Sarbanes-Oxley Act of 2002

George Louthan

April 6, 2010

Overview and Motivation

- Also called Sarbox or SOX
- Corporate reforms to address dishonest financial practices
- Applies only to public corporations
- Motivated by highly publicized scandals involving Enron, WorldCom, and others
  - Corporate Looting and Theft
  - Securities and Accounting Fraud
  - Auditing Failures
- 11 titles, emphasizing auditing and executive accountability
- Why we care: makes requirements for "internal controls" to prevent "material misstatements"

Titles 1-4

PCAOB Establishes the Public Company Accounting Oversight Board, which has SOX-backed regulatory authority

Auditor independence Regards approval requirements and conflict of interest limitation for auditors. For example, auditing companies may not provide other services for audit clients.

Corporate Responsibility* Senior executives are personally responsible for correctness of financial reports

Enhanced Financial Disclosures* New, more detailed financial reporting requirements; requires "internal controls" for assuring the accuracy of financial reports, and audits thereof

Titles 5-8

Analyst Conflicts of Interest Code of conduct for securities analysts, including conflict of interest disclosure

Commission Resources and Authority SEC has the authority to govern brokers, advisors, and dealers in securities

Studies and Reports Requires SEC and Comptroller General to conduct various studies and produce reports

Corporate and Criminal Fraud Accountability Criminal penalties for interference with financial records, and whistle-blower protections

Titles 10-11

White Collar Crime Penalty Enhancement Failure to certify corporate financial reports is a criminal offense; new, stronger sentencing guidelines (no more resort prison)

Corporate Tax Returns CEO must sign the company's tax return

Corporate Fraud Accountability New authorities for SEC to freeze "unusual" transactions, criminalization of corporate records tampering

Section 404

- Title 4, Section 404 is the primary section associated with risk management
- Public companies were already required to make annual reports to the SEC
- Section 404 requires this to include an "internal control report", which:
  - states the responsibility of management for establishing and maintaining an adequate internal control structure
  - contains an assessment of the effectiveness of the internal control structure
- The result of this, section 302, and associated regulation is that organizations and auditors must conduct "Sarbanes-Oxley 404 top-down risk assessments"

SOX Requirements vs PCAOB Requirements

- Sarbanes-Oxley itself does not directly create any IT requirements
- PCAOB (Public Company Accounting Oversight Board), however, specifically included IT controls as "internal controls"
- This decisions means IT security controls and audits thereof are required by SOX (Section 404)

Section 404 Risk Assessment

- Top-down Risk Assessment specified by PCAOB Auditing Standard No. 5 (Effective Nov, 2007)
- Focuses on the risk of "material misstatement to the financial statements and related disclosures".

Section 404 Risk Assessment

- Explicitly mentioned IT risks for material misstatement:
  - Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
  - Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions.
  - Unauthorized changes to data in master files.
  - Unauthorized changes to systems or programs.
  - Failure to make necessary changes to systems or programs.
  - Inappropriate manual intervention.
  - Potential loss of data.

Is IT audit needed?

- PCAOB: "The identification of risks and controls within IT is not a separate evaluation. Instead, it is an integral part of the top-down approach."
- Need for specialized IT audit depends upon (AU319):
  - Complexity of the entity's systems
  - Significance of changes made to existing systems
  - Extent of data sharing
  - Extent of entity's participation in electronic commerce
  - Use of emerging technologies
  - Significance of electronic-only evidence

General Requirements

- SOX requires documentation and audit of "internal controls"
- Section 404 and PCAOB require periodic "top-down risk assessments"
- Management assesses controls, and auditors audit that assessment
- Risk assessments and controls specifically focused on correctness of financial statements
- IT is only one small part of Sarbanes-Oxley

IT Requirements

- IT-related SOX assessment focused specifically upon risk of material misstatements on financial documents (sometimes called MMR)
- Only one part of an overarching, top-down risk assessment
- Frequently tied to COBIT or other standards due to generality or vagueness
- SOX IT requirements defined primarily by SEC and PCAOB, not Congress

Side Note: Supreme Court Challenge

- SOX is currently under Constitutional challenge in *Free Enterprise Fund v. Public Company Accounting Oversight Board*
- Separation of Powers challenging the appointment of PCAOB members by the SEC
- Oral arguments were December 7, 2009; no decision yet.

References

- SANS Sarbanes-Oxley Whitepaper. http://tinyurl.com/ybexnv7
- Sarbanes Oxley Act of 2002, hosted by University of Cincinnati College of Law. http://tinyurl.com/k8qqv
- Serena Software. The Impact of Sarbanes-Oxley on IT and Corporate Governance. http://tinyurl.com/ydgzy42
- PCAOB Auditing Standard No. 5. http://tinyurl.com/ye5sprj
- PCAOB AU 319. http://tinyurl.com/yajyvst
- On the Docket: Free Enterprise Fund and Beckstead and Watts v. Public Company Accounting Oversight Board. http://tinyurl.com/yavkxz7