Sarbanes-Oxley (SOX) Compliance Checklist

http://www.correlog.com/support.html

The Sarbanes-Oxley Act (SOX) is Federal law for all publicly held USA corporations, and establishes extensive civil and criminal penalties for non-compliance.

The main intention of SOX is to establish verifiable security controls to protect against disclosure of confidential data, and tracking of personnel to detect data tampering that may be fraud related. The central purpose of the act is to reduce fraud, build public confidence and trust, and protect data that may affect companies and shareholders.

This act consists of multiple sections, all of which require compliance by a company. The two principle sections that relate to security are Section 302 and Section 404, summarized below:

- **Section 302.** This section is intended to safeguard against faulty financial reporting. As part of this section, companies must safeguard their data responsibly so as to ensure that financial reports are not based upon faulty data, tampered data, or data that may be highly inaccurate.

- **Section 404**. This section requires the safeguards stated in Section 302 (as well as other sections) to be externally verifiable by independent auditors, so that independent auditors may disclose to shareholders and the public possible security breaches that affect company finances. Specifically, this section guarantees that the security of data cannot be hidden from auditors, and security breaches must be reported.

CorreLog satisfies the above requirements by creating a system to track user access, security information and controls, file integrity, change management, and other security indicators. With a verifiable audit trail, staff can then document every step to auditors or assessors and provide them with detailed reports that demonstrate changes made to information systems can be detected, corrections verified, and anomalies explained. The path from data to information to knowledge is quick and responsive.

Each pertinent subsection of these two main sections of SOX is discussed in detail within the paragraphs that follow. (Actual sections of SOX are available from a variety of sources, and are paraphrased below in the context of security frameworks. See Appendices for specific references.)

Section 302.2 – Establish safeguards to prevent data tampering.

Explanation. This section of SOX requires that the signing officer must attest to the validity of reported information. Safeguards must exist to prevent tampering with data, so that data is verifiably true.

CorreLog tracks user access to all the computers that contain your sensitive data. It detects logins to those computer systems processing financial data, and protects this data in a variety of ways: it ensures that the system is performing as expected (with regard to performance, access and software updates) and it detects break-in attempts to computers, databases, websites and storage disks. CorreLog monitors disk activities, disk mount points and use of removable storage including CD/DVD burners and removable USB storage devices.

Section 302.3 – Establish safeguards to establish timelines.

Explanation: This section of SOX requires that the signing officer attest to the fact that reported information is fairly presented, including accurate reporting for the time periods. Safeguards must exist that the data relates to a verifiable time period.

CorreLog timestamps all data as it is received. As a real-time system, the data is immediately stored at a remote location as it is generated, preventing alteration or loss of this data by any action that can occur at the managed node. Additionally, this log information is compressed, moved to a new location (i.e. a secure archive), and a checksum is created. The MD5 checksum is encrypted, preventing any tampering with the file or checksum. This completely secures audit trails so they cannot be altered.

Section 302.4.B – Establish verifiable controls to track data access.

Explanation: This section of SOX requires internal controls over data, so that officers are aware of all relevant data. Data must exist in an internally controlled and verifiably secure framework.

CorreLog can process more than 2000 messages per second and can handle burst traffic of more than 10,000 messages in one second (depending upon the supporting hardware.) In a two-tier architecture, CorreLog can receive messages from virtually unlimited numbers of sources. Additionally, CorreLog is a highly extensible system that permits collection of data through file queues, FTP transfers, and databases, independent of the actual framework (such as COBIT and ISO 27000 standards.)

Section 302.4.C – Ensure that safeguards are operational.

Explanation: This section of SOX requires that officers have evaluated the effectiveness of the internal controls as of a date within 90 days prior to the report. The security framework must be periodically reviewed and verified.

CorreLog is a robust background process, which operates continuously on your network. Because it is a web based program, it is available from an unlimited number of seats, and its operation can be checked and reviewed by any individual with a remote login to the system. Additionally, CorreLog provides a suite of facilities that can issue daily reports to e-mail addresses or distribute reports via RSS, making it easy to verify that the system is up and running. CorreLog provides clear indications of its startup times, shutdown times, as well as these times for all managed devices.

Section 302.4.D – Periodically report the effectiveness of safeguards.

Explanation: This section of SOX requires officers to generate a report on the effectiveness of the security system, and state their conclusions. The security framework should report its effectiveness to auditors and officers of the enterprise.

CorreLog is easy to use, and requires minimal training. CorreLog generates multiple types of reports, including a report on all messages, critical messages, and self-generated alerts. Reports can be automatically distributed via e-mail and RSS, and are provided in Excel format (as well as other formats) to make the job of the auditor easy. Additionally, CorreLog archives reports for later review and forensics, so that auditors can see a clear indication of operation and the types of data being tracked, and easily draw their conclusions. Finally, CorreLog incorporates a ticketing system that illustrates what kind of security problems and activities have taken place recently, or in the distant past.

Section 302.5.A&B – Detect Security Breaches

Explanation: These two subsections of SOX are similar to those found in Section 404 A&B, and require that security breaches (either due to flaws in the control system, the security system, or due to fraud) be detected.

CorreLog uses an advanced correlation engine, which performs semantic analysis of messages in real-time. The system employs correlation threads, correlation counters, correlation alerts, and correlation triggers, which refine and reduce incoming messages into high-level alerts. These alert open tickets, which document the security breach, and which can also trigger actions such as sending e-mail, or updating an incident management system. The result is a reduction of large amounts of logged data into real-time security alerts that are sent directly to security personnel and auditors.

Section 404.A.1.1 – Disclose security safeguards to independent auditors.

Explanation: This section of SOX relates to management appointed auditors, and requires them to review control structures and procedures for financial reporting. The existence of a security framework, and parties responsible for the operation of the security framework, must be disclosed to auditors.

CorreLog provides access and security to auditors using role-based permissions. For example, auditors may be permitted complete access to specific reports and facilities without the ability to actually make changes to these components, or reconfigure the system. Additionally, because CorreLog is a secure and web-based application, auditors do not have to be physically present to assess security aspects, or any particular operation of the system. All aspects, including the downloading of reports, can be performed remotely (given proper authentication of the user.)

Section 404.A.2 – Disclose security breaches to independent auditors.

Explanation: This section of SOX requires auditors to assess the effectiveness of the internal control structure. The general effectiveness of the security framework must be measured and disclosed.

CorreLog is designed to be a complete security logging solution, capable of detecting security breaches, notifying security personnel in real time, and permitting resolution to security incidents to be manually entered and stored. In particular, the stream of input messages is continuously correlated to create tickets (which record security breaches and other events.) The CorreLog ticketing system includes an e-mail interface that can quickly notify both auditors and security officers of compromised files, security breaches, and other significant events. Tickets can be summarized in reports to allow easy assessment and disclosure of recent and past security breaches.

Section 404.B – Disclose failures of security safeguards to independent auditors.

Explanation: This section of SOX requires auditors to be aware of (and report on) significant changes to internal controls, and significant failures that could significantly affect internal controls. Verification must exist that the security framework has been both operational and effective.

CorreLog schedules periodic tests of network and file integrity, and verifies that certain messages are logged, indicating successful tests. CorreLog interfaces easily with common, security-test software, including port scanners, to verify that CorreLog is successfully monitoring system security. CorreLog provides numerous self-monitoring functions that can trigger alarms and real-time e-mail messages to multiple individuals responsible for both maintaining the system, and auditing its performance. This provides a clear indication of operation and security coverage needed to satisfy this particular requirement.

COBIT and ISO 27000 Support

Sarbanes-Oxley makes multiple references to "internal control" of data. To meet this requirement, companies must establish rules and guidelines by which the organization is controlled and audited.

There are many acceptable techniques for establishing this type of governance; one of the most popular methods of establishing "internal control" is to implement the "COBIT Framework", created by ISACA. COBIT is an extensive set of guidelines and tools that describe processes and organizational requirements needed to promote security and create good governance capable of satisfying SOX requirements. The framework consists of its own standards, as well as many other standards, including ISO/IEC 27000.

CorreLog supports the COBIT framework and ISO/IEC 27000 in various ways. The ISO/IEC 27000 standard directly relates to information security, and CorreLog satisfies these important requirements by implementing verifiable security controls and safeguards on your computer network as follows:

- CorreLog monitors file integrity and file structures on information systems, including hardware, software, network, and security infrastructure. It then provides detailed change audit information to enable agency staff to quickly pinpoint, analyze, and recover from any undesirable change. CorreLog delivers assurance that authorized changes are completed, and that unauthorized or ad hoc changes that circumvented policy are detected and immediately reported.

- With a verifiable audit trail, staff can then document every step to auditors or assessors and provide them with detailed reports that demonstrate changes made to information systems can be detected, corrections verified, and anomalies explained. The path from data to information to knowledge is quick and responsive.

- By implementing change detection and reporting with configuration assessment, CorreLog assesses every change as authorized, within policy and compliant, ensuring systems achieve a known and trusted state. CorreLog then helps maintain that known and trusted state by establishing a secure baseline to measure change against, and then monitors against that baseline through ongoing, tunable change detection and reporting.

An organization cannot claim to have a comprehensive information security policy, or meet COBIT framework objectives, without monitoring the security message being constantly logged on platforms within your enterprise. An enterprise that installs CorreLog, with no other action, takes a major step forward in creating and maintaining an enterprise security policy that satisfies ISO/IEC 27000, COBIT objectives, and the legal obligations of Sarbanes-Oxley.

Appendix: Sarbanes-Oxley Section 302

SEC. 302. CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS.

(a) REGULATIONS REQUIRED. — The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer of officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that —

(1) the signing officer has reviewed the report;
(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;
(3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;
(4) the signing officers:

(A) are responsible for establishing and maintaining internal controls;
(B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;
(C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and
(D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function) —
(A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and
(B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

Appendix: Sarbanes-Oxley Section 404

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) RULES REQUIRED. — The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall —
(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING. — With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

Appendix: References and External URLS

http://www.sec.gov/rules/proposed/s74002/card941503.pdf

A white paper, hosted by the USA Security and Exchange Commission (SEC), proposing practical, cost effective compliance strategies. According to the preface: Traditional audit/compliance approaches and tools in use in most companies today are woefully inadequate to meet the virtually "real time" assessment and monitoring expectations imposed by sections 302 and 404, and an automated SIEM system (such as CorreLog) is required.

http://www.correlog.com/solutions-and-services/sas-compliance-sox.html

An introductory discussion of SOX compliance requirements, hosted by CorreLog, Inc. SOX regulations serve a somewhat different purpose from various other standards and guidelines. Unlike most security compliance measures, SOX is intended to create traceable data to prove (or disprove) corporate fraud and malfeasance in accounting and administration. In practice, the mechanics of implementing SOX compliance are almost identical to that of implementing a corporate security process, as described here.

http://www.correlog.com/solutions-and-services/index-compliance.html

An overview of CorreLog compliance features. In addition to SOX compliance, CorreLog provides auditing and analysis services for organizations concerned with meeting SIEM requirements stated by PCI/DSS, NERC, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Proactively manage your system security, and achieve regulatory compliance. Our solutions install quickly, and with no surprises

CorreLog, Inc.

http://www.correlog.com
mailto:sales@correlog.com