

ADVENTNET INC.

# How IT Can Aid Sarbanes-Oxley Compliance

---

Whitepaper

**Notice:** This document represents the current view of AdventNet and makes no representations or warranties with respect to the contents as of the date of publication. AdventNet cannot guarantee the accuracy of any information presented after the date of publication due to continually changing market conditions.

## About Sarbanes-Oxley Act:

The Sarbanes-Oxley Act, SOX in short, came into reckoning in July 2002. This act effected major changes in corporate governance and financial reporting with the objective “to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws”. The SOX Act is categorized into 11 titles with sections 302, 404, 401, 409, 802, and 906 being the most significant ones. Section 404 and (to some extent) Section 302 lays the foundation on how IT can aid SOX compliance.

## Section 404 - Management Assessment of Internal Controls

This section pertains to the guidelines laid down by the Securities and Exchange Commission on what SOX demands. According to the SEC, companies must: "Include in their annual reports a report of management on the company's internal control over financial reporting".

The control report must include:

- "A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting."
- "Management's assessment of the effectiveness of the company's internal control over financial reporting."
- "A statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting."
- "A statement that the registered public accounting firm that audited the company's financial statements...has issued an attestation report on management's assessment of the company's internal control over financial reporting."

## Section 302 - Corporate Responsibility for Financial Reports

For each company filing periodic statutory financial reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 it is required to include certifications that:

- The signing officers have reviewed the report.
- The report does not contain any material untrue statements or material omission to make the statements considered misleading.
- The financial statements and other related financial information fairly present the financial condition and the results of operations in all material respects.
- The signing officers are (a) responsible for internal controls (b) designed such internal controls (c) have evaluated these internal controls within the previous ninety days and (d) have reported on their findings.

- The signing officers have disclosed (a) all deficiencies in the design or operation of internal controls and (b) any information on any fraud that involves employees who are involved with internal activities.
- The signing officers have indicated any significant changes in internal controls or related factors that could have a negative impact on the internal controls.

By reincorporating their activities or transferring their activities or corporate locations outside of the United States organizations may not attempt to avoid these requirements

## SOX Requirements for IT

IT can aid Organizations to manage the internal controls and conform to the guidelines laid out in SOX. Its common knowledge that all network systems are capable of storing information of all the activities that took place within the system in their log files. These log files contain wealth of information which can be mined to obtain information on user level activities like logon success or failure, system level activities like file read, write or delete, host session status, account management and others. Monitoring these logs will assist in detecting system problems, and obtain log trail for forensic investigation. And generating reports for these activities provide management with internal control specified by SOX.

Section 802 of SOX mandates that records are maintained for seven years after the auditor concludes the audit. So it can be safely assumed that as far as system logs are concerned, they need to be stored or archived for posterity. Here again IT can handle this requirement by providing a centralized repository where logs collected from disparate systems can be collected, normalized, aggregated, and archived.

## Introducing ManageEngine® EventLog Analyzer

ManageEngine® EventLog Analyzer ([www.eventloganalyzer.com](http://www.eventloganalyzer.com)) is a web-based, agent-less syslog and windows event log management solution that collects, analyzes, archives, and reports on event logs from distributed Windows host and, syslog's from UNIX hosts, Routers & Switches, and other syslog devices.

EventLog Analyzer helps you to:

- Zero in on applications causing performance and security problems
- Determine unauthorized access attempts and other policy violations
- Identify trends in user activity, server activity, peak usage times, etc.
- Obtain useful event, trend, compliance and user activity reports
- Understand security risks in your network
- Monitor critical servers exclusively and set alerts

- Understand server and network activity in real-time
- Alert on hosts generating large amounts of log events indicating potential virus activity
- Schedule custom reports to be generated and delivered to your inbox
- Generate reports for regulatory compliance audits
- Identify applications and system hardware that may not be functioning optimally
- Centralized archival all collected logs
- And more...

## Using ManageEngine® EventLog Analyzer for SOX Compliance Audits

EventLog Analyzer lets corporations collect, retain and review terabytes of audit trail log data from all sources to support Sarbanes-Oxley Section 404's IT process controls. These logs form the basis of the internal controls that provide corporations with the assurance that financial and business information is factual and accurate.

The types of reports that EventLog Analyzer provides for SOX Audits are as follows:

**User Logon Report:** SOX requirements (Sec 302 (a)(4)(C) and (D) - log-in/log-out monitoring) clearly state that user accesses to the system be recorded and monitored for possible abuse. Remember, this intent is not just to catch hackers but also to document the accesses to medical details by legitimate users. In most cases, the very fact that the access is recorded is deterrent enough for malicious activity, much like the presence of a surveillance camera in a parking lot.

**User Logoff Report:** SOX requirements (Sec 302 (a)(4)(C) and (D) clearly state that user accesses to the system be recorded and monitored for possible abuse. Remember, this intent is not just to catch hackers but also to document the accesses to medical details by legitimate users. In most cases, the very fact that the access is recorded is deterrent enough for malicious activity, much like the presence of a surveillance camera in a parking lot.

**Logon Failure Report:** The security logon feature includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

**Audit Logs Access Report:** SOX requirements (Sec 302 (a)(4)(C) and (D) - review and audit access logs) calls for procedures to regularly review records of information system activity such as audit logs.

**Object Access Report:** Identify when a given object (File, Directory, etc.) is accessed, the type of access (e.g. read, write, delete) and whether or not access was successful/failed, and who performed the action.

**System Events Report:** Identifies local system processes such as system startup and shutdown and changes to the system time or audit log.

**Host Session Status Report:** Indicates that someone reconnected to a disconnected terminal server session. (This is only generated on a machine with terminal services running.)

**Security Log Archiving Utility:** Periodically, the system administrator will be able to back up encrypted copies of the log data and restart the logs.

**Track Account Management Changes:** Significant changes in the internal controls sec 302 (a)(6). Changes in the security configuration settings such as adding or removing a user account to a administrative group. These changes can be tracked by analyzing event logs.

**Track User Group Changes:** Tracking event logs for changes in the security configuration settings such as adding or removing a global or local group, adding or removing members from a global or local group, etc.

**Track Audit Policy Changes:** EventLog Analyzer lets corporations comply with internal controls sec 302 (a)(5) by tracking the event logs for any changes in the security audit policy.

**Successful User Account Validation Report:** Identifies successful user account logon events, which are generated when a domain user account is authenticated on a domain controller.

**Unsuccessful User Account Validation Report:** Identifies unsuccessful user account logon events, which are generated when a domain user account is authenticated on a domain controller.

**Track Individual User Actions Report:** EventLog Analyzer lets corporations comply with internal controls sec 302 (a)(5) by auditing user activity.

**Track Application Access:** EventLog Analyzer lets corporations comply with internal controls sec 302 (a)(5) by tracking application process.

## About AdventNet

*Enabling Management Your Way™*

Founded in 1996, AdventNet is a software company with a broad portfolio of elegantly designed, affordable products and web services. AdventNet offerings span a spectrum of vertical areas, including network & systems management (ManageEngine.com), security (SecureCentral.com), collaboration, CRM & office productivity applications (Zoho.com), database search and migration (SQLOne.com), and test automation tools (QEngine.com).

AdventNet and its global network of partners provide solutions to multiple market segments including: OEM's, global enterprises, government, education, small and medium-sized businesses and to a growing base of management service providers. [www.adventnet.com](http://www.adventnet.com), [www.zoho.com](http://www.zoho.com)