussions individuals can expect if they knowingly alter, destroy, conceal, or falsify financial records. Penalties include a prison sentence of up to 10 years.
- **Penalties for fraud:** Section 807 outlines the criminal repercussions for fraud against shareholders or others. Securities fraud is punishable by a prison sentence of up to 25 years and/or a steep fine.
- **Whistleblower protections:** Section 806 provides protections for employees who discover and notify authorities about instances of fraud.

These key sections highlight much of the actionable material within SOX. Sections 302 and 404, however, directly relate to the role of IT professionals in SOX compliance.

SOX SECTION 302

Section 302 requires the principal executive officer or officers (the CEO and CFO) to formally verify the information submitted in quarterly and annual reports filed under the Securities Exchange Act of 1934. Certifying the report tells the SEC that the officer(s):

1. Reviewed the contents of the report.
2. Acknowledged that the report contains no omissions or false statements.
3. Agreed that the information provided in the report fairly represents the financial well-being and operations of the company.
4. Recognized the need to create and govern internal controls, design appropriately transparent controls, evaluate the efficacy of all controls before certifying the report, and present results of the evaluation within the report.
5. Disclosed any deficiencies within the internal controls and any instances of fraud to the auditors involved.
6. Indicated within the report if the company made any changes to internal controls or related areas that could affect the truthfulness of its evaluations.

While Section 302 clearly indicates the importance of a clear strategy for internal controls, it does not list a specific number or type of internal controls a company must use or assess. Every company is responsible for developing its internal controls infrastructure.

SOX SECTION 404

Section 404 is often regarded as one of the most complex and costly compliance sections of SOX. This section requires companies to develop a formal report about the scope and effectiveness of its internal controls structure for financial reporting. The section also requires auditors involved with public companies to evaluate and report on their clients' internal controls assessments. Making sure that all of these details are accurate and tracked on a daily basis can utilize a significant amount of company resources, including the IT department.

THE IMPACT OF SECTIONS 302 AND 404 ON IT DEPARTMENTS

SOX Sections 302 and 404 outline the primary compliance issues executive officers ask IT departments to address. Specifically, these sections highlight the need to protect the integrity and security of all financial information stored on paper and in digital formats. The sections also set an expectation that each company develop an internal strategy to control, audit, and optimize the system on an annual basis.

Information security is not outlined directly in the language of SOX, but strong IT oversight is the logical answer to maintaining adequate internal controls. For a company to remain in compliance with SOX, it must demonstrate data control and robust security.

HOW DOES THE SOX ACT WORK?

Publicly listed companies are responsible for understanding SOX and developing a financial records strategy and framework that provides clear and traceable financial data. Any time a company modifies its internal control structure or a file within the record-keeping pipeline, it must document the change by providing the following details: What was revised, why it was changed, when the information was modified, and who performed the revision.

Many companies choose to use generalized frameworks that most auditing institutions accept. COSO and COBIT are two popular frameworks companies use to develop and maintain internal controls. They help IT departments address the basics of internal control – the infrastructure environment, potential risks, communication monitoring, and management controls, and oversight.

Organizations typically work with external auditors to ensure their approaches comply with SOX requirements. These auditors are responsible for conducting intensive testing to confirm the adequacy of all internal controls. Throughout the year, the company and external auditors work together intermittently to adjust internal controls and optimize certain areas. Before the end of the fiscal year, the external auditing partner conducts a final test to ensure the quality and accuracy of a finalized internal report.

The external auditors are responsible for submitting a formal opinion regarding the overall compliance of the company. During the SOX testing periods, company CEOs, CFOs, and IT professionals are in the spotlight. They are responsible for maintaining a high-quality system of internal controls. To facilitate this process, PricewaterhouseCoopers, LLC (PwC) has created a checklist of SOX compliance requirements and timeline for complying with each.

REQUIREMENTS FOR SOX COMPLIANCE IN IT

IT professionals must create and maintain internal systems of control for financial reporting that comply with SOX requirements. Specifically, this involves:

- **Creating a security policy:** Security policies protect the integrity of the data a company keeps for compliance. A robust security policy covers all digital communications, software as a service (SaaS) subscriptions, electronic file recordkeeping, paper file practices, and other forms of documentation associated with financial records.
- **Maintaining network security:** To protect data from corruption and cyberattacks, IT professionals must adequately secure the company's network. Cybersecurity for file transfers, patching OS and application vulnerabilities, and using network best practices such as maintaining firewalls all play a vital role in SOX compliance.
- **Developing transparent change and security logs:** SOX requires businesses to keep traceable lines of financial information. For IT professionals, this means developing a system for reporting changes, invalid logins, access requests, and error remediation easily.

These examples represent a small portion of IT activities specifically related to SOX compliance.

THE SOX AUDIT PROCESS

Under SOX requirements, companies undergo internal and external auditing processes. Internally, the company develops a report on internal controls per Section 404 stipulations. The internal document confirms the accuracy of financial data and the efficacy of internal controls. Internal auditors often use a framework such as COBIT to inspect the company's existing controls and financial recordkeeping practices thoroughly.

External SOX auditors go through the information listed in the internal report and verify the report's findings based on experience. They then offer final opinions relating to the overall efficacy of the program, and deliver an official notice regarding the quality of financial statements the SEC requires. External auditors are trained to look for discrepancies, misstatements, and errors in internal controls and financial reports.

WHAT IF A SOX AUDIT FAILS?

Certified internal reports confirm the executive officers' compliance with SOX. If a SOX regulator finds a purposeful error within a company's certification, the CEO and/or CFO can face a $5 million fine and up to 25 years in prison.

Businesses can perform an interim audit and, if it fails, can use that as an opportunity for the company to make adjustments or repair any errors. An external auditor outlines any problems found within the internal controls and reports. Auditors may deliver a report of issues but may not provide possible solutions. Companies can use the information provided by auditors to overcome potential compliance problems and reduce the risk of noncompliance, something that can permanently harm a company's reputation.

OPTIMIZING SOX COMPLIANCE MANAGEMENT

Whether your organization is working toward SOX compliance or another regulatory requirement, compliance management involves the same basic process. You need a formal policy, procedures, controls, and a testing or verification process (audits). And, of course, to support that verification process, documentation is key. IT professionals should invest in resources that not only contribute to the security objectives of a compliance framework, but also help withstand audits and avoid the many negatives associated with noncompliance.

The Sarbanes-Oxley Act affects IT professionals in all publicly traded companies, and can impact some privately held firms as well, so you'll need to work in close collaboration with SOX auditors, internal compliance specialists, and executive management to develop an approach to compliance

that works for your business. The right combination of resources, education, and due diligence not only improves compliance results, but also enhances a company's credibility, reputation, and helps build long-term financial security.

SOLARWINDS LOG & EVENT MANAGER

SolarWinds® Log & Event Manager is an affordable, award-winning SIEM solution that produces out-of-the-box compliance reports for SOX. Log & Event Manager can be installed in minutes and easily generates compliance reports quickly using audit-proven templates.

NEXT STEPS

1. Watch this Continuous Compliance with SolarWinds Log & Event Manager video that provides an overview of SOX and other compliance frameworks, the ramifications of not maintaining compliance, and how SolarWinds Log & Event Manager can help in your security and compliance efforts.

2. Try **SolarWinds Log & Event Manager** for yourself. Download a free 30-day trial and have it up and running in less than an hour.

ABOUT SOLARWINDS

SolarWinds provides powerful and affordable IT management software to customers worldwide from Fortune 500® enterprises to small businesses, government agencies and educational institutions. We are committed to focusing exclusively on IT Pros, and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale while providing the power to address all key areas of the infrastructure from on premises to the Cloud. Our solutions are rooted in our deep connection to our user base, which interacts in our THWACK® online community to solve problems, share technology and best practices, and participate in our product development process. Learn more today at http://www.solarwinds.com/.

*For additional information, please contact SolarWinds at 866.530.8100 or e-mail **sales@solarwinds.com.***
*To locate an international reseller near you, visit **http://www.solarwinds.com/partners/reseller_locator.aspx***