Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

Sarbanes-Oxley Links IT to Corporate Compliance

Linda Volonino
Canisius College

Guy Gessner
Canisius College

George Kermis
Canisius College

Sarbanes-Oxley Links IT to Corporate Compliance

Linda Volonino
Canisius College
volonino@canisius.edu

Guy H. Gessner
Canisius College
gessner@canisius.edu

George F. Kermis
Canisius College
kermisg@canisius.edu

ABSTRACT

In the wake of financial frauds and related audit issues, the US Congress passed the Sarbanes-Oxley (SARBOX) Act of 2002. Key to becoming SARBOX compliant are information systems (IS) that satisfy the mandates regarding internal controls, corporate governance, and fraud detection. These legal developments focusing senior management's attention on (1) internal controls are present and functioning i and (2) the adequacy of the internal audit (IA) and information technology (IT) departments to help management satisfy its SARBOX requirements

This tutorial identifies the requirements ("sections") of SARBOX that affect IS , including auditing, security, business intelligence, customer relationship management, supply chain management, and electronic records (e-records) management. By explaining the three major compliance and corporate governance mandates, this article suggests important research areas, which include IS assurance methods for evaluating and documenting internal controls for reporting purposes, IT infrastructure and data warehousing, and best practices in auditing for evidence of fraud.

Keywords

Sarbanes-Oxley Act, internal control, auditing, corporate governance, electronic records management, legal issues

INTRODUCTION

SARBOX Redesigns Federal Securities Laws

By nearly unanimous votes in July 2002, US Congress passed into law the Sarbanes-Oxley Act, the most radical redesign of federal securities laws since the 1930s.[1] This 131-page law is to protect investors by improving the accuracy and reliability of corporate disclosures—and plugging loopholes in existing securities laws [Zelizer, 2002]. Enacted in response to public anger at accounting fraud and corporate governance failures, SARBOX mandates that companies have in place stringent policies and procedures for reporting financial information accurately. These mandates break new ground in the fight against corporate fraud and require a wide variety of IT to be in compliance. To compel compliance, violators of any rule of the SEC issued under the Act face civil or criminal sanctions.

SARBOX has given the government broad power to prosecute senior management for inaccurate financial reports, fraud, or destruction of financial records or audit documents. In one of the first cases of document destruction brought under SARBOX, Thomas Trauger, a former senior partner at Ernst & Young, was arrested on charges of destroying audit papers and obstructing federal investigations [Iwanta, 2003]. The Justice Department charged Trauger with two criminal counts of falsifying records and obstructing investigations by the SEC and the Office of the Comptroller of the Currency, the federal agency that oversees financial firms. Under SARBOX, Trauger faces potential penalties of up to 25 years in prison and $500,000 in fines.

[1] The Sarbanes-Oxley Act of 2002 is the popular name for the "Public Company Accounting Reform and Investor Protection Act of 2002," the "Corporate Auditing and Accountability Act" or H.R.3763. It is also referred to as SARBOX or "the Act."

SARBOX-compliance has International Reach

Even though SARBOX is a US law, it has international implications. International companies with offices in the US must comply with its requirements [Nash, 2003]. SARBOX impacts European companies, many of which are dually listed on exchanges in Europe and the US, or which have subsidiaries headquartered in the US [Singleton, 2003]. Specifically, Section 106 states that its jurisdiction includes any foreign public accounting firm that prepares or furnishes an audit report to a publicly traded US company.

SARBOX-Compliance Demands Like Recurring Y2K

In effect, SARBOX-compliance demands on IT are like those of Y2K—recurring four times a year. IT is going to be held accountable for the quality and integrity of information generated by IS because failure carries strict criminal penalties—fines and jail time—for senior executives and directors [ISACA, 2003]. SARBOX compliance is now "a matter of survival for businesses, and a question of freedom for directors" [Nash, 2003]. AMR Research says 85 percent of companies predict that SARBOX will require them to make changes to their IT and application infrastructure [Surmacz, 2003].

Before discussing how this new legislation will change IT and internal controls, it is helpful to understand its background and set forth its major provisions.

Background: Enron and Loopholes in Securities Laws

Fraud and corruption at Enron were possible because of loopholes in the securities laws and auditing failures. Between 1996 and 2000, Enron reported sales increase from $13.3 billion to $100.8 billion. Enron was America's seventh largest company, with the potential of being the world's largest by revenue [Ackman, 2002]. However, within months Enron dropped from 7th largest US company into bankruptcy. How? It cooked the books and accounting firm Arthur Andersen did not try to stop it.

Enron took advantage of an accounting loophole that allowed the company to use gross value instead of net value when calculating profits from energy contracts [Ackman, 2002]. It sold the same product over and over again, but reported the product's full value in revenue each time. Many "buyers" were sham partnerships, or special purpose entities (SPEs), created by Enron executives. A recorded $1.2 billion in stock issues was "paid for" with a receivable (asset) [Benston, 2003]. Financial statements and annual reports did not disclose how Enron made its enormous profits, nor were the figures or SPEs questioned until it was too late. There were warning signs, but auditors responsible for disclosing material differences ignored them. One blatant warning was that each of Enron's 19,000 employees was generating $5.3 million in revenues annually. In comparison, Goldman Sachs generated $1.7 million per employee; while Microsoft, IBM, and Citigroup generated much less than $1 million per employee [Zelizer, 2002].

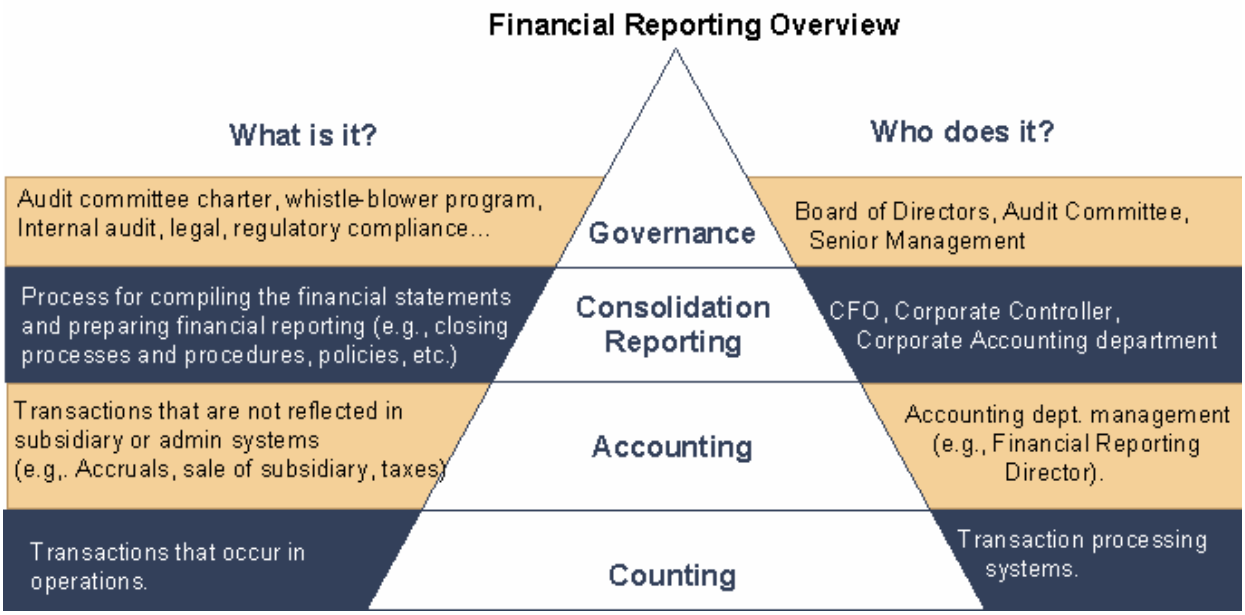
SARBOX Alters Corporate and Accounting Requirements

SARBOX significantly alters corporate and accounting requirements in six important areas: (1) auditor oversight, (2) auditor independence, (3) corporate responsibility, (4) financial disclosures, (5) analyst conflicts of interest, and (6) civil and criminal penalties for fraud and document destruction. [Anderson and Black, 2002]. The Act calls for the formation of a powerful Public Company Accounting Oversight Board (PCAOB, or "Oversight Board"). Firms must be able to produce unaltered e-records, other documents, and documentation of controls in a timely manner when summoned by PCAOB [Patzakis, 2003].

The Act specifies its requirements in "sections," several of which greatly concern managers and those in IT. Sections 302 and 906 require management's certification of their company's financial results. Section 404 requires executives to attest not only on their companies' financial statements, but also on control processes surrounding collection of the data behind them—down to the transaction level [Gallagher, 2003]. Section 409 requires real time disclosures. Compliance with those sections require that each step in a transaction—from order, to payment, to storage of data, to aggregation into financial reports—will need to be audited, verified, and monitored so that key people can be alerted promptly when something goes wrong. Figure 1 shows the inputs, activities, reporting processes, and disclosures that are needed to meet SARBOX financial reporting requirements.

Compliance with financial reporting and other requirements are impacting a wide variety of IT operations and creating significant challenges related to managing, reporting, and protecting data and business records. Regardless of whether they are deliberate or accidental, compliance failures or the alteration or destruction of business records, including e-records, carry strict criminal penalties [Patzakis, 2003].

The second section of this paper discusses the sections of the Act that have the greatest impact on IT. The third section identifies SARBOX-compliance research areas.



Adapted from John Lambeth, Sarbanes-Oxley Workshop. PriceWaterhouseCoopers, February 10, 2004.

Figure 1. Overview of Financial Reporting Requirements

The SEC and other regulatory agencies will, under SARBOX, seek to insure corporate responsibility through laws on internal controls, corporate governance, and fraud and records retention. Therefore, it is important that those who design, audit, or manage information systems understand these three compliance issues.

SARBOX SECTIONS IMPACTING IT

Internal Controls: Title III—Corporate Responsibility

Section 302. Corporate Responsibility for Financial Reports

Section 302 applies to financial statements and other financial information. It requires CEOs and CFOs to certify ("sign") all of the following in each annual and quarterly report:

- That they have reviewed the report, and, to the best of their knowledge, the report does not contain an untrue statement or omit any material fact.
- That the report fairly presents the issuer's financial condition and results of operation.
- That they are responsible for establishing and maintaining internal controls and have designed “Disclosure Control Procedures” (DCP) in such a way that all material information relating to the issuer and its consolidated subsidiaries is made known to them during the reporting period.
- That they have evaluated the effectiveness of internal DCP within the 90 days prior to the report and they have presented in the report their conclusions about the effectiveness their DCP as of that date;
- That they have disclosed to the company's auditors and to the audit committee all significant deficiencies in the design or operation of internal controls as well as any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls;
- That there have been no significant changes in internal controls that could affect statements in the future, and that if there are such changes, of what type and importance. [Coffee, 2002].

The personal certification requirement is designed to deter corporate executive fraud by instilling personal accountability. The intent of stronger internal controls is to increase the reliability of financial reporting by reducing risk of fraud and other misstatements [Kliegman, 2003].

Internal Controls: Title IV—Enhanced Financial Disclosures

Section 404. Management Assessment of Internal Controls

Another main thrust of SARBOX is management's assessment of internal controls—Section 404. Most companies focus on Section 404 because it requires that CEOs and CFOs certify the effectiveness of the financial controls they have in place [Hoffman, 2003]. It requires a new disclosure document referred to as an *internal control report.* An internal control report, which is to be included in every annual report, must:

- "state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting" [Section 404(a)].
- contain management assessment of "the effectiveness of the internal control structure and procedures of the issuer for financial reporting," which the audit firm must "attest to and report on" [Section 404(b)].

Section 404 addresses both the design and operational effectiveness of financial reporting controls by requiring that internal control processes, procedures, and practices must be documented and tested. The SEC maintains that the purpose of Section 404 is to provide investors and others with reasonable assurance that companies have designed processes to help ensure that transactions are properly authorized, recorded and reported, and assets are safeguarded against unauthorized or improper use. As such, the intent of Section 404 is to prevent fraud and demonstrate adequate control.

Section 401. Disclosures in Periodic Reports

Section 401 requires disclosure of "all material off-balance sheet transactions, arrangements, obligations (including contingent obligations) and other relationships" that might have a "material current or future effect" on the financial health of the company. Each annual report must include management's opinion regarding the effectiveness of the issuer's internal control procedures and a description of management's role in establishing and maintaining those procedures [Zelizer, 2002]. Section 401 restricts the use of pro forma information [Coffee, 2003]. This section states that information contained in a public company's reports must be "presented in a manner that . . . reconciles it with the financial condition and results of operations of the issuer under generally accepted accounting principles."

Section 409. Real Time Issuer Disclosures.

Section 409 requires companies to disclose any events that may have material impacts on their financial condition or operations on a "rapid and current basis" and "in plain English." While what is meant by *timely* has yet to be defined, it might be as soon as 48 hours from event. This section states that disclosure may need to "include trend or qualitative information and graphic presentations, as the Commission determines . . . is necessary or useful for the protection of investors and in the public interest."

Corporate Governance Title IX—White Collar Crime Penalty Enhancements

Section 906. Corporate Responsibility for Financial Reports

Section 906 holds CEOs, CFOs, and corporate directors both accountable and liable for the accuracy of financial disclosures. In contrast to Section 302, Section 906 penalties only apply if the officer knows of the problem or error when certifying a report [Razzano, 2003]. According to Section 906:

- Certifying a report knowing it does not meet the requirements of this Section results in a fine of up to $1,000,000, or imprisonment of not more than 10 years, or both.
- Willfully certifying any statement knowing it does not meet the requirements results in a fine of up to $5,000,000, or imprisonment of not more than 20 years, or both.

Fraud and Records Retention:Title VIII—Corporate and Criminal Fraud Accountability, Section 802. Criminal Penalties for Altering Documents

Section 802 applies to the retention of corporate audit records and expressly includes e-records in the mandate. This section creates new criminal penalties for document alteration and destruction. Section 802 imposes a fine and/or imprisonment of up to 10 years for failure of any accountant who conducts an audit of a publicly traded company to "maintain all audit and review work papers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded." This new statute is much broader than those that were available to federal prosecutors at the time of the Andersen indictment [Anderson and Black, 2002].

Procedures for preserving e-records that comply with SARBOX requirements are needed since they will be subject to greater scrutiny. SARBOX legislation demands e-records management like never before now that an unprecedented pool of e-records is being created that is subject to discovery [Volonino, 2003]. For example, e-records may need to be stored in read-only format throughout their mandatory retention period, and safeguarded through sound computer security procedures to prevent alteration [AOMAR, 2003].

The Oversight Board was given broad investigative powers largely involving the production of e-records. Section 105 authorizes the Oversight Board to "require the production of audit work papers and any other document or information in the possession of a registered public accounting firm or any associated person thereof." This section also authorizes the Board to suspend or bar any individual from association with a registered public accounting firm or to suspend or revoke the registration of any public accounting firm for failure to produce requested documents. Firms will need mechanisms to conduct enterprise-wide discovery efforts to retrieve electronic evidence (e-evidence) in response to Oversight Board inquiries.

SARBOX-COMPLIANCE RESEARCH AREAS

This massive, zero-tolerance legislation has created challenges that rival those of any IT implementation. The research issues emerging from the challenges range from behavioral factors for facilitating collaborative policy development to technological factors to automate data flows.

Collaboration on Policy Development

To be in compliance with regulatory boards, companies need to develop and deploy effective computer security response and investigation policies. Those policies will require collaboration between corporate IT security teams and IT auditors. Methods to facilitate this collaboration need to be devised.

Business Intelligence and E-Records Management

From the BI perspective, the important sections pertain to e-record management. SARBOX links e-record management accountability between internal and external record managers in a supply-chain fashion—as electronic data interchange (EDI) and ecommerce has linked data, documents and records in commercial transactions. This chain-of-accountability requires that companies deploy e-record storage methods that enable efficient retrieval. Strategies for reliable and verifiable e-record management and retrieval are needed.

System Integration for Fraud Detection

There is a serious lack of IS that can verify accountancy information that links sales, stock, and returns to meet compliance demands. Consider a classic fraud scheme that involves dispatching more goods than were actually sold, thus generating bogus sales in the last month of the quarter. Then in the first month of the next quarter, the "after returns" get accounted for and generate negative sales. To detect this fraud and many other types, IS must be capable of seamlessly linking both the

sales estimates and sales reality to the financial function. Simply looking at historic accounting information cannot detect fraud, much less detect it before another financial report is issued. Methods for IS integration and fraud detection are needed as well as understanding the nature and warning signs of fraud.

Electronic Discovery for Corporate Compliance

Numerous investigations by New York Attorney General Eliot Spitzer and the SEC and private class action lawsuits alleging fraud relied heavily on internal electronic communications [Volonino, 2003]. These cases illustrate the risk of electronic discovery facing all public companies. Research into how to prepare to respond to requests (or demands) for e-records by the Oversight Board is urgently needed. Electronic discovery ties to research in e-record management and fraud detection.

Transaction Control and documentation

Batch or historic reporting systems need to be reviewed and updated to support real-time reporting requirements. Transactions must be controlled and documented even though what constitutes sufficient documentation of controls remains vague. Nonetheless, to document the accuracy and integrity of the flow of information through transactions, risks and controls be understood sufficiently. Linkages and inter-dependencies among transactions and processes (including where transactions start and stop) must be identified. IS are needed that can specify what can go wrong in data processing, where controls are needed, how to prevent and detect control problems, and who is responsible for monitoring the controls.

Section 404 requires organizations to test and document processes and procedures designed to prevent fraud and demonstrate adequate control. Consider control issues for procurement. Those control issues would include proper division of duties, e.g., ordering, receiving, stocking, invoice approval, invoice payment. Research is needed into what are best practices in IS design and integration to:

- Validate and restrict purchases to authorized suppliers and amounts.
- Restrict purchase requests to authorized employees.
- Validate approval of a purchase request to authorized management levels.
- Record purchase transactions correctly in purchasing or financial systems.
- Give only authorized employees real-time access to contracts or notifications that may impact financial reporting.

Documenting process control involves addressing:

- How to document processes and controls.
- How to verify the effectiveness of internal controls.
- How to determine an adequate level of monitoring and preventative measures.
- How to implement controls across multiple processes.
- How to implement processes across a decentralized organization.
- How to design inventory management processes that increase control of assets against unauthorized use.

Managing Greater Management Involvement

In their reports, managers must address the design and operating effectiveness of internal controls. To do so, those internal controls must be tested. The testing that needs to be done will depend on the IS and type of control being validated. It is important to note that testing must be done to establish a basis for management's conclusion. Simply asking whether controls are adequate is not sufficient. Senior management will be taking an active role in evaluating IS and audit processes.

CONCLUDING REMARKS

Determination to increase corporate responsibility has ushered in new legislation that impacts IT directly. The Sarbanes-Oxley Act requires all US public companies registered with the SEC to prepare for ongoing audit activities and document

management responsibilities in 2004. With increased disclosures, new enforcement schemes, and emphasis on corporate accountability, SARBOX delivers significant reform—and demands on IS.

This article presented an overview of SARBOX to provide a basic understanding of the purpose and intent of those sections that will drive IT-related research. Policies, methodologies, and IT are needed for retention of financial and audit records for seven years; certification of internal financial controls by senior management; and disclosure of any events that will have a material impact on finances 'on a rapid and current basis.'

REFERENCES

1. Ackman, Dan (2002) "Enron the Incredible," Forbes.com, Jan. 15. (current February 22, 2004) http://www.forbes.com/2002/01/15/0115enron_print.html
2. Anderson, Peter J. and Black, Alana Rae (2002) "Accountants' Liability After Enron," S&P's: The Review of Securities & Commodities Regulation, 35(18) Oct. 23, p. 227.
3. AOMAR (Accounting Office Management & Administration Report), (2003) April, p. 8.
4. Benston, George J. (2003) "The Regulation of Accountants and Accountants and Public Accounting Before and After Enron," Emory Law Journal, 52(*1325) Summer.
5. Cangemi, Michael P. (2003) "Sarbanes-Oxley Act," The Information Systems Control Journal, 3, p. 5.
6. Coffee, Jr., John C. (2002) "A Brief Tour of the Major Reforms in the Sarbanes-Oxley Act," ALI-ABA Course of Study Materials—Course number SH097, December.
7. Emeritz, Robert. (2003) "Southern District of NY Revisits, Revises *Rowe* Standards for E-discovery Cost Allocation," Digital Discovery & e-Evidence, 3(6) June. pp. 1, 6-7.
8. Gallagher, Sean (2003) "Gotcha! Complying with Financial Regulations," Baseline Magazine, August 1, (current February 22, 2004). http://www.baselinemag.com/article2/0,3959,1211224,00.asp
9. Haider, M.W. (2004) "RIM Guide to the Sarbanes-Oxley Act," ARMA International, (current February 22, 2004) http://www.arma.org/legislative/rim_guide.cfm
10. Hoffman, Thomas (2003) "Users Struggle to Pinpoint IT Costs of Sarbanes-Oxley Compliance," November 21, Computerworld, (current February 22, 2004) http://www.computerworld.com/managementtopics/management/itspending/story/0,10801,87446,00.html
11. ISACA website. (current February 22, 2004) http://www.isaca.org
12. Iwata, Edward (2003) "Accountant Arrested under Sarbanes-Oxley," USA Today, Sept. 25, (current February 22, 2004) http://www.usatoday.com/money/companies/regulation/2003-09-25-ernst_x.htm
13. Kliegman, Edwin J. (2003) "Sarbox's Unseen Costs," CFO Magazine, November.
14. Leibowitz, Wendy R. (2003) "Conference Highlights Theory and Practice in Electronic Records Management", Digital Discovery & e-Evidence, 3(1) January 2003. pp. 1, 4-5.
15. Michaluk, Gerald (2004) "Sarbanes-Oxley: New Technology Needed," Business Week. No. 3869, Feb. 9, p. 8.
16. Nash, Emma (2003) "Compliance Must by Top of Your Agenda," Computing, November 27, p. 33.
17. Patzakis, John (2003) "New Accounting Reform Laws Push For Technology-Based Document Retention Practices," International Journal of Digital Evidence, 2(1) Spring.
18. Razzano, Frank C. (2003) "Outline of Sarbanes-Oxley Act of 2002 and Rules," ALI-ABA Course of Study Materials, Corporate Governance Institute, Sponsored with the cooperation of the Columbia Law School Center on Corporate Governance, June.
19. Singleton, Tommie (2003) "The Ramifications of Sarbanes-Oxley," Information Systems Control Journal, 3, pp. 11-16.
20. Staff Writer (2003) "Procurement Perspectives: What Sarbanes-Oxley 404 Means to You," Business Wire, November 18.
21. Surmacz, Jon (2003) "Financial Fallout," CIO Magazine, May 28, (current February 22, 2004) http://www2.cio.com/metrics/2003/metric552.html

22. Trends. (2003) "Instant Messages Emerging as Newest Source of E-Evidence," Digital Discovery & e-Evidence, 3(9) September, pp. 1-3.
23. Volonino, Linda (2003) "Electronic Evidence and Computer Forensics," Communications of AIS, 12(27) November. pp. 457-468.
24. Zelizer, Ethan G. (2002) "The Sarbanes-Oxley Act: Accounting for Corporate Corruption?" University of Chicago Loyola Consumer Law Review, 15(*27) (15 Loy. Consumer L. Rev. 27).

APPENDICES

Appendix I: Records and Information Management (RIM) Guide

The Association for Information Management Professionals (ARMA) has published a records and information management (RIM) guide to the Sarbanes-Oxley Act (Haider, 2004). The RIM guide, in Excel spreadsheet format, lists the different categories of records and highlights who is responsible for compliance. http://www.arma.org/legislative/rim_guide_sarbanes.xls This guide also helps distinguish which compliance issues are internal to the firm and which compliance issues are the responsibility of external suppliers, such public accounting firms.

LIST OF ACRONYMS

AICPA	American Institute of Certified Public Accountants
BI	Business intelligence
CFE	Certified Fraud Examiners
DCP	Disclosure Control Procedures
IA	Internal audit
IS	Information systems
ISACA	Information Systems Audit and Control Association
ISSA	Information Systems and Security Association
IT	Information technology
NASD	National Association of Securities Dealers
PCAOB	Public Company Accounting Oversight Board ("Oversight Board")
SEC	Securities and Exchange Commission
SARBOX	Sarbanes-Oxley Act of 2002 (the "Act")
SPE	Special purpose entities
US	United States