Sox and IT

How the Observer® Performance Management Platform can help IT Professionals comply with the data practices components of Sarbanes-Oxley.

Executive Summary

U.S. Congress passed the Sarbanes-Oxley Act of 2002 (SOX) to stabilize U.S. markets in light of recent corporate scandals (Enron, WorldCom) that cost investors millions of dollars and deflated the U.S. economy. This Act reforms corporate governance particularly by adding integrity to internal processes that affect earnings and financial disclosures. Ultimately, these changes are supposed to regain consumers' trust in publicly traded companies and help them make appropriate investing decisions.

In general, SOX requires publicly traded companies to be more financially accountable. However, becoming more responsible extends beyond the accounting department–complying with SOX requires cooperation and support among many business units, including IT.

IT supports the corporation's drive to comply with SOX by securing and protecting financial data on the network. IT is also required to consistently document this effort. Without IT support, a corporation simply cannot comply with SOX and will endure retribution from the Securities and Exchange Commission, which regulates SOX.

The Observer Platform can help support IT's role in SOX compliance by securing, monitoring, and documenting financial and other activity on the network.

The purpose of this document is to provide a brief overview of SOX, and how the Observer Platform can help IT fulfill its responsibilities.

SOX Summary

Most of the IT department's responsibilities in the SOX Act fall under sections 302 and 404. Section 302 requires the public company to affirm in each report that internal controls are adequate and they have not disclosed any knowingly false or misleading statements–presenting a fair representation of financial conditions. Both the public company's officers and public accounting firm must attest to the accuracy of the reporting. Any significant deficiencies found in the internal controls or fraud that involves management or employees must be reported.

Section 404 requires reports to identify management's responsibilities for establishing and maintaining adequate internal controls, and provide an assessment of the effectiveness of the internal controls and procedures affecting financial reporting. The public accounting firm must attest once again to the fairness and accuracy of the reporting.

Refer to the Appendix for the exact excerpt for sections 302 and 404 of the SOX Act.

Sarbanes-Oxley requires publicly traded companies to be more financially accountable.

Auditing Frameworks

There is a lot of room for interpretation of SOX–the Act does not specify a specific internal control framework or IT governance practice appropriate for compliance. In addition, the auditors who are required to attest to financial reports are typically not experts in IT technologies. To overcome these challenges, SOX references the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework. COSO provides an integrated framework to help businesses assess and enhance their internal control systems and align their IT governance practices with SOX.

There are five main components of the COSO framework that are relevant to SOX:

Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring.

1) Internal Environment

The Internal Environment depicts the company's philosophy for risk management and sets the basis of integrity and ethics they oblige to uphold in the environment.

2) Risk Assessment

The purpose of Risk Assessment is to identify potential risks (security breaches, for example), the likelihood of those risks, and the consequent ramifications of those risks to determine how they should be managed.

3) Control Activities

This includes all the policies and operating procedures that are established to mitigate the risks identified in the Risk Assessment and ensure risk responses are handled appropriately. These activities should address the organization of and controls for information systems, as well as specific application guidelines to support accurate and timely processing of transactions.

4) Information and Communication

When creating the standard operating procedures, management must consider the flow of information within the company to ensure it effectively supports employees' activities. In addition, all relevant data needs to be identified, captured, and presented in a coherent format.

5) Monitoring

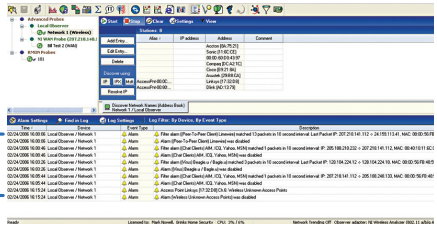
Internal controls need to be monitored on a continual basis to ensure the security and integrity of the information flowing throughout company and the validity of the corresponding reports. Modifications to internal controls should be made as necessary and recorded in the disclosure.

The Observer Platform's Role in SOX

The Observer Platform can be an essential tool for an IT administrator to have in place throughout the reporting period. The following technical brief outlines how this powerful solution can help comply with the data practices components of SOX.

Risk Management

Real-time monitoring for security breaches, plus the ability to measure server and application availability and performance should be part of any comprehensive risk management plan. Observer Analyzer's Triggers and Alarms can log many common threats to performance and security, including viruses, illegal peer-to-peer activity, and broadcast storms.

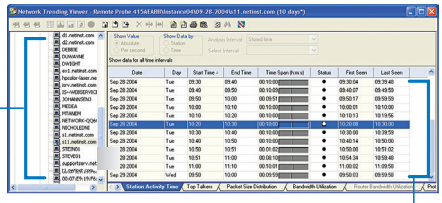


Alarms identify network threats.

Documentation

According to section 302 of the SOX Act, internal controls need to ensure that the information flowing within the company, and the devices involved in the processing, recording, and storage of financial information, is documented and appropriately isolated. The Observer Platform's network trending capabilities capture network activity over long periods of time, making it especially useful for validating the IT component of financial reports during the reporting period. Network trending reports allow the CIO to certify the integrity of financial data in the following ways:

- **Station Activity** time can reveal which systems participated on the network during the reporting period. For example, the functionality status of central servers and retail branches during the reporting period can be identified.

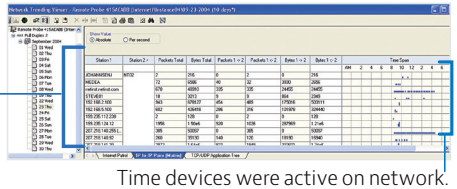


Systems that participated on network.

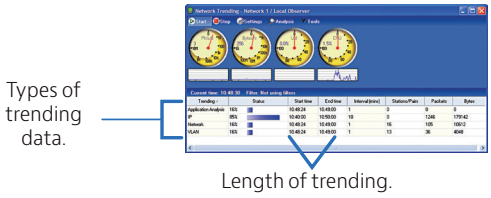
Time systems participated on network.

Observer Analyzer's trending captures network activity over long periods of time, making it useful for validating IT compliance.

- The Observer Platform's **IP to IP Pairs** and **Internet Patrol** can show what "conversations" took place for key systems during the reporting period–both by identifying when the communication occurred and with which systems. This can, for example, prove that only authorized systems accessed servers storing confidential financial information.

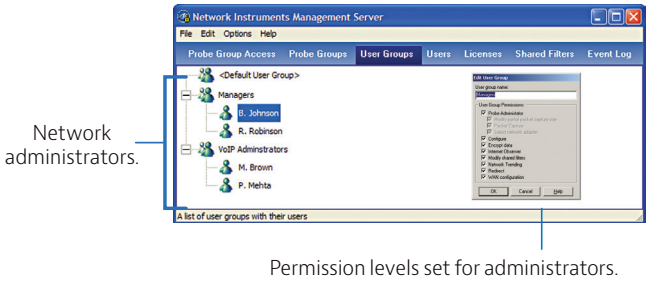


- The Observer Platform can collect **trending** data across all supported topologies (802.11 a/b/g, gigabit, Ethernet, WAN). Therefore, if the financial system depends on WAN links, deploying a Network Instruments WAN hardware probe to collect trending data can help prove that key WAN circuits were monitored and functional during the reporting period.



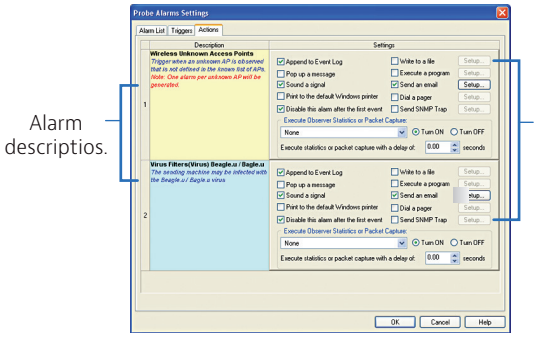
Secure Log-In

Observer Management Server (OMS) helps protect the integrity of financial data by retaining a list of usernames, passwords, and permission levels for multiple Observer Probes on the network. This ensures only designated administrators are managing specific activity. OMS also detects and documents all successful and unsuccessful login attempts to the management devices.



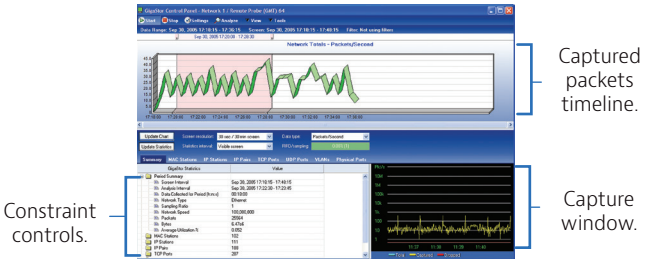
Warning System

The Observer Platform's Triggers and Alarms can also identify suspicious activity and automatically alert an administrator. For immediate response to problems such as a security breach, Triggers and Alarms can be configured to run a packet capture when problem activity is triggered–eliminating the need to manually track it down. This effort to immediately address problems can be documented, and is looked favorably upon by auditors.



Historical Analysis

Suspicious activity is not always immediately evident. With its simple time-based navigation utility and extensive storage capacity, Observer GigaStor™ makes it possible to sort through days, weeks, even months worth of network data down to the nanosecond. Therefore, an incident that occurred weeks ago can be quickly investigated and documented. The GigaStor can also reconstruct the stored data, providing hard evidence such as e-mails, web pages (including images), instant messages, and VoIP conversations.



The right network analyzer allows IT professionals to comply with data practices components of Sarbanes-Oxley.

Cost/Benefit Analysis

Adjusting internal control standards and IT governance processes to comply with SOX will naturally induce expenses, but these expenses can quickly escalate if not managed wisely. Utilize the Observer Platform to help manage and report on financial communications and network conditions–all while keeping expenses at a minimum. No other network monitoring solution can provide this much functionality and security in one solution, and at such a reasonable price.

Flexible reporting of network activity like that offered by Observer simplifies SOX compliance.

Conclusion

IT has been designated as a key role player in SOX compliance. Although it may take considerable effort to coordinate management philosophies and implement an organized and acceptable set of standards, SOX compliance can ultimately enhance business functions–not just please the SEC. Relying on the Observer Platform to help support the company's mission to comply with SOX will make meeting those standards much easier and more reasonable than with any other tool.

The Observer Platform helps IT professionals comply with the data practices components of Sarbanes-Oxley in the following ways:

SOX Role	Observer Feature	Description
Risk Mangement	Triggers and Alarms	Identifies many common threats
Documentation	Station Activity	Reveals which system participated on the network during the reporting period
	IP to IP Pairs Internet Patro	Show conversations that took place between key systems
	Historical Analysis	Store days, even weeks' worth of network data, providing hard evidence of network communications including web pages, e-mails, phone conversations, and instant messages.
Security	Secure Log-in	Retains a list of permission levels on network probes to protect the integrity of financial data.
	Triggers and Alarms	Immediately alert IT of suspicious activity

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the Viavi office nearest you,
visit viavisolutions.com/contacts.

soxandit-wp-ec-ae
30176222 901 0914