SOX: Q-Compliance

REAL-TIME RISK MANAGEMENT & CON-MON COMPLIANCE FOR FINANCIAL ENTITIES

SOX Checklist

- ✓ 1. Protect against and prevent data tampering
- ✓ 2. Establish timelines for data storage and safeguarding
- ✓ 3. Establish verifiable controls to track data access
- ✓ 4. Ensure that safeguards are operational
- ✓ 5. Periodically report the effectiveness of safeguards
- ✓ 6. Detect security breaches and disclose breaches to SOX auditors
- ✓ 7. Disclose security safeguards, and failures, to SOX auditors

SOX GOAL:
"TO PROTECT INVESTORS BY IMPROVING THE ACCURACY AND RELIABILITY OF CORPORATE DISCLOSURES."

The Sarbanes-Oxley Act of 2002, often called SOX, typically brings financial accounting standards to mind, along with a few controversial company names—think Enron, Tyco, WorldCom, etc. The common theme between these companies is irreparable damages to reputations as a result of scandalous financial governance, accountability practices, and a lack of information security standards. The SOX legislation was passed in an effort to protect shareholders in public companies whose accounting data accuracy and transparency, whether intentional or not, may be subject to manipulation.

Data accuracy and security is a high stakes game. Company executives must accept responsibility for the truthfulness and accuracy of financial information about their companies. If the data is found to be manipulated or falsified in any way, the penalties range from delisting on stock exchanges to 20 years behind bars.

InfoSec-focused sections of SOX that IT managers should care about:

1) Section 302 – If your business uses electronic transmission of data for accounting, you must ensure high data security standards. Executives must attest to the adherence to those security controls, and bear responsibility for the accuracy of reports.
2) Section 404 – An outside firm must audit your adherence to security controls for the monitoring and maintenance of accounting and financial records and information. Then the SEC gets to see the results.
3) Section 409 – Investors and the public must be informed as soon as there is a material change to the company's financial status and ability to operate.
4) Section 802 – Altering any data that is of concern to the SEC in any way constitutes a crime, and the punishment will be severe.
5) Section 906 – Whoever submits a financial report with inaccurate or falsified data is liable.

Compliance with SOX requirements is an ongoing concern for all enterprises. While IT personnel bear witness to information assurance and the integrity of stored historical records related to the financial status of the company, it is ultimately leadership's name on the dotted line. To be SOX compliant, seven years of financial records must be accurately stored for the enterprise, company boards, management personnel, and accounting firms.

Q-Compliance is purpose-built to help you streamline and automate complex cybersecurity auditing and compliance requirements like SOX and leverage industry best practices and standards such as the NIST Risk Management Framework and 800-53 controls to help you implement and measure your compliance against SOX.