ManageEngine
Log360

The role of IT in achieving SOX compliance

www.manageengine.com/log-management

Introduction

In 2002, U.S. Congress passed the Sarbanes-Oxley Act (SOX) to protect the interests of shareholders and the general public. The act guards against errors and malpractice in enterprise accounting systems and policies by mandating adequate security measures, transparent procedures, and accurate corporate disclosures.

SOX was drafted in response to accounting scandals at prominent companies like Enron and Arthur Andersen, which caused investors to lose billions of dollars. By improving corporate governance and accountability, the act aims to minimize the chance of fraudulent accounting practices by enterprises and auditing firms.

All companies—American or otherwise—which are registered with the Securities and Exchange Commission (SEC), along with those companies which provide financial services to these companies, must comply with this act. This means that all publicly-traded U.S. companies, publicly-traded non-U.S. companies with a U.S. presence, companies looking to go public, and companies providing all of them with financial services are subject to SOX compliance.

SOX compliance requires major contributions from the finance and IT departments of an enterprise. This paper concentrates on the IT side of achieving SOX compliance.

SOX sections relevant to the IT department

Section	What it's about
Section 302: Corporate responsibility for financial reports	The principal executive and financial officers of a company bear ultimate responsibility for the accuracy of financial reports and internal controls in place over the accounting systems.
Section 404: Management assessment of internal controls	All annual financial reports must include an internal control report, which: a. States that management is responsible for the internal control structure. b. Includes an assessment of the effectiveness of the internal control structure. c. Requires a registered external auditor to attest to the accuracy of this assessment.
Section 409: Real time issuer disclosures	Companies must disclose to their stakeholders and the general public any information which could affect their financial condition or operations, in a rapid and timely manner.
Section 802: Ensure records retention	All physical and electronic communications and other records related to a company's financial transactions are to be retained and made available to external auditors for a minimum of five years.

How IT can aid in SOX compliance

Given that most financial records are stored electronically, your organization's IT processes and systems play a key role in achieving SOX compliance. Financial data lost or damaged due to error or carelessness is not a valid excuse for non-compliance. According to section 302, senior executives must be able to state that all sensitive data was stored and processed securely. A completely accurate financial report can still be called into question if weaknesses are exposed in the company's IT systems. This is why an organization's security policies, backup systems, and audit reports must be ironclad.

To adhere to sections 302, 404, 409, and 802 of SOX, IT teams should:

- Supply senior executives with in-depth audit reports in accordance with the internal control structure.
- Keep IT systems up-to-date and constantly monitor for any security loopholes.
- Identify and secure all devices, applications, and IT processes that deal with sensitive financial data.
- Test all systems and applications for weaknesses.
- Set up alerting mechanisms to detect security incidents on time.
- Investigate and respond to incidents efficiently to minimize damage and create detailed forensic reports.
- Have a system in place to communicate confirmed incidents to all stakeholders.
- Consolidate all financial records, communications, and related logs and store them securely.
- Set up automated back up procedures and test them periodically.
- Guard against employee error by offering awareness programs on phishing and other social engineering attacks.
- Define clear access policies and ensure users are only given the rights they need to perform their jobs.

Achieving SOX compliance with Log360

Log360 helps your organization achieve SOX compliance by helping you audit and secure your sensitive financial records. With Log360, you can audit activities related to confidential financial data and secure that data from unauthorized accesses and attacks; investigate potential security incidents; and safely retain audit logs for as long as necessary.

Section 302: Corporate responsibility for financial reports

Log360 comes with over 1,200 intuitive, predefined reports detailing the various activities on your network. This includes activities in your Windows, Unix, and IBM systems, applications, network devices, file servers, as well as your Active Directory, Office 365, and Exchange Server environments. You can even build custom reports for in-house financial applications using the custom log parser.

You can use these reports to keep senior executives informed about the safety and integrity of important financial data. Required reports can be exported or scheduled as needed, and multiple customization options are available. Additionally, role-based access control allows you to restrict the viewing of these reports to authorized users.

Highlights

Comprehensive network auditing | Custom log parser | PDF and CSV report exporting | Report scheduling | Report customization | Role-based access control

Section 404: Management assessment of internal controls

To set up effective internal controls over your accounting systems, you need to consider several aspects of network security. Log360 helps you cover the following areas:

- **Audit accesses and changes to confidential financial records.** Preserve data integrity and prove that data was handled properly by providing detailed audit trails. You can also generate reports to prove that your data is regularly backed up and can be restored in the event of any damage.
- **Monitor privileged user activity.** Ensure that privileged accounts are not compromised, and they are used responsibly.
- **Detect attacks across your network.** Get instant notifications for:
  - Suspicious activity patterns correlated across multiple devices.
  - Attacks detected by your firewalls, IDS/IPS, and other network devices.
  - Malicious entities interacting with your network.
  - Anomalies detected within your Active Directory, Office 365, Exchange Server, and file server environments.
  - Other suspicious events like policy changes, logs being cleared, etc.
- **Provide transparency on network status.** Report on vulnerabilities, viruses, system crashes, and other issues discovered in your network. SOX requires transparency on all issues which could affect the security of your financial records, and these reports help you provide it.

Highlights

Predefined SOX compliance report | DDL/DML reports | Windows and Linux file integrity monitoring | Privileged user monitoring | Event correlation | Threat intelligence | Vulnerability reports

Section 409: Real-time issuer disclosures

SOX requires public disclosures on "a rapid and current basis" of any events which could affect the financial status of a company. These events include security breaches of your financial systems or data. To confirm that a security incident has taken place or is taking place, you must be able to conduct a thorough forensic investigation in a timely manner. Log360's search engine facilitates quick investigations and allows you to arrive at the root cause of an incident with minimal effort.

Its built-in ticketing features and help desk integrations also allow you to streamline incident management. By automatically assigning incident tickets, tracking their status, and maintaining an internal knowledge base of past incidents, you can oversee a smooth incident resolution process.

Highlights

Advanced search engine | Built-in ticketing console | External help desk integrations

Section 802: Ensure records retention

Records pertaining to all financial transactions and communications must be retained for at least five years for an organization to be compliant with SOX rules. Logs are an important part of these records. With Log360, you can choose how long you wish to retain your logs, and you can import the archived logs at any time for further investigation. Logs are transmitted and stored in a secure, tamper-free manner to ensure that they cannot be called into question in the event of an audit.

Highlights

Flexible duration log retention | Tamper-free archival | Secure web communication | Historic log import

Conclusion

IT plays an important role in supporting an organization's journey towards SOX compliance. With its comprehensive log management and security features, Log360 helps IT administrators build a strong internal control system to safeguard a company's sensitive financial data.