



Sarbanes-Oxley and Computer Log Files

The Answer to Compliance is in the Logs

Executive Summary

The Sarbanes-Oxley Act (SOX) of July 2002 weighs heavy regulatory compliance and financial reporting requirements for publicly held corporations. Designed to protect the investing public from officers and auditing firms that fraudulently misrepresent the financial stability of corporations, it mandates safeguards to assure greater financial accuracy, disclosures and controls. As a core component of a SOX compliance framework, log management solutions significantly complements a corporation's efforts to meet these cumbersome regulatory requirements.

As both "controls" and "evidence of controls", event logs of systems and user activity record transactions that form the basis to address information assurance and regulatory compliance issues. It establishes the means to bridge the gap between financial transactions and business controls that can affect the integrity of a company's financial status - translating SOX compliance policies and procedures into practicable IT audit solutions.

Specifically, event logs address important provisions of the Sarbanes-Oxley Act, such as Section 404's mandate that executive officers attest to the effectiveness of internal controls. With complete event log monitoring, reporting and assessment, organizations can demonstrate adherence to said internal controls. They can reduce the risk of public fraud disclosure and criminal penalties for altering documents under Section 802 by providing evidence of the retention and protection of financial audit records. They also facilitate the timely reporting and real-time disclosure requirements of Section 409, as well as Section 302's mandate that executives certify the accuracy of financial reports. Finally, effective log management enables corporations to demonstrate records file integrity, satisfying Section 1102's mandate against record tampering.

When event log aggregation, retention, correlation, reporting and investigation are properly implemented using best practices, compliance with SOX regulations becomes more attainable and cost-effective.

Overview

As knowledge becomes an increasingly vital corporate asset, a key challenge of our digital economy is coping with a relentless deluge of information. This information can converge to become knowledge, which includes an awareness of actions that produce known results—otherwise known as controls. This relationship between information, knowledge and controls is particularly relevant to corporate decision-makers because regulatory compliance — especially in light of the conformance deadline for the Sarbanes-Oxley Act -- is a moving target. The law's relative immaturity, vague implementation guidance, and a lack of precedents against which to measure exposure to legal risks, combined with numerous solutions produce an environment characterized by uncertainty and confusion.

Some companies have responded to this challenge by adding compliance management attributes to existing tools and procedures. However, these add hoc functions are usually not a part of the original information technology and process infrastructure. On the other hand, log management technology has always been used for IT root-cause analysis and information assurance controls. As an inherent part of system design made available to IT professionals for

The Securities and Exchange Commission SEC enforces and sets the implementing rules that accountants must follow in tracking and recording corporate compliance under SOX. This effort is assisted by the Public Company Accounting Oversight Board (PCAOB) and Financial Accounting Standards Board (FASB), both private, self-regulating bodies designated by the SEC to establish the standards of financial accounting and reporting related to SOX compliance. It is important to note that Sarbanes-Oxley Act regulates behavior rather than technology, thereby avoiding the difficult task of prescribing specific technical solutions in an environment where the life cycle of rule-making is exponentially slower than the creation of new technology. The downside to behavior-based regulation is that implementation of SOX amidst the spectrum of information technologies can be daunting.

Logs and the implementation quagmire

Corporate executives face a major challenge in addressing SOX compliance from a technical IT perspective. Traditionally, CFOs have assessed financial integrity issues at an information accounting level – by noting data discrepancies in such areas as payroll processing,

SOX compliance entails ongoing detection, monitoring, evaluation and documentation of effective internal controls. Fulfilling these requirements requires that appropriate infrastructure controls include an automated and reliable log management strategy.

system administration purposes, this log technology can make SOX regulatory objectives much more achievable and manageable.

Log management technology provides information assurance at the front-end, thereby diminishing the drain on corporate resources associated with other risk-reduction responses. If we hold that the value of information is proportionate to the problem it addresses minus the cost of discovery, the accuracy, timeliness and usefulness of log information help address SOX information assurance requirements without creating a poverty of attention, time, effort, skills and other knowledge discovery costs. As such, engaging log management technology can yield significant economic benefits.

How is SOX driving the requirement for companies to retain, control and utilize logs?

Regulations Minus (-) Guidance Equals (=) Confusion

Utilizing event logs help companies comply with SOX by providing visibility into IT activities across devices, applications and systems throughout an enterprise. SOX was designed to make public companies' reporting more accurate and re-establish investor confidence in the integrity of corporate disclosures and financial reporting. Under this legislation, publicly traded companies face regulatory pressure to deliver financial transparency and comply with more stringent financial requirements.

accounts payable and receivable, and fixed asset accounting – to measure potential indicators of error or fraud. As a core component of a SOX compliance framework, system logs enable organizations and their auditors to assess the reliability and integrity of financial reporting and the systems and user activity associated with financial reporting.

How do we map computer log solutions to SOX requirements?

SOX compliance requires ongoing detection, monitoring, evaluation, and documentation of effective internal controls. Fulfilling these requirements means that appropriate infrastructure controls include an automated and reliable log management strategy.

Key Sections Relevant to Event Logs

The Sarbanes-Oxley legislation dictates a higher level of responsibility; accountability and transparency that can be attained with the assistance of event log management technology.

(1) Section 404 – CEOs, CFOs and auditors must document and attest to the effectiveness of internal controls.

Log Relevance for Section 404:

The essence of Sox's disclosure-based system of regulation is accurate and reliable financial reporting and data integrity. Under Section 404's mandate, CEOs and CFOs must attest to the integrity of internal controls. To do so, public log management solutions allow the monitoring, collection, retention, documentation, and notification of user and system activities which can impact financial reporting.

Logs as accepted industry standard for controls:

To comply with Section 404 regulations and evaluate the effectiveness of internal controls, corporate management must utilize a "suitable and recognized control framework." A common framework is represented by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This widely adopted framework is endorsed by the American Institute of Certified Public Accountants (AICPA), and is accepted by the U.S. government as the standard model for internal controls. Under COSO, logs are considered 'pervasive general computer controls' for information security purposes.

Logs as evidence management:

To support assertions on internal controls effectiveness, companies need to provide related and documented evidence. Failure to document a system of controls and its associated evidence will likely be considered an internal controls weakness. Current trends favor a broader interpretation of "internal controls". The General Accounting Office (GAO)'s position and the final rules for Section 404 are rather expansive: they invite substantial changes from the traditional accounting views of "internal controls". As a result, almost anything that may compromise internal controls could arguably be determined as a material weakness.

Logs and testing of internal controls:

Under SEC rules for implementing SOX Section 404, controls subject to assessment by corporate executives include:

- controls over initiating, recording, processing and reconciling of account balances;
- controls related to initiating and processing of non-routine and non-systematic transactions;
- controls concerning selecting and applying appropriate accounting policies;
- controls related to preventing, identifying and detecting fraud.

Internal controls testing and reporting will be inseparable from financial statement audits. In fact, no opinion on audited financial statements can be provided absent testing and opining on these controls.

Positive internal controls testing must be performed to fulfill 404 requirements. Inquiry alone -- i.e., showing proper financial reporting -- will not be considered sufficient testing of internal controls. If an auditor detects a "material misstatement" that was not identified by management, this discovery will likely trigger a red flag and indicate a "material weakness" in internal controls under Section 404 requirements.

Logs and internal controls associated with partners, clients, and service providers (Attestation Standards):
The Public Company Accounting Oversight Board (PCAOB) issued a statement asserting that "the use of service providers does not reduce the responsibility of corporate executives for maintaining effective internal controls." When outsourcing business functions, such as

data processing, payroll, accounts payable and receivable, as well as related web services, executives must consider any service organizations' activities when attesting to the effectiveness of their internal controls over financial reporting.

Public companies cannot minimize SOX responsibilities and offload liability through outsourcing. Nor can they delegate regulatory compliance. For example, if outsourced services are considered material to a company's financial reporting process or operations, the fact that management has no information or assurance on the service provider's internal controls means that executives have no basis for their Section 404 certification and should disclose that information. Executive management, for instance, would face a difficult challenge attesting to the reliability of a company's system of internal controls if it can not provide reasonable information assurance of outsourced providers' systems processing financial transactions or storing sensitive information.

From a legal risk perspective, the PCAOB's statement broadens the pool of potential lawsuit defendants. A public company -- including its executive management and auditors -- as well as its service providers and their executive management and auditors, are all considered agents at risk.

Since event log information represents a core dataset that is often relied upon by internal auditors, they can offer significant value to the auditors of service providers who review, assess and report on the reliability of the systems and processes that are provided to a public company. From the perspective of a public company desiring to limit its legal exposure, the commonality of logs across enterprises makes it attractive to include digital log management as a regularly negotiated term in outsourcing contracts.

Furthermore, outsourcing partners are subject to potential SOX penalties as a public company's agents. From either perspective, logs can provide appropriate safeguards against legal risk exposure. It is in both parties' best interest to implement logs as evidence of internal control compliance.

Enterprise log management:

In today's distributed and mobile computing business environment, companies with limited resources are challenged to monitor proliferating interfaces and controls among decentralized business units. A centralized framework of systems logs from existing network devices, security applications, hosts and business applications can prove less costly than an alternative that would consist of piecing together point solutions across an enterprise's architecture, while simultaneously meeting Section 404 requirements.

(2) Section 802 – Criminal Penalties for Altering Documents

This section mandates the retention and protection of financial audit records.

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry on any record, document or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any

department or agency of the United States... shall be fined under this title, imprisoned not more than 20 years, or both.

Data Retention Standards:

Documents that form the basis of audit reviews – including electronic records -- must be maintained for seven years after an accountant's audit or review of an issuer's financial statements. These records include an accounting firm's work papers, as well as certain documents that contain conclusions, opinions, analyses or financial data related to the audit or review. Detailed system logs provide very useful contextual information regarding the suspected alteration of a document. For example, log analysis of file timestamps that are related to document access, modification or creation are often used to refute or support claims by accused 802 violators.

(3) Section 1102: Tampering with a Record or Otherwise Impeding an Official Proceeding

Similar to the Section 802, the Section 1102 states that, '*whoever alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding shall be fined under this title or imprisoned not more than 20 years, or both.*' As sources of business transactions, event records are subject to longer retention and archival requirements. As such SOX requires that the event records to be saved for up to seven years. Furthermore, an inability to present such records as compliance evidence can be considered tantamount to impeding or obstructing an investigation.

Logs and retention and reporting requirements:

Since digital records cannot be labeled or segregated as systematically as physical records, companies often feel obligated to retain massive volumes of data to avoid SOX penalties. With each employee acting as a potential document administrator, companies are challenged to identify and sort out records that are pertinent to audits. This forces companies to err on the side of caution and save everything to avoid the risk of incurring criminal penalties for manipulating documents. Email communications compound the problem since they often contain financially relevant business transaction information. As business records, they are subject to longer retention and archival requirements. Therefore, instead of a 60-day retention period, SOX would require additional volumes of information to be saved for up to seven years. What's more, the inability to "prove-up" compliance evidence can be tantamount to impeding or obstructing an investigation.

A log management framework designed to efficiently and reliably store large amounts of data, and to allow timely access and querying of that saved data, meets the spirit and letter of Section 802.

Finally, self-reporting, remediation and cooperation efforts can significantly limit legal risk exposure under SOX regulations. The SEC has stated that effective self-policing and cooperation with law enforcement could reduce corporate liability. As a result, logs can be critical in assisting law enforcement or in-house investigation activities. By answering the who, what, when, where, and how variables that investigators rely upon, they provide the digital footprints of past computer activity that affects business processes. Reliable logging technology is therefore particularly well-suited to ensure that critical evidence is useful for legal actions.

(4) Section 409 – Timely Disclosure

Under this Section, public companies must report material changes in their financial or operating condition on a rapid and current basis. Specifically, these material changes must be reported within 48 hours of detection. This requirement means that material security incidents, regulatory fines or litigation require rapid identification, collection, and analysis of evidence that can prove/disprove that provision.

Log technology is commonly used by IT professionals for systems administration purposes, i.e. to keep computers and networks functioning properly. As such, logs management provides actionable information based on recorded evidence.

(5) Section 302 – Corporate Responsibility for Financial Reports

This section holds corporate executives accountable for the veracity of financial statements, by requiring that they certify the accuracy of their financial reports.

"The CEO and CFO of each issuer shall prepare a statement to accompany the audit report to certify the "appropriateness of the financial statements and disclosures contained in the periodic report, and that those financial statements and disclosures fairly present, in all material respect, the operations and financial condition of the issuer." A violation of this section must be knowing and intentional to give rise to liability, however.

Some of the controls subject to assessment by corporate executives, as per the SEC rules for implementing Section 404 of SOX are:

- Controls over initiating, recording, processing and reconciling account balances;
- Controls related to the initiation and processing of non-routine and non-systematic transactions.

Effective log monitoring and analytics provides due process regarding these controls.¹

¹ SenSage would like to acknowledge Erin Kenneally, M.F.S., J.D., Forensic Analyst and Attorney with the San Diego Supercomputer Center, University of California at San Diego, and a Forensic Analyst and Attorney with the University of California San Diego Supercomputer Center, for her invaluable contribution to this paper.

The SenSage Advantage

As we have discussed, SOX compliance requires collecting, retaining and analyzing terabytes of event data for as long as seven years. Most commercial and “homegrown” security information management (SIM) solutions rely on relational database management system (RDBMS) approaches that were not designed for high-volume, event-data capture, analysis, and long-term retention. Thus, these systems are inherently limited in fully meeting SOX mandates for consistent monitoring and iterative analysis.

SenSage’s enterprise security analytics solution eliminates these deficiencies. Specializing in delivering the combination of event-data collection, compression, retention and analytics, SenSage provides the most scalable means to centrally aggregate, efficiently analyze, dynamically monitor and cost-effectively store high-volumes of event log data.

Specifically, SenSage collects data from a broad range of sources at a sustained rate of 87,500 events per second, and scans that data at 2,000,000 records per second (assuming a five-node cluster). This real-world scan rate is that of a complex sub-string URL search with full data extraction. As such, users do not have to make compromises about which systems to monitor or which data to collect. And, it allows users to get faster results from a huge repository of multiple-source event data.

When storing event data, SenSage can compress it to as little as 10 percent of the original, raw, event-log data; and 2.5 percent the size of that stored using an RDBMS. Since SenSage is based on a purpose-built repository with self-optimized storage, it also avoids RDBMS tuning and archiving. Clearly, users can store all their event data without outrageous storage and administrative costs.

SenSage’s Real Time Compliance Monitoring Demonstrates SOX Compliance

SenSage enables corporations to meet compliance requirements with both pre-defined and customized reports as part of its out-of-the-box solution. This is a significant advantage, since our customizable query and reporting capabilities allow corporations to augment pre-defined report packages, and/or rapidly meet specific compliance requirements that arise during SOX audits or forensic investigations.

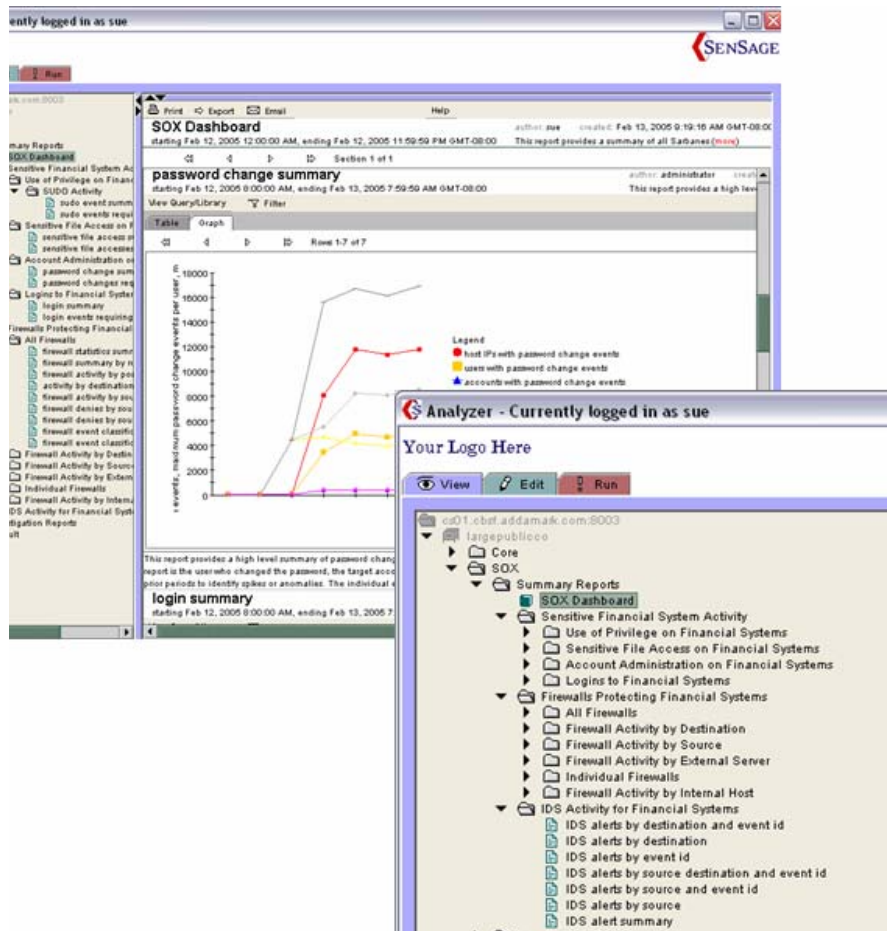
SenSage also provides unified compliance reporting. Unlike some competitive alternatives that offer one set of reports for one firewall vendor, and a different set of reports for another, SenSage reports cover all products within a given category, thereby streamlining the task of managing a large and heterogeneous environment.

These pre-defined compliance reports create a SOX dashboard to help corporations track compliance with each of the sections of SOX discussed in this paper. Specifically, the following table outlines each of the report groups and how they map to SOX requirements. Please note that each individual report group within the SenSage SOX dashboard includes dozens of individual out-of-the-box graphical and tabular reports. These reports are customizable and exportable in a variety of formats and can also be automatically generated and sent on a user-defined schedule.

SenSage Report Group Category	Relevant SOX Sections
Investigate Users	404, 802, 1102, 409, 302
Activity on Financial Systems	404, 802, 1102, 409, 302
Logins to Financial Systems	404, 802, 1102, 409, 302
Users to Investigate for Financial Fraud	404, 802, 1102, 409, 302
Business Critical System Activity	404, 802, 1102, 409, 302
Use of Privilege on Financial Systems	404, 802, 1102, 409, 302
Email Activity Summary	404, 802, 1102, 409, 302
IDS Activity for Financial Systems	404, 802, 1102, 409, 302
Firewalls Protecting Financial Systems/All Firewalls	404, 802, 1102, 409, 302
Firewalls Protecting Financial Systems/Individual Firewalls	404, 802, 1102, 409, 302
Firewalls Protecting Financial Systems/Firewall Activity by Destination	404, 802, 1102, 409, 302
Firewalls Protecting Financial Systems/Firewall Activity by Source	404, 802, 1102, 409, 302

SenSage's SOX Dashboard

SenSage's SOX dashboard provides immediate insight into an organizations' compliance posture as seen below. Assets are grouped according to their compliance relevance and events are prioritized based on the criticality and value of each SOX-related asset. This enables organizations to prioritize remediation activity around compliance initiatives.



Summary

SenSage provides unparalleled performance and a scalable means for organizations to centrally aggregate, efficiently analyze, dynamically monitor and cost-effectively store massive volumes of event log data. This functionality is absolutely essential in order to satisfy SOX requirements with respect to audit data.²

About SenSage, Inc.

SenSage, the leading provider of enterprise security analytics, offers unparalleled performance and a scalable means for organizations to centrally aggregate, efficiently analyze, dynamically monitor and cost-effectively store massive volumes of event log data. Our solutions empower companies to readily respond to business-critical threats, conduct thorough and precise investigations, and maintain compliant operations. Based in San Francisco, CA, SenSage currently protects Global 2000 customers in financial services, government, healthcare, manufacturing, and technology. The company markets its product directly and through partners including Cerner, EMC, Hewlett-Packard, and Lockheed Martin. For more information, visit www.sensage.com.

² The information provided in this white paper is for guidance purposes only and is published as legal analysis, not legal advice. While every effort is made to provide quality legal information, there are no claims, promises or guarantees in respect of any specific legal problem. As legal information must be tailored to the specific circumstances of each case, and laws are constantly changing, we recommend you consult a lawyer if you want professional assurance that our information, and your interpretation of it, is appropriate to your particular situation.