



404Audit

Risk Assessment and Compliance Monitoring Tool



Sen. Paul S. Sarbanes & Rep. Michael G. Oxley



SOX Background

The Sarbanes Oxley (SOX) Act was created to restore investor confidence in US public markets, which was damaged by scandals and lapses in corporate governance. The Act aims to enhance corporate governance and accountability through internal checks and balances.

Section 404 requires senior management and business process owners to establish and maintain an adequate internal control structure. Also, they need to assess and report its effectiveness on an annual basis. The reliability of reporting depends heavily on a well-controlled IT environment.

The SEC (Securities and Exchange Commission) has mandated the use of a recognised internal control framework. The SEC has made specific reference to the recommendations of COSO (Committee of the Sponsoring Organisations of the Treadway Commission).

The US Public Company Accounting Oversight Board (PCAOB) approved auditing standard No. 2 titled "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements".

Most have found they require IT control considerations beyond those provided by COSO or PCAOB.

Help is here: 404Audit

404Audit is a risk analysis and auditing tool. In developing this software, IT controls from COBIT (Control Objectives for Information and Related Technology) framework were linked to the IT control categories identified in PCAOB & COSO. Consideration was also given to the controls and guidelines outlined in ISO 17799, ITIL (Information Technology Infrastructure Library), Common Criteria and SysTrust.



Although these guidelines and standards address operational objectives, only those related directly to financial reporting were selected. However, there is an inevitable overlap as processes are developed.



So what does the software do?

The tool is a unique solution that assesses the internal controls of an organisation against those required by the Sarbanes Oxley Act. The tool also evaluates the overall readiness of an organisation through an assessment based around the Audit Committee and the Chief Financial Officer.

The power of the solution is in the design.

Initially the organisation is profiled, a number of factors are taken into consideration including (but not limited to):

- Location of Organisation
- Size of Organisation
- Turnover
- The number of computers used
- The OS (operating systems) used

Nearly 30 factors are used to perform a risk analysis against the controls in place to protect the Confidentiality and Integrity of information and ensure its Availability for the financial reporting process.

This is not merely a gap analysis, the profiling section uses up to date statistical data gathered from over 10,000 resources to assess the risks involved. These resources include the CSI, FBI, CERT, Symantec and the Global Instability Index.

When the audit is complete a number of reports and charts are available. It also produces an overall % percentage score and risk rating on a scale of 1 to 10. Each individual area of the ISMS (Information Security Management System) is also scored and assessed.





So what are the Benefits?

➤ Graphic Display of Sarbanes Oxley Compliance Level
➤ Can be used as part of SOX annual report
➤ Graphic Display of Enterprise Information Security Risk Exposure
➤ Automatic Creation of Actions Plans
➤ Duty of Care – enhances corporate reputation
➤ Can help reduce insurance premiums for InfoSec insurance
➤ Helps reduce risk
➤ Can help achieve SOX compliance
➤ Categorisation of actions against COSO controls

Further Benefits?

➤ **Credibility, trust and confidence**

Your customers and business partners can feel confident of your commitment to keeping their information safe.

➤ **Cost Savings**

The cost of a single information security breach can be significant. A risk analysis reduces the risk of such a cost being incurred and this is important to stakeholders and other investors.

➤ **Compliance**

Performing a detailed risk analysis helps to show the authorities (and other parties) that you comply with all the relevant laws and regulations. It also helps reduce the need for multiple assessments.

➤ **Commitment**

Helps to ensure and demonstrate commitment at all levels of the organisation. It also provides opportunity for continuous improvement through regular audits.

➤ **Busines**

Provides more avenues for trade in the global market through bilateral and multilateral agreements on mutual recognition of the information security standards and optional certification.





Next Step

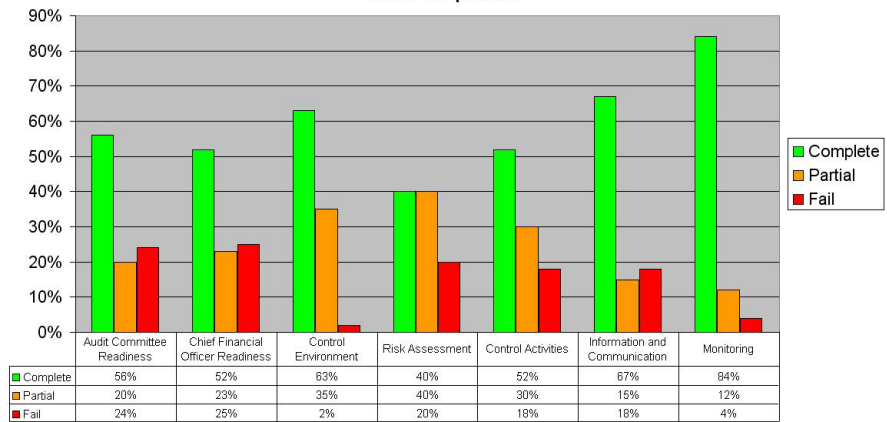
Contact the Information Security Experts at :
<http://www.TeamInfoSec.com>

Signing of the Sarbanes-Oxley Act in Washington 2002



Some sample output charts

SOX Compliance



SOX Compliance

