

---

# Assessment and Compliance with Sarbanes-Oxley (SOX) Requirements

DataGuardZ Whitepaper



---

## What is the history behind Sarbanes-Oxley Act (SOX)?

In 2002, the U.S. Senate added the Sarbanes-Oxley Act (SOX) to the network of securities regulations in order to keep corporate America in check. It was named after its sponsors - U.S. Senator Paul Sarbanes (D-MD) and U.S. Representative Michael G. Oxley (R-OH). This Act was created to protect investors and the U.S. economy from the threat of scandal in and corruption by publicly traded companies. That legislation became effective after a series of accounting scandals led to the failure of several major corporations (Enron, WorldCom, Tyco International, Adelphia), the conviction and imprisonment of multiple key executives, and the failure of a major public accounting firm (Arthur Andersen).

## SOX - What is it?

Essentially, SOX requires that every publicly traded company's executive members evaluate and maintain responsibility for the accuracy and completeness of all financial information that is released to the public. This Act also requires that companies release information regarding those controls that are in place in order to ensure the accuracy and reliability of their financial information. SOX contains 11 titles that describe specific mandates and requirements for financial reporting. Each title consists of several sections.

Title I consists of nine sections and establishes a new regulatory authority to set public accounting auditing standards. The Public Company Accounting Oversight Board (PCAOB), which essentially replaced the American Institute of Certified Public Accountants' (AICPA's) self-regulated auditing rulesetting authority, provides independent oversight of public accounting firms that are performing audit services ("auditors"). It also creates a central oversight board tasked with registering auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX. SOX changes many of the processes that public companies had used for their own governance, to report their financial results to the Securities and Exchange Commission (SEC) in the United States, and to their investors. These SOX initiated changes touch boards of directors, senior management practices, and the adequacy of the internal controls used to support their financial and other processes. The most important sections of SOX for the senior managers, the board, internal audit, and other key members of the management team are:

---

**Section 302:** Corporate Responsibility for Financial Report  
**Section 404:** Management Assessment of Internal Controls  
**Section 409:** Real Time Issuer Disclosures

While many portions of SOX may require changes and adjustments, Section 404 rules on internal controls have caused management and internal auditors the greatest level of pain and suffering. Strictly interpreted, the legislation laid out some very tight internal control compliance rules.

## **SOX Section 404: What does it mean to you?**

In compliance with SOX Section 404, each annual report must include a statement by executive officers to the effect that they are responsible for the establishment and maintenance of the internal control structure and other procedures for financial reporting. In addition, the Internal Control Report must also include an assessment of all internal controls related to the financial information that has been released. This assessment is required to inform investors not only about the structure of the controls, but also about their efficacy.

## **What is at stake if you don't follow the rules?**

SOX was created to address the accounting deficiencies and hold senior managers – specifically the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) – criminally and civilly accountable for the financial reports and internal controls of their company. Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. Section 304 requires that if an enterprise is required to restate its earnings due to some material violation of securities laws, the CEO and CFO must reimburse the company for any bonuses or incentives received on the basis of the original, incorrect statements issued during the past 12 months. The same applies for any profits received from the sale of enterprise securities during that same period.

Title IX increases criminal penalties for white-collar crimes and also contains the penalties for executives who do not certify the accuracy of the company's financial reports or who certify reports that do not meet SOX compliance standards. In addition to civil lawsuits

---

and damage to their image in the marketplace, CEOs and CFOs of companies that are non-compliant with SOX are subject to financial penalties and potential incarceration. Situations where willful deceit can be proven carry fines of up to \$1 million and 10 years in prison. However, in the event that wrongful certification has been submitted intentionally, the maximum penalty rises to \$5 million and 20 years in prison.

## **What are you required to do to comply with SOX mandates as it relates to Information Technology?**

Information Technology (IT) controls are specific activities performed by persons or systems designed to ensure that business objectives are met. They are a subset of an enterprise's internal control. IT control objectives relate to the confidentiality, integrity, and availability of data and the overall management of the IT function of the business enterprise.

IT controls are often described in two categories:

- IT general controls; and
- IT application controls.

IT general controls include controls over the IT environment, computer operations, network security, access to programs and data, program development and program changes.

IT application controls refer to transaction processing controls, sometimes called "input-processing-output" controls. IT controls have been given increased prominence in corporations listed in the SOX Section 404.

## **How can DataGuardZ assist you in achieving IT SOX compliance?**

DataGuardZ offers IT consulting services designed specifically to help you comply with SOX regulations as it relates to your control framework around the IT environment. We have developed a comprehensive approach which is based on our extensive experience and knowledge of the SOX Act geared to help you build towards compliance.

Our multi-phased approach is designed to assess and document your company's internal controls. This approach includes four phases:

- 
- Planning
  - Assess design effectiveness
  - Assess operating effectiveness
  - Ongoing monitoring/developing ongoing strategy for compliance

Our proprietary SOX methodology is modeled on COSO & COBIT Frameworks, assesses and evaluates internal controls and aids companies in deriving essential business value from compliance with SOX.

At DataGuardZ, we believe that compliance with SOX not only helps organizations adhere to the laws of the land but also serves as the armor against future corporate battles and lays the roadmap for organizational excellence. Our experienced consultants have worked on numerous compliance consulting assignments for a number of Fortune 500 companies across various industries and understand the unique challenges you face in meeting SOX requirements. With this in mind, we offer a customized, flexible approach that's based on your needs.

## **DataGuardZ Core Competencies**

Our team of professionals are technology, legal, security and IS audit experts who have earned multiple advanced degrees and certifications including J.D. (Juris Doctorate), M.B.A. (Master of Business Administration), ISO 27001:2005 Lead Auditor, CFE (Certified Fraud Examiner), CISSP (Certified Information Systems Security Professional), SSCP (System Security Certified Professional), CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Security Control), ABCP (Associate Business Continuity Planner), CCSA (Check Point Certified Security Administrator), CCNP (Cisco Certified Network Professional), Microsoft Certified Systems Engineer (MCSE), Microsoft Certified Database Administrator (MCDBA), Microsoft Certified Technology Specialist (MCTS), VCP (VMware Certified Professional) 3, 4, and 5.