Sarbanes-Oxley Act of 2002 and IT Education

Craig A. VanLengen
Northern Arizona University, Flagstaff, AZ, USA

Craig.vanlengen@nau.edu

Abstract

Even though information technology (IT) educators have been teaching basic principles of information systems for over 20 years, business organizations have chosen to ignore or not implement them. By not integrating information systems and allowing uncontrolled manual intervention it was easier to commit the frauds and the financial scandals of the late 1990's and early 2000's. The frauds and financial scandals have resulted in a large increase in business regulation with many compliance requirements and possible fines and jail sentences for non-compliance. IT educators need to take some lessons from their accounting colleagues (Titard, 2004) and modify IT curriculum to take advantage of the compliance environment to focus on the basic principles of creating quality up-to-date information for organization decision making and to see them implemented.

Keywords: Sarbanes-Oxley, IT Education, IT curriculum, information systems, financial fraud, SEC compliance.

Introduction

Congress passed the Sarbanes-Oxley Act (SOX) in 2002 as a response to the public outcry over the financial scandals of many large corporations (Haskin, 2004). Top level management, chief executive officers (CEO's) and chief financial officers (CFO's), took advantage of poor internal control and reporting systems to misstate the actual financial position and results of their corporations for personal gain. Congress charged the Securities and Exchange Commission (SEC) with the responsibility of implementation and oversight. Since the passage of SOX in 2002 the SEC has been busy issuing rules and interpretations on the requirements of the act.

Most of the literature on the SOX act center around what finance and accounting professionals are doing to comply with the act. Underlying the concerns of accounting and finance is the data and information requirements that are specified or alluded to in the act. This paper will discuss what information technology (IT) professionals and educators need to be aware of in SOX.

IT Education Related to Sarbanes-Oxley

O'Brien (2004, p. 261) defines information quality as those characteristics that make information products valuable and useful. O'Brien (2004) presents these characteristics in dimensions of time, form, and content. The time dimension includes timeliness and currency, which provide up-to-date information needed for real-time decision making. Real-time reporting of material events is a requirement of SOX (Katz, 2003, 2004b). The form dimension requires that information be presented at the appropriate level of detail that is easy

to understand and interpret. The content dimension covers the areas of accuracy, relevance, completeness, conciseness, scope, and use for performance measurement. The areas of accuracy and completeness fall under the internal control certifications required by SOX. The important point to make here is that these characteristics of information quality are not new. These characteristics have been recognized by the IT profession for over 20 years, not just since 2002 after the passage of SOX.

Knowledge of internal controls and designing of controls into information systems is also not a new concept. Henry and Borrus (2005) state, "after all, Section 404 restates what was already required in other federal laws and regulations. Since the late '70s, the Foreign Corrupt Practices Act has required companies to have internal controls, and auditors have long been expected to test them before signing off on financial statements." The only difference is that now execs and auditors must certify that the controls work and that no material weaknesses exist (Henry & Borrus, 2004).

So if we have known about information quality and the necessity of controls why did we see the financial abuses of the late 1990's and early 2000's? It would appear that top-level management chose to override and/or ignore them. Carpenter, Fennema, Fretwell, and Hillison (2004) indicate that systems of controls are no better than the people that create, use, and supervise them. Durak (2004) makes this point by stating that "management can easily manage and boost earnings by changing the assumptions underlying key accounting estimates." Carpenter et al. (2004) also feel that external auditors need to be more skeptical and unpredictable in their audit of a company and quit trying to sell consulting services to their clients. The thing that is different with SOX, that was not in the previous acts, is the "jail time" penalty for non-compliance (Carpenter et al., 2004; & Henry & Borrus, 2004).

Risk management is another technique proposed as a way to mitigate problems with SOX compliance. Satzinger, Jackson, and Burd (2004) discuss risk management and mitigation as part of a software development project. Basically it requires management and development staff to identify risks, estimate the outcomes and the possibility of their occurrence, assign a priority to each identified risk, and to develop and implement strategies to mitigate the risks. Once again risk management is not new to the information systems profession.

Another area of concern for SOX compliance is real-time reporting. We have been covering real-time systems capabilities for over 20 years. Katz (2003, 2004b) discusses the requirements of Section 409. Under "Section 409 companies must report material changes in the financial or operating condition of the company 'on a rapid and current basis'" (Katz, 2004b). Corporations must be able to do real-time reporting to the U. S. Securities and Exchange Commission (SEC) with a current report (8-Ks) within two business days. If the information system is not fully computerized and integrated this could be virtually impossible. Organizations will need information systems that perform real-time exception reporting on financial and non-financial data.

Besides financial information section 802 requires all business records, including those on electronic media, to be saved for 'not less than five years.' Lunt (2004) makes it clear that e-mail must be retained because it has become a standard way to do business. E-mails are used to answer customer inquiries, discuss business strategy, negotiate contracts, exchange invoices and payments, and to file regulatory documents. Basically if an e-mail or any attachments relate to a transaction or decision making of the organization it must be retained. Telberg (2003) states "smart document management is no longer just a good idea; it's required by law." Organizations must record and manage all documents whether on paper or in an electronic form.

Marlin (2004) reports on the requirements of Section 404 that requires public corporations with a market cap greater than $75 million to "include a statement attesting to the effectiveness of internal controls over financial reporting with their 2004 annual reports." The deadline for this state-

ment was delayed several times and the latest effective date was November 15, 2004. Ramos (2004) states that, "a company's financial reporting process must enable it to capture, record, process, summarize and report financial data" (p. 45). Marlin (2004) also reports that companies will spend greater than $1 billion on technology for SOX compliance and the cost continue to grow. Compliance requires companies to report material weaknesses in their internal control systems (Ramos, 2004). A material weakness is defined as a weakness that is significant and probable.

Another area brought out by Nyberg (2003) is the whistle-blower protection provided for by SOX. Under SOX Section 806 an employee with a "reasonable belief" of securities fraud is protected from retaliation by their employer. Even if an employee is found to be incorrect they are still provided protection under the act.

Small and medium sized public companies will also have to comply in the future. Parry (2004) points out that compliance rules are not different for them and in many cases audit compliance is dependent on the auditing firm. Smaller businesses do not have the negotiating expertise, knowledge base or resources that larger organizations have.

Many companies have been outsourcing business processes. Schneider (2004) cautions organizations on trying to use outsourcing of business processes as a means of obtaining SOX compliance. Outsource providers must be audited on an annual basis and provide audit reports identifying controls over the processes, the control objectives and preferably an auditor's opinion on the effectiveness of the controls. Organizations that outsource business processes must insist on full disclosure of controls and audit outcomes so that they can certify SOX compliance.

Basic Requirements

SOX is presented in Titles I to XI, with each title broken out into sections (Sarbanes, 2004a). The sections that will be discussed include those related to controls and the characteristics of quality information. SOX sections 302 and 404 require public companies to establish implement and evaluate internal controls as they relate to financial reporting (Sarbanes, 2004b, 2004c). Full text of the Sarbanes-Oxley Act can be found at (http://www.law.uc.edu/CCL/SOact/soact.pdf . It is important to recognize that controls do not start at the financial reporting level but start at the lowest level of operations. All operations of an organization impact financial reporting. Therefore it is important that controls are in place to provide for the information quality characteristic of performance monitoring by monitoring and reporting on the efficiency and effectiveness of operations.

SOX requires the audit committee to understand and assess strategic, operational, reputational, regulatory, and information risks (Banham, 2003). Companies are required to have processes in place to do a "reasonable" effort of discovering these risks and then reporting on them. This requires software that would capture the identified risks, probability of occurrence and capture events that would impact these risk areas.

Katz (2004) also identified other problems of compliance with SOX on the estimates that are used for employee benefits. For example what is the proper amount of liability to record for employee health care and defined benefit retirement plans? What is going to be the increase in insurance costs and what amount will be necessary to fund the retirement plans?

Problems with Current Control and Reporting Systems

Cantu, Gonzalez, Leal, Koong, and Liu (2004) conducted a survey of compliance by firms listed in the Russel 1000 Index. They evaluated compliance with the August 29, 2002 deadline for corporate executives to certify that the information in their annual reports was deemed accurate and

acceptable. They found that about 70 percent of the corporate executives were able to certify that the scheduled reports were correct by the deadline. In most cases the reports required revisions prior to the certification. Cantu's et al. (2004) survey reported that thirty percent of the organizations were not able to make the deadline. Telberg (2005) reported that in the last round of SOX compliance reporting six hundred U.S. companies admitted in their section 404 review "material weaknesses" in their internal control systems. Cantu et al. (2004) surmised that most of the organizations have not paid attention to what computer educators have been teaching for years about the necessity of data quality and processes to produce quality information products.

Kerner (2004) sees the volume of data and information already makes compliance difficult. The real-time data reporting to regulatory agencies will demand that the data be stored on direct access devices. The volume of data and information will continue to get worse. Goff (2003) reports on surveys that found most corporate executives are drowning in a sea of ever increasing data and information. A recent study by NCR Corp found that corporate executives had two to three times the information in the current year than what they had in the prior year (Goff, 2003).

Besides having too much information experts also estimate that "10 percent to 30 percent of the data flowing through corporate systems is bad – inaccurate, inconsistent, formatted incorrectly, entered in the wrong field, out of a value range, and so on" (Goff, 2003). Estimated losses from poor data were set at $600 billion (Kerner, 2004). SOX Section 404 requires corporate executives to certify the accuracy of their financial reports (Sarbanes, 2004c). Given the possible penalty of jail time (Henry & Borrus, 2005) how can corporate executives certify accuracy of their financial statements when the financial data used to create these reports are of such poor quality?

Goff (2003) reports on the problem Pfizer had when trying to implement a financial data warehouse. Corporate financial information was spread across 14 distinct systems. Goff (2004) reports on a Hackett Group estimate "that the average $1 billion company maintains 48 financial programs, along with nearly three enterprise resource planning (ERP) systems." Even organizations that are using one ERP system have several instances of the ERP system running. In many cases organizations are unable to "prove" or show how transaction data gets rolled up into the general ledger that is used for financial reporting. Kugel (2005b) reports that the consolidation process for most companies is a sequential, bottom-up process that is manual and very labor intensive. Companies need to change the consolidation process to a more centralized and synchronous process with little manual intervention. Add to the current problem with financial data the addition of e-mails, contractual data, presentation files, memorandums, and other correspondence.

Not only is volume a problem, a recent survey reported on by Taub (2004) found that over 90 percent of the respondents had identified gaps in their organizations internal control framework. One-third of the respondents identified "lack of process control-related documentation," as the internal control problem area.

Implications for Business and IT Education

After the corporate scandals at Enron, WorldCom and others numerous accounting programs made changes to their course offerings and the use of real-life case studies (Titard, 2004). A majority of accounting programs are predicting increases in enrollment at both the bachelor's and master's levels for 2004 after experiencing declines in accounting graduates of 27 percent from 1995 to 2002 (Titard, 2004). Accounting graduates are receiving more instruction on fraud awareness and detection and recognizing ethical issues (Titard, 2004).

Information systems curriculum regularly teach the concepts of information quality, system integration, monitoring of systems with exception reporting, business process reengineering, and using technology as an enabler for improvement. It appears that IT educators need to teach them

with more emphasis and use the breakdowns of the recent past as real-world case studies of what can go wrong if we ignore them.

As was already stated by O'Brien (2004, 261) information quality should be a primary concern for all business organizations. Cantu et al. (2004, p. 5) states that "compliance with governing standards and the ability to generate accurate reports affects all types of information systems." Beal (2003) gives seven steps a company can use for compliance with SOX. These steps include an information system that monitors both financial and non-financial data, Web-based, real-time capability, performance indicators monitored by software, a "sandbox" for analysis of "what-if" scenarios of future events, continuous flow of information from all sources, and lastly since most large organizations do business world-wide an international awareness. Beal (2004) sees SOX as a positive force that can be used to improve business process management performance. SOX requires reliable and credible information so business executives should use the requirements of the act to improve these areas.

Beal (2004) also states that technology needs to be used as an enabler for improvement of business processes and information reporting, yet according to a survey by IBM "only 19% of respondents said they were fully utilizing their ERP systems." Technology can be used on improving performance score carding to indicate control risks, planning, budgeting, forecasting and business modeling, and financial consolidation and reporting. Technology can provide the real-time access to financial reports, detection of control violations, and provide the audit trail necessary for compliance (Malwitz 2004).

Burriesci (2004) notes a study by Aberdeen that companies will provide for SOX reporting requirements within process improvement efforts. Incorporating regulatory reporting within new or existing IT systems would be a major improvement over an add-on system to provide the reporting after-the-fact. Gardner (2004) also reports on an Aberdeen study that found most IT managers would leverage and extend existing software to meet compliance with SOX. Kugel (2005a) feels that companies need to look beyond immediate compliance with SOX. Financial systems need to be redesigned by automating as much as possible, incorporating compliance controls, and reduce auditing requirements to make the creation of financial information and corporate decision-making as efficient as possible. Section 404 of SOX requires companies to replace informal control systems with formal systems to prevent fraud and insure quality (Sarbanes, 2004c). Eighty percent of the companies that must comply with SOX indicated that it was important to eliminate rekeying of data and automate accounting adjustments and accruals (Kugel, 2005a). Kugel (2005a) feels companies need to address other efficiency concerns such as using a standard chart of accounts for all parts of the organization and reducing the use and reliance on spreadsheet analysis. After financial systems are redesigned for efficiency and effectiveness an effort needs to be made to providing leading indicators for management to use in decision making. This way decision making can become future driven instead of focusing on past performance.

Another take on the problems with data integrity is from the security view. Hurley (2003a) asks, how can corporate executives certify the quality of the data and information when the data is insecure or the security to the data is untested? Hurley (2003b) recommends that organizations put someone in charge of evaluating security risks and implementing a security plan to defend against the identified risks. Schwartz (2004) states that security of information systems data and services requires multi-factor authentication. Security measures need to be simple so that they are used and not bypassed. If security measures become too difficult of complex uses will find a way around them or avoid them.

Business executives including IS professionals must be able to show that financial systems are compliant, financial reporting is timely and accurate, and do a better job of fraud monitoring, detection, and reporting. IT systems must be improved to automate and integrate processes, enhance

control and facilitate audits, provide documentation of processes and other supporting information on a timely basis (Kugel, 2003, 2004).

Compliance with SOX will require companies to document and show how detailed transactions are included in higher level financial systems (Leibs, 2003). Organizations need to automate current manual and error prone processes involved in financial reporting. Compliance with SOX may reach hundreds of business process and thousands of activities within those processes (McKie, 2004). IT and business need to be aligned (Noel, 2004). Business activities must be tied to processes and the processes must be documented and mapped to financial reporting. Trying to manage this effort without software would be a monumental effort.

Organizations can use SOX compliance to build a process-based management system as a foundation to building an integrated information system. All financial information will be expressed in activities and the business processes they support. Transactions and processes will be supported by documentation that is traceable, can be monitored and auditable (Sorensen, 2004).

Conclusion

IT professionals and IT educators need to take a lesson from accounting professionals and educators (Titard, 2004) and use compliance with Sarbanes-Oxley to reinforce the basic principles of information systems. These principles include: information quality, system integration, monitoring of systems with exception reporting, business process reengineering, and using technology as an enabler for improvement. IT educators need to use case studies of the frauds and financial reporting abuses to reinforce the need to apply basic principles of information systems. We would not need all the additional regulation if business organizations had applied the basic principles and auditing firms had required them prior to issuing a "clean" opinion on the fairness of the financial reports (Henry & Borrus, 2004). Since basic IT principles were not appropriately applied, IT educators can leverage the increase in regulatory compliance to reinforce basic principles and include information assurance in IT curriculum. IT educators need to use the information systems breakdowns of the recent past as real-world case studies of what can go wrong if we ignore the basic information systems principles.

References

Banham, R. (2004). Sarbanes-Oxley offers one more reason to tackle enterprise risk management. Retrieved November 2, 2004, from http://www.cfo.com/article.cfm/3009436?f=RequiredReading

Beal, B. (2003). Seven steps to Sarbanes-Oxley compliance. Retrieved January 8, 2004, from http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci938537,00.html

Beal, B. (2004). Study: Sarbanes-Oxley 'catalyst' for process management. Retrieved January 8, 2004, from http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci943310,00.html

Burriesci, J. (2004). More pain than bane: Start-ups survive Sarbanes-Oxley strictures. *Intelligent Enterprise, 7* (5), 7-9.

Cantu, I., Gonzalez, D., Leal, H., Koong, K., & Liu, L. (2004). Information certification under the Sarbanes-Oxley act: Implications for computing educators. *Information Systems Education Journal, 2* (14), Retrieved November 2, 2004, from http://isedj.org/2/14/ISEDJ.2(14).Cantu.pdf

Carpenter, T. D., Fennema, M. G., Fretwell, P. Z., & Hillison W. (2004). A changing corporate culture. *Journal of Accountancy, 197* (3), 57-63.

Durak, R. (2004). How companies get into trouble. Retrieved April 13, 2004, from https://www.cpa2biz.com/News/Viewpoint/How+Companies+Get+Into+Trouble.htm

Electronic evidence (2004). Retrieved November 24, 2004, from http://www.sarbanes-oxley.com/displaysection.php?level=2&pub_id=IC-Primer&chap_id=IC2&message_id=199

Gardner, W. D. (2004). Study: Sarbanes-Oxley doesn't worry most IT managers. Retrieved February 25, 2004, from http://www.informationweek.com/story/showArticle.jhtml?articleID=18200214

Goff, J. (2003). Drowning in data. Retrieved November 2, 2004, from http://www.cfo.com/article.cfm/3010723?f=RequiredReading

Goff, J. (2004). Sarboxing. Retrieved November 2, 2004, from http://www.cfo.com/article.cfm/3011495?f=related

Haskin, D. (2004). ISO 17799 for SOX requires security, mindset changes. Retrieved November 3, 2004, from http://www.cioupdate.com/trends/article.php/3316961

Henry, D., & Borrus, A. (2005). No escaping Sarbanes-Oxley. Retrieved January 10, 2005 from http://www.businessweek.com/bwdaily/dnflash/jan2005/nf2005016_5163_db016.htm

Hurley, E. (2003a). Security and Sarbanes-Oxley. Retrieved January 8, 2004, from http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci930493,00.html

Hurley, E. (2003b). A holistic approach to compliance. Retrieved January 8, 2004, from http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci940979,00.html

Katz, D. M. (2003). What you don't know about Sarbanes-Oxley. Retrieved November 1, 2004, from http://www.cfo.com/article.cfm/3008498?f=RequiredReadingFavorites

Katz, D. M. (2004a). Sarbanes-Oxley and Health Plans. Retrieved November 2, 2004, from http://www.cfo.com/article.cfm/3013811?f=RequiredReading

Katz, D. M. (2004b). The reality of real-time reporting. Retrieved November 2, 2004, from http://www.cfo.com/article.cfm/3014387?f=RequiredReading

Kerner, S. M. (2004). SOX deadline arrives. Retrieved November 13, 2004, from http://www.enterprisestorageforum.com/continuity/features/article.php/3435351

Kugel, R. D. (2003). Sarbanes-Oxley: The reporting dimension. Retrieved November 3, 2004, from http://www.intelligentbpm.com/feature/2003/11/0311feat1_1.jhtml?_requestid=490435

Kugel, R. D. (2004). Leveraging IT to enhance financial control – and save money. *Intelligent Enterprise, 7* (5), 23-25, 35.

Kugel, R. D. (2005a). The silver lining in SOX. Retrieved February 2, 2005 from http://www.intelligententerprise.com/showArticle.jhtml?articleID=56200373

Kugel, R. (2005b). Consolidating with compliance. Retrieved February 2, 2005 from http://www.intelligententerprise.com/showArticle.jhtml?articleID=57700807

Leibs, S. (2003). Internal controls: In a world gone Sarbanes-Oxley, have finance and IT found common ground? Retrieved January 1, 2004, from https://www.cpa2biz.com/News/Selected+Features/Internal+Controls.htm

Lunt, P. (2004). Are you too casual about e-mail? Retrieved February 12, 2004, from http://www.transformmag.com/showArticle.jhtml?articleID=17500848

Malwitz, M. (2004). Supporting compliance with BPM. Retrieved November 13, 2004, from http://www.cioupdate.com/trends/article.php/3383101

Marlin, S. (2004). SunTrust Banks may not make Sarbanes-Oxley deadline. Retrieved November 16, 2004, from http://informationweek.com/story/showArticle.jhtml?articleID=52601610

McKie, S. (2004). R U compliant? Retrieved November 29, 2004, from http://www.intelligententerprise.com/showArticle.jhtml?articleID=51201372

Noel, J. (2004). Sarbanes-Oxley as an IT-business alignment driver. Retrieved November 2, 2004, from http://searchcio.techtarget.com/columnItem/0,294698,sid19_gci1009520,00.html

Nyberg, A. (2003). Whistle-blower woes. Retrieved November 2, 2004, from http://www.cfo.com/article.cfm/3010455?f=RequiredReading

O'Brien, J. A. (2004). *Management information systems: Managing information technology in the business enterprise* (6th ed.). New York :McGraw-Hill/Irwin.

Parry, E. (2004). SOX and the SMB: A tale of two auditors. Retrieved November 16, 2004, from http://searchsmallbizit.techtarget.com/qna/0,289202,sid44_gci1025347,00.html

Ramos, M. (2004). Section 404 compliance in the annual report. *Journal of Accountancy, 198* (4), 43-48.

Sarbanes-Oxley Act of 2002 (2004a). Retrieved November 24, 2004, from http://www.sarbanes-oxley.com/section.php?level=1&pub_id=Sarbanes-Oxley

Sarbanes-Oxley Act. (2004b). Retrieved November 16, 2004, from http://www.sarbanes-oxley.com/displaysection.php?level=2&pub_id=Sarbanes-Oxley&chap_id=PCAOB3&message_id=21

Sarbanes-Oxley Act. (2004c). Retrieved November 16, 2004, from http://www.sarbanes-oxley.com/section.php?level=2&pub_id=Sarbanes-Oxley&chap_id=PCAOB4

Satzinger, J. W., Jackson, R. B., & Burd, S. D. ((2004). *Systems analysis and design in a changing world* (3rd ed.), pp. 692-695. Boston: Course Technology.

Schneider, C. (2004). Stuck in the SAS 70s. Retrieved November 2, 2004, from http://www.cfo.com/article.cfm/3011799?f=related

Sorensen, D. (2004). Governance as catalyst: The new management system. *Intelligent Enterprise, 7* (5), 16-20, 35.

Schwartz, J. (2004). An executive perspective on viruses, spam and Sarbanes-Oxley. Retrieved March 17, 2004 from http://www.sun.com/aboutsun/media/features/schwartz-attacks.html

Taub, S. (2004). Internal auditors find control gaps. Retrieved November 2, 2004, from http://www.cfo.com/article.cfm/3014159?f=RequireReading

Telberg, R. (2003). Sarbanes-Oxley adds pressure to go digital. Retrieved December 15, 2003, from http://www.hp.com/sbso/solutions/accounting/expert_insights/cpa_paperless.html

Telberg, R. (2004). SOX whistleblower gets CPA support. Retrieved April 5, 2004, from https://www.cpa2biz.com/News/Telberg/SOX+Whistleblower+Gets+CPA+Support.htm

Telberg, R. (2005). U.K., Europe face twin issues of SOX and IFRS. Retrieved February 7, 2005, from https://www.cpa2biz.com/News/Telberg/UK+Europe+Face+Twin+Issues.htm

Titard, P. L., Braun, R. L., & Meyer, M. J. (2004). Accounting education: Response to corporate scandals. *Journal of Accountancy, 198* (5), 59-65.

Biography

Craig A. VanLengen is an associate professor of computer information systems in the College of Business Administration at Northern Arizona University. He holds degrees with majors in accounting, information sciences, and educational computing and technology. His primary teaching responsibilities are in Web technology and development, systems analysis and design, introductory programming, and introduction to computer information systems. Current research interests are in CIS/MIS curriculum, Web development and use, human computer interaction, and computers and problem-solving.