Communications of the Association for Information Systems

Volume 14 Article 11

August 2004

Holistic Compliance with Sarbanes-Oxley

Linda Volonino
Canisius College, volonino@canisius.edu

Guy H. Gessner
Canisius College, gessner@canisius.edu

George F. Kermis
Canisius College, kermisg@canisius.edu

Communications of the Association for Information Systems

HOLISTIC COMPLIANCE WITH SARBANES-OXLEY

Linda Volonino
Information Systems
Guy H. Gessner
Marketing
George F. Kermis
Accounting
Canisius College
volonino@canisius.edu

ABSTRACT

The theory underlying US securities laws is that investors are helpless without reliable information [Zelizer, 2002]. When Enron's collapse and other corporate frauds made it clear that "practically every element of our system of safeguards failed until it was too late to repair the damage," Congress reinforced those laws by passing the Sarbanes-Oxley (SARBOX) Act [O'Malley, 2002]. This new law demands that C-suite executives confirm their confidence in the quality and integrity of information generated by information systems by signing the figures off personally. Under SARBOX, the Securities and Exchange Commission holds executives accountable for reliable internal controls, record retention, and fraud detection. In turn, executives are looking to information systems and to IS auditors to help them meet their regulatory responsibilities.

This article discusses SARBOX mandates and the intent of regulatory agencies. That understanding lays the foundation needed to develop holistic SARBOX compliance programs with information technology and business process improvements. Holistic compliance is an enterprise-wide and long-term approach that views the new law as opportunities to improve internal controls and public reporting. Holistic compliance stands in contrast to simply complying with the rules or silo compliance; i.e., efforts scattered throughout business silos. We identify SARBOX requirements ("sections") concerning IS and IS research. Research areas to achieve minimal compliance include methods for IS assurance and auditing, risk management, and electronic records management (ERM). Research in business intelligence, data warehousing and mining, and supply chain management are necessary for holistic compliance that improves competitive position. While research efforts in these areas are not new, regulations have made them more compelling and urgent issues for senior management.

Keywords: Sarbanes-Oxley Act, IS compliance issues, internal controls, auditing, risk management, electronic records management, legal issues

I. INTRODUCTION

BACKGROUND: ENRON AND LOOPHOLES IN SECURITIES LAWS

Fraud and corruption at Enron were possible because of a combination of loopholes in the securities laws and because of auditing failures. Enron was America's seventh largest company, with the potential of being the world's largest by revenue [Ackman, 2002]. Between 1996 and 2000, Enron reported sales increases from $13.3 billion to $100.8 billion. However, within months Enron dropped from 7th largest US company into bankruptcy. How? It cooked the books along with their accounting firm Arthur Andersen because there were no material disincentives to stop it.

Enron took advantage of an accounting loophole that allowed the company to use gross value instead of net value when reporting 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.

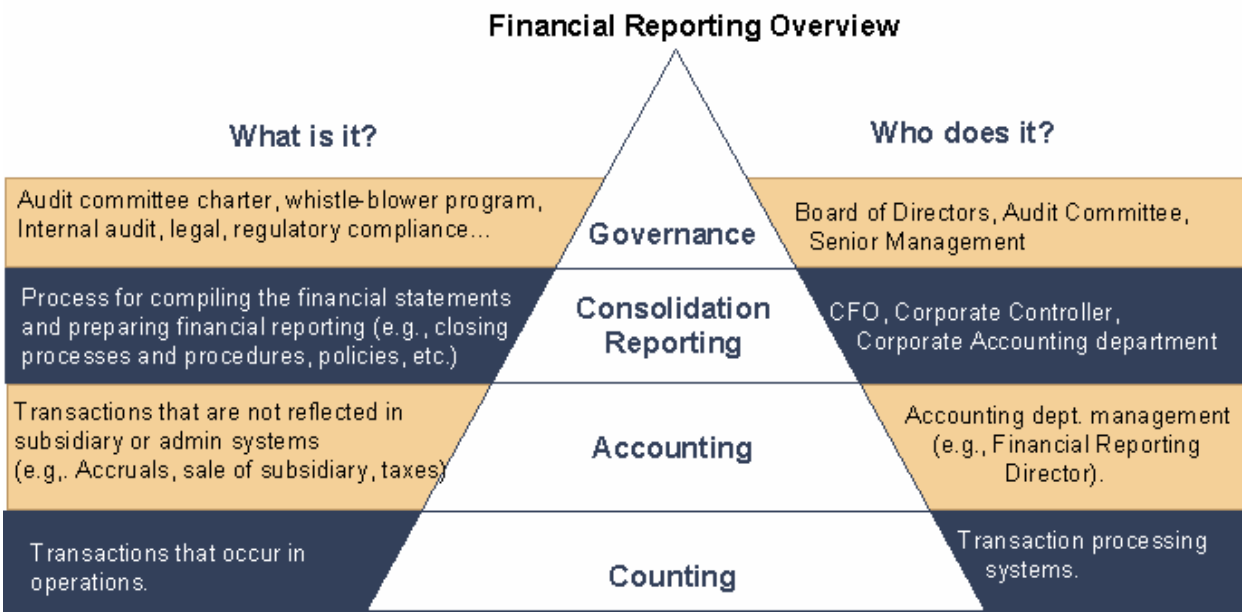
CONGRESSIONAL REACTION

Determined to prevent the second coming of Enron, Congress passed the Sarbanes-Oxley Act in 2002.[1] Congress' goals are to restore investor trust, stabilize markets, and plug loopholes in existing securities laws [Zelizer, 2002]. This anti-corporate crime law is stringent, the penalties for those who break it are notably harsh, and the regulatory agencies that it has created are powerful.

The Act contains eleven Titles that specify mandatory requirements in "sections," several of which greatly concern executives and those in IT. (See Appendix III.) Several Titles are the Corporate and Criminal Fraud Accountability Act (Title VIII), the White-Collar Crime Penalty Enhancements Act of 2002 (Title IX), and the Corporate Fraud Accountability Act of 2002 (Title XI). Important sections include sections 103 and 802 that specify audit record retention and security requirements. 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 the control processes surrounding collection of the data behind them—down to the transaction level [Gallagher, 2003]. Section 409 requires real time disclosure of financial and operating events. Compliance with these two 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. Details of SARBOX sections impacting IT and IT-mediated business processes are explained in Section III.

Figure 1 shows the inputs, activities, reporting processes, and disclosures that are needed to meet SARBOX financial reporting requirements.

[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."



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

Figure 1. Overview of Financial Reporting Requirements

Compliance with these financial reporting and related 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 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-COMPLIANCE DEMANDS ARE LIKE RECURRING Y2K

Quarterly financial reports will have to be filed 35 days after the end of each quarter (down from 45 days). Annual reports will be due 60 days after the close of the fiscal year (down from 90 days). These reports must also document and attest to the effectiveness of financial controls that produced the numbers.

In effect, SARBOX-compliance demands on IT are like those of Y2K—recurring four times a year. Unlike year 2000 remediation projects, the ISs and procedures that are put in place must be maintained diligently for the life of the company. Auditors and regulators will be demanding to be shown the basis for financials. IT is going to be held accountable for the quality and integrity of information generated by IS because they cannot afford to be wrong. Failure carries strict fines and jail time for senior executives and directors. SARBOX compliance has been described as "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].

HOLISTIC APPROACH TO COMPLIANCE

Knowing that executive commitment is key to success, executives are held personally liable for violations. They must confirm their confidence in the quality and integrity of information generated

by IS by signing the figures off personally. To be in compliance, chief officers must certify that their financial results are accurate, that all material information is reported in a timely fashion, and that ironclad process controls protect the quality and integrity of their financial data.

While SARBOX is the federal legislation that gets the most attention, there are other compliance requirements that put demands on IS infrastructures and processes. The Gramm-Leach-Bliley Act of 1999, USA PATRIOT Act, Basel II[2], and HIPAA[3] require solid processes to collect and control data. Furthermore, there are less familiar industry-specific laws, such as those affecting the transportation (railroad) industry requiring, for example, that they provide detailed shipping information within four hours of a suspected terrorist attack. Common to all of these laws is some mix of civil, criminal, or other punitive measures for violators. It is evident that there will be ongoing legislation that increases demands on IT and business processes. Compliancy is not possible without ISs that can reveal the real financial status or other details of the organization quickly and accurately.

Basic compliance efforts lead to immediate tactical results, but run the risk of being a series of patches or silo compliance efforts. If at the same time, companies view the new law as opportunities to improve operations, they can get better returns from the longer-term strategic value of business improvement and competitive advantage. These holistic solutions include redesigning business processes to reduce unnecessary complexity, improve information quality and risk management, and document organizational knowledge.

ORGANIZATION OF THIS TUTORIAL

Section II discusses IT management issues relevant to the new responsibilities imposed by SARBOX. This section provides a framework for a holistic approach to achieve the highest return on investment in compliance. It identifies opportunities for IT to contribute to an organization's long-term growth. It shows why expending a lot of effort on a silo approach tends to be riskier and less effective given ongoing regulatory mandates. Section III discusses the sections of the Act with the greatest impact on IT. Section IV identifies SARBOX-compliance research areas.

II. IT MANAGEMENT ISSUES

NEW STATURE OF IT SYSTEMS AND PROCESSES

Executives and boards of directors must attest that stringent policies and procedures are in place in their companies for reporting financial information accurately and promptly. Specifically, they must attest that processes provide reasonable assurance that the company's:

- transactions are properly authorized
- assets are safeguarded against unauthorized or improper use, and
- transactions are recorded properly and reported promptly.

These requirements involve a wide variety of IT to sustain compliance and controls. The challenge is that for decades, IT based its stature on reliability and availability. As of 2004, it rests on the honesty and truthfulness of IT systems and information [Hackathorn, 2004]. Corporate leaders need to know:

> *Can we trust our ISs to record valid business activity and our data warehouse to report valid business performance?*

IT's ability to answer these questions is vital.

---

[2] The New Basel Capital Accord
[3] Health Information Privacy and Accountability Act

FINANCIAL INFORMATION IS PUBLIC PROPERTY

Financial reports and audits of those reports are the property of the public—and not the company. This concept explains why all regulations share a common goal—information reporting that is timely, transparent, and trustworthy. The methods to achieve this goal are "compliance mandates" and penalties. SARBOX gives the SEC broad power to prosecute senior management for inaccurate financial reports, fraud, or destruction of financial records or audit documents. For example, Sarbanes-Oxley 404[b] requires a system of internal controls to assure the proper authorization and recording of transactions. Internal control requires that data passing from transactions and events through to financial statements be controlled and preserved so as to not destroy the details.

What is striking about Section 404b is that it mandates an annual management report and auditor review concerning the effectiveness of internal controls. In the past, regulators were limited because they could only punish attempts to "knowingly circumvent or knowingly fail to implement a system of internal accounting controls..." [15 U.S.C. § 78m[b][5]]. Now, violators of any rule issued under this Act may face civil or criminal charges, jail time, and fines regardless of whether they knowingly failed to comply.

CONTROL SYSTEMS AND PROCESSES TO PROTECT PUBLIC INTERESTS

Calls for internal control systems can be found in literature dating back to 1958 [Raphaelson and Walden, 2004]. That year the American Institute of Certified Public Accountants [AICPA] attempted to define a system to ensure corporate control over transactions, assets, and operations. Among other things, AICPA recommended that procedures be developed to safeguard assets from pillaging and misuse, and to maintain complete and accurate financial records. However, the SEC did not mandate these procedures.

Then in September 2003, regulators "fired a warning shot" of their readiness to protect public interests by using enhanced powers to bring actions against violators [Kerrison, 2003]. They charged former Ernst & Young partner Thomas Trauger with "obstruction of justice" for destroying audit papers and obstructing an investigation into a failed Internet credit card issuing company [Iwanta, 2003]. Under SARBOX, he faces up to 25 years in prison and $500K in fines.

The U.S. Department of Justice (DOJ) white-collar crime task force is also involved in the crackdown on corporate fraud. The task force prosecuted top executives at Enron, WorldCom, HealthSouth, and Adelphia, and won over 200 convictions. In July 2004, former Enron CEO Kenneth Lay was indicted on eleven counts of securities fraud and conspiracy. Lay faces up to 175 years in prison and $5.75 million in fines if convicted on all counts included in his indictment [CNN Money, 2004].

While SEC regulators intend to protect investors by minimizing risk of accounting fraud or corporate governance failures, IS management must also protect public safety. Specifically, the U.S. PATRIOT Act of 2001 and Executive Order 13224 demand that companies conduct better oversight of their business partners and employees to ensure that nothing they or the company does supports terrorism in any manner.

SARBOX ALTERS CORPORATE AND ACCOUNTING REQUIREMENTS

SARBOX significantly alters corporate and accounting requirements in six important areas: [Anderson and Black, 2002]:

- auditor oversight,
- auditor independence,
- corporate responsibility,

- financial disclosures,
- analyst conflicts of interest, and
- civil and criminal penalties for fraud and document destruction.

The Act called 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 or they will be sanctioned [Patzakis, 2003].

A standard adopted March 9, 2004 by the PCAOB will require auditors to evaluate and express an opinion about the fraud controls in place at any company they audit starting Nov. 15, 2004.

III. SARBOX SECTIONS IMPACTING IT

INTERNAL CONTROLS: TITLE III—CORPORATE RESPONSIBILITY

Section 302. Corporate Responsibility for Financial Reports

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

- That they 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 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 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 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 play a significant role in the issuer's internal controls.
- That no significant changes were made 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 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 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 also 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 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.

Financial Executives International, an association of corporate finance managers, conducted a survey in May 2003 to determine estimated Section 404 compliance costs. On average, the 83 respondents predicted spending $480,000 on software, consulting services and employee training in advance of the compliance deadlines [Hoffman, 2003]. Fortune 1,000 companies are estimated to have spent an average of $2.5 million on SARBOX compliance work in 2003.

Section 409. Real Time Issuer Disclosures.

Section 409 requires companies to disclose any events that may impacts on their financial condition or operations materially 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 an 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 apply only if the officer knows of the problem or error when certifying a report. 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 CORPORATE AND CRIMINAL FRAUD ACCOUNTABILITY

Section 802. Criminal Penalties for Altering Documents

Section 802 applies to the retention and protection of corporate audit documents and related records. It expressly includes e-records in the document management mandate. Document management is the making available of documents and information associated with them when and where required for a particular set of operations. This section creates new criminal penalties for altering, falsifying, or destroying documents.

These provisions are intended to close loopholes revealed in the prosecution of the Enron and Arthur Andersen cases. These provisions are not limited to registered public accounting firms, publicly traded companies, or investment banking firms. They apply to every individual and/or organization that retains records.

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 statutes that were available to federal prosecutors at the time of the Andersen indictment [Anderson and Black, 2002].

IV. SARBOX-COMPLIANCE RESEARCH AREAS

This massive, zero-tolerance legislation has created challenges that rival those of any IT implementation. To comply fully with the spirit of the law, rather than minimally comply with the letter of the law, is the better approach. The former approach—holistic compliance—may be the only way companies can sustain SARBOX compliance.

INFORMATION QUALITY ASSURANCE

Information quality is fundamental. Companies must ensure transparency, accuracy, timeliness, and reliability of their financials and operations. Information quality improvements will require research into:

- Process simplification and standardization
- Data simplification and standardization
- Technology standardization and integration

Numerous research issues emerge from these challenges, including behavioral factors for facilitating collaborative policy development and technological factors for automating data flows. To be in compliance with regulatory boards, companies need to develop and deploy effective information security response and investigation policies. Those policies will require collaboration between corporate IT security teams and IT auditors. Methods to identify policy requirements and facilitate collaboration need to be devised.

RETENTION OF ELECTRONIC COMMUNICATION

SARBOX legislation demands e-records management (ERM) now that e-records are subject to discovery in court trials and can be used as electronic evidence. Some industries affected by industry-specific regulations include financial services, health care, pharmaceuticals, and government. These regulations often specify retaining all electronic communications for three to six years or more. For example, pharmaceutical manufacturers must make their e-mail searchable for regulatory, audit, and legal inquiries, and keep e-mail metadata such as sender and subject line information online and easily accessible. After July 26, 2003, these organizations were required to file and report e-records, including e-mails.

While it was once acceptable to keep e-mail archives offline for only a few months, they must now be kept online for years [Allen, 2004]. SARBOX links ERM accountability between internal and external record managers in a supply-chain fashion—as EDI (electronic data interchange) and ecommerce link data, documents and records in commercial transactions. This chain-of-accountability must be documented and stored for efficient retrieval. E-mail management systems are needed with the ability to retain e-mail for a specified period of time, the ability to delete records based on corporate or regulatory policy, and the capability to query and retrieve specific records or associated content. Strategies for reliable and verifiable ERM and retrieval are also needed.

For companies whose records are subject to government audit, criminal penalties will apply if the document retention policy frustrated inquiry rather than facilitated it [Rowan, 2004]. The penalty for obstruction of justice by destroying documents or records related to an investigation increased from 18 months in prison to 30 to 37 months. The new sentencing measures took effect January 25, 2003

ERM systems must be able to manage all types of records, including documents, audits, e-mail, Web pages, forms, spreadsheets and other digital assets across the full information lifecycle, from creation to archive to deletion.

BUSINESS INTELLIGENCE AND KNOWLEDGE MANAGEMENT

The monumental task of documenting internal control effectiveness and preserving the details of workflows falls to business intelligence (BI). BI and knowledge management (KM) are key to holistic compliance. BI and KM ensure that institutional knowledge is documented and preserved. These functions can play a useful role in strengthening financial controls. The full power of BI capabilities should be directed toward improving overall efficiency and competitive position.

Audit tools are not enough for long-term SARBOX compliance because they lack two key features:

1. A document repository for distributing control documentation, approval, and testing to employees throughout the organization; and

2. Maintaining access control, version control, an audit trail, and e-records retention.

Audit tools are not suited for tracking SARBOX compliance efforts, including control documentation, review and approval, and testing.

IT SECURITY

The link between corporate governance and IT security is strengthening. While the act stops short of mandating detailed security provisions, the requirements for companies to produce audit reports is driving a recognition that IT security policies and procedures are an essential part of the process. A company could have comprehensive processes, but if there is a problem with the system that provides the data, the processes become of little or no value.

“Enhanced Regulatory Compliance” regulations, such as Gramm-Leach-Bliley, SARBOX, and HIPAA, require organizations to ensure that unauthorized users cannot access systems that contain sensitive data. Confidentiality breaches or unauthorized access must be reported promptly to those whose private data was compromised and to government agencies.

SYSTEM INTEGRATION FOR FRAUD DETECTION

Little software is available that allows I verifying accountancy information that links sales, stock, and returns to meet compliance demands. Data passed from events and transactions to financial statements must be controlled—and preserved so as not to destroy the details essential for fraud detection. 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 are understanding the nature and warning signs of fraud.

ELECTRONIC DISCOVERY FOR CORPORATE COMPLIANCE

Electronic discovery ties to research in e-record management and fraud detection. Numerous investigations by New York Attorney General Eliot Spitzer and by 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 reduce exposure and prepare to respond to e-record requests (or demands) by the Oversight Board (Section II) is urgently needed.

TRANSACTION CONTROL, INTEGRATION, 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 information flows from transactions to reports—particularly since a lot of information is lost in the multiple passes through the data—control mechanisms must 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, for example, control issues for procurement. These issues include proper division of duties, e.g., ordering, receiving, stocking, invoice approval, and 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.

SARBOX compliance requires IS to take on expanded roles, responsibilities and relationships. This expansion of responsibility is still a work in progress. 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. Therefore, senior management will be taking an active role in evaluating IS and audit processes. This involvement will revive research in systems to facilitate communication horizontally and vertically throughout the organization.

CONCLUDING REMARKS

SARBOX and other regulations created significant challenges that impact IT directly. SARBOX requires all US public companies registered with the SEC to prepare for ongoing audits and security checks, real-time disclosure of material facts, and document management responsibilities. With 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.' We propose that companies embrace a holistic compliance approach to achieve higher return on investment on their compliance efforts. Approaching holistic compliance from the strategic perspective of generating higher information integrity through IT and business processes that improve data flows and reporting capabilities, for example, can lead to lead to legitimate improvements in profitability.

EDITOR'S NOTE: Editor's Note: This tutorial, which was presented at AMCIS 2004, was received on July 14, 2004 and was published on August 15, 2004

REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Ackman, D. (2002) "Enron the Incredible," *Forbes.com,* Jan. 15. http://www.forbes.com/2002/01/15/0115enron_print.htm (current Aug. 10, 2004)

Allen, D. (2004) "E-Mail Storage: Your Next Mission-Critical Application," *Network Magazine,* March 1. http://www/networkmagazine.com/showArticle.jhtml?articleID=18201783 (current Aug. 10, 2004)

Anderson, P.J. and Black, A.R. (2002) "Accountants' Liability After Enron," *S&P's The Review of Securities & Commodities Regulation,* (35)18, Oct. 23, p. 227.

Benston, G.J. (2003) "The Regulation of Accountants and Accountants and Public Accounting Before and After Enron," *Emory Law Journal,* 52(section 1325) Summer.

CNN Money (2004) "Ken Lay Files for Quick Start to Trial," August 9 http://money.cnn.com/2004/08/09/news/newsmakers/enron_lay.reut(current Aug. 10, 2004)

Coffee, Jr., J.C. (2002) "A Brief Tour of the Major Reforms in the Sarbanes-Oxley Act," ALI-ABA Course of Study Materials—Course number SH097, December. https://d2d.ali-aba.org/index.cfm?fuseAction=displayCoursebookPaper&COMPONENT=2438&NAVMODE=coursebooks&NAVSUBMODE=2434 (current Aug. 10, 2004) Note: A fee of $19 is levied by Lexis-Nexis to view this article.

Gallagher, S. (2003) "Gotcha! Complying with Financial Regulations," *Baseline Magazine*, August 1, http://www.baselinemag.com/article2/0,3959, 1211224,00.asp (current Aug. 10 2004).

Haider, M.W. (2004) "RIM Guide to the Sarbanes-Oxley Act," *ARMA International,* http://www.arma.org/pdf/RIMGuideSarbanes.pdf (current Aug. 10, 2004)

Hackathorn, R. (2004) "Nurture the Wealth," *Intelligent Enterprise.* 7(3) March 6, p. 10-13.

Hanna, G. (2004) "What Lies Beneath: Technology That Supports Effective Compliance," *Legal Tech Newsletter*. (21)10 January 12, p. 1-6.

Hoffman, T. (2003) "Users Struggle to Pinpoint IT Costs of Sarbanes-Oxley Compliance," *Computerworld,* Nov. 21 http://www.computerworld.com/industrytopics/financial/story/0,10801,87613,00.html (current Aug. 10, 2004)

Iwata, E. (2003) "Accountant Arrested under Sarbanes-Oxley," *USA Today,* Sept. 25,http://computercops.biz/modules.php?name=News&file=article&sid=3610 (current Aug. 10, 2004)

Kerrison, O. (2003) "E&Y Partner One of First Victims of Sarbanes-Oxley after NextCard Probe," *The Accountant*, October 31, p. 3.

Kliegman, E.J. (2003) "SARBOX'S Unseen Costs," *CFO Magazine*, November.

Leibowitz, W.R. (2003) "Conference Highlights Theory and Practice in Electronic Records Management", *Digital Discovery & e-Evidence*, (3)1 January 2003. pp. 1, 4-5.

Nash, E. (2003) "Compliance Must be Top of Your Agenda," *Computing,* November (27), p. 33.

O'Malley, S. (2002) "Statement Before the Senate Committee on Banking, Housing, and Urban Affairs," *Accounting and Investor Protection Issues Hearing. 107th Congress.* http://64.233.167.104/search?q=cache:-VICy_vOZZkJ:www.niea.org/documents/NIEA 04 winter news.pdf+O'Malley,+S.+(2002)+"Statement+Before+the+Senate+Committee+on+Banking,+Housing,+and+Urban+Affairs,"+Accounting+and+Investor+Proh (current Aug. 10, 2004)

Patzakis, J.(2003) "New Accounting Reform Laws Push For Technology-Based Document Retention Practices," *International Journal of Digital Evidence*, (2)1 Spring.

Raphaelson, I.H. and Walden, J. (2004) "Internal Controls: Cure-all or Snake Oil?" *Business Crimes*, (11)3, April 5, pp. 3-6.

Rowan, E. (2004) "Paper Shuffling, Byte by Byte," *Texas Lawyer.* (20)18, July 5, pp. 30-35.

Surmacz, J. (2003) "Financial Fallout," *CIO Magazine*, May 28, http://www2.cio.com/metrics/2003/metrics552.html (current Aug. 10, 2004)

Volonino, L. (2003) "Electronic Evidence and Computer Forensics," *Communications of AIS,* (12)27 November. pp. 457-468.

Zelizer, E.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).

APPENDIX I: SEC EXTENDED DEADLINE FOR REPORTING ON INTERNAL CONTROLS.

The SEC extended the compliance dates for Section 404 of the Sarbanes -Oxley Act. Section 404 requires public companies to include a report by management in its annual company financial filings a description and assessment of internal controls over financial reporting and disclose any material weaknesses in those systems. The rules also require a firm's outside auditor to attest to management's assessment of the company's internal controls. Large companies (those with equity market capitalization over $75 million) must comply beginning with the first fiscal year ending on or after Nov. 15, 2004 (originally June 15, 2004). Smaller companies must comply beginning with their first fiscal year ending on or after July 15, 2005 (originally April 15, 2005).

APPENDIX II: RECORDS AND INFORMATION MANAGEMENT (RIM) GUIDE

The Association for Information Management Professionals (ARMA) 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 as public accounting firms.

APPENDIX III: SARBANES-OXLEY ACT'S TABLE OF CONTENTS

TITLE I—PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
- Section 101. Establishment; administrative provisions.
- Section 102. Registration with the Board.
- Section 103. Auditing, quality control, and independence standards and rules.
- Section 104. Inspections of registered public accounting firms.
- Section 105. Investigations and disciplinary proceedings.
- Section 106. Foreign public accounting firms.
- Section 107. Commission oversight of the Board.
- Section 108. Accounting standards.
- Section 109. Funding.

TITLE II—AUDITOR INDEPENDENCE
- Section 201. Services outside the scope of practice of auditors.
- Section 202. Preapproval requirements.
- Section 203. Audit partner rotation.
- Section 204. Auditor reports to audit committees.
- Section 205. Conforming amendments.
- Section 206. Conflicts of interest.
- Section 207. Study of mandatory rotation of registered public accounting firms.
- Section 208. Commission authority.
- Section 209. Considerations by appropriate State regulatory authorities.

TITLE III—CORPORATE RESPONSIBILITY
- Section 301. Public company audit committees.
- Section 302. Corporate responsibility for financial reports.
- Section 303. Improper influence on conduct of audits.
- Section 304. Forfeiture of certain bonuses and profits.

Section 1105. Authority of the Commission to prohibit persons from serving as officers or directors.
Section 1106. Increased criminal penalties under Securities Exchange Act of 1934.
Section 1107. Retaliation against informants.

LIST OF ACRONYMS

AICPA	American Institute of Certified Public Accountants
BI	Business intelligence
DCP	Disclosure Control Procedures
DOJ	Department of Justice
ERM	Electronic records management
GLB	Gramm Leach Bliley Act
HIPAA	Health Information Portability and Accountability Act
IS	Information systems
ISACA	Information Systems Audit and Control Association
IT	Information technology
KM	Knowledge management
NASD	National Association of Securities Dealers
PCAOB	Public Company Accounting Oversight Board ("Oversight Board")
RIM	Records and Information Management
SARBOX	Sarbanes-Oxley Act of 2002 (the "Act")
SEC	Securities and Exchange Commission
SPE	Special purpose entities
US	United States

ABOUT THE AUTHORS

Linda Volonino is professor of Information Systems and department chair at Canisius College. She is director of the Master's program in Telecommunications Management and a Certified Information Systems Security Professional (CISSP). Her research and consulting areas are computer forensics and the role of IT in compliance. Website: http://is.canisius,edu

Guy H. Gessner is associate professor of Marketing and chair of assurance of learning at Canisius College. His research and consulting include the cost and complexity of compliance and its impact on customer relationship management.

George F. Kermis is associate professor of accounting at Canisius College. A Certified Public Accountant in New York State, he has worked in the international accounting firm Peat, Marwick, Main & Co. for six years. His research interests are in auditing, cost accounting, and compliance for financial institutions and service enterprises.

Communications of the Association for Information Systems

ISSN: 1529-3181