INFORMATION TECHNOLOGY PROFESSIONALS MEET SARBANES-OXLEY

Gary P. Schneider, University of San Diego

Carol M. Bruton, California State University San Marcos

ABSTRACT

The Sarbanes-Oxley Act of 2002 (SOA) is a law that will affect the lives of top level company officers along with finance and accounting professionals. Top level officers are responsible for the veracity of financial reporting under the SOA. Finance and accounting professionals have traditionally been the corporation's experts regarding financial and operational controls. However, in today's world, information technology (IT) professionals play a key role in designing and maintaining the systems that enforce those controls. This paper examines the challenges that IT professionals will face as they find themselves face-to-face with the provisions of the SOA, a law that could put executives in jail and cause middle managers to lose their jobs.

INTRODUCTION

The Sarbanes-Oxley Act of 2002 (SOA) was passed in the United States (U.S. Code, 2002) in response to a series of significant failures in corporate governance, including Enron (Schwartz, 2001) and the related failure of accounting firm Arthur Andersen (Eichenwald, 2002), HealthSouth (Day, 2003), Tyco (Sorkin, 2002), and WorldCom (Moules & Larsen, 2003). Even Europeans, many of whom were convinced that this rash of management frauds were a result of American's hyper-capitalism mania and could never happen in the refined atmosphere of the continent, found that they were not immune when Parmalat's $15 billion in understated debt and huge overstatements of sales and earnings were exposed.

The SOA imposes a number of reporting and compliance requirements on companies, their managers, and their directors. It also imposes a number of requirements on the systems of internal control used in companies. In this paper, we examine how IT professionals will need to be involved with SOA compliance activities in companies that are subject to the law.

IT REPORTING LEVELS IN THE ORGANIZATION

In many organizations, IT professionals report to a Chief Information Officer (CIO) who reports, in turn, to a Vice President of Finance or Administration. This traditional reporting path places the top IT officer of many companies below the senior decision making level. Companies that do this see IT as a service function and not as a source of competitive advantage (Laudon & Laudon, 2004; Oz, 2004). The senior finance or administration officer often has an accounting background. In many cases, this means that the person to whom the CIO reports knows little about IT issues. An increasing number of companies, including Novell and FedEx, have taken a different tack. These companies have placed responsibility for IT investments and IT strategy in the hands of their boards of directors (Hoffman, 2004). These companies have realized that there is significant legal risk involved if IT projects are not managed properly because inadequate controls can result from IT project failures (Hardesty, 2004). An understanding of internal control demands an understanding of the underlying accounting and administrative systems of the company (Hall, 2004). As every business of any size has computerized its accounting and administrative systems, the people who know these systems well and who understand their design are increasingly members of the ranks of IT professionals. IT professionals, both inside the company and in consulting firms outside the company, can provide valuable services to the company as it attempts to comply with the internal control standards set by the SOA.

DOCUMENTATION OF CONTROLS

The Sarbanes-Oxley compliance deadlines that most large companies will face in 2004 and 2005 for the first time include a major challenge. Section 404 of the SOA requires that companies subject to the law document their internal controls, including internal IT controls. However the SOA is unclear about which controls need to be documented and how the documentation should be accomplished.

The control documentation must include a risk assessment process and must result in the documentation of controls. Company internal IT auditors have been doing this type of work, documenting and testing general and application controls over software, for years (Gelinas & Sutton, 2002; Hall, 2004). Audit firms have begun to explore ways to monitor their clients' IT risk assessment procedures and assess the information systems audit work that is done by clients' internal IT audit staff. Hoffman (2004a) notes that the Public Company Accounting Oversight Board (PCAOB) has not told companies to use any specific method or approach when documenting IT controls. A number of options exist (such as COBIT, COSO or ISO 17799), which makes it difficult for the audit firms to provide advice to their clients about which controls need to be documented (Hoffman, 2004b).

SAS 70 REPORTS

Suppliers of IT services, such as software vendors, system integrators, and system design and implementation consultants, provide their customers with annual reports, called SAS 70 reports (so named after the Statement on Auditing Standards Number 70, which established internal control guidelines many years ago). These SAS 70 reports describe the accounting and operational controls that exist in the systems they sell or have designed and installed. Not all vendors and consultants produce these reports and many SAS 70 reports do not include enough detail to satisfy SOA requirements. In some cases, the SAS 70 reports are sent too late to be included in the annual audit work and financial statement preparation. Some companies who have outsourced their software development work to offshore contractors are now finding that their contractor has no IT testing or revision controls. To the extent that these contractors create financial or key information systems for companies, they could put the outsourcing company at risk with respect to SOA compliance (Hoffman, 2004a).

SPECIFIC IT RISKS UNDER SOA

Although SOA is, at its base, legislation designed to control financial activities, the main way it accomplishes this goal is to require companies to produce better financial reports. Oversight of internal controls has long been seen as a good way to do this (Romney & Steinbart, 2002; Winters, 1994). SOA's focus on internal controls does appear, however, to go beyond the policy reviews, procedures and external financial audits that companies have relied on in the past. The SOA gives the Securities and Exchange Commission (SEC) the responsibility for defining exact compliance regulations for internal control sufficiency, but it is virtually certain that IT controls will be included in the list (Kubilus, 2003). To date, IT professionals have been standing by as CEOs, CFOs, lawyers and company auditors identify and deal with SOA compliance issues. CIOs will soon need to enter the fray and bring IT controls into the picture.

One classic risk area is in the failure to adequately segregate duties. In IT, separation of program development, testing, and implementation can be critical. Many IT organizations are unaware of the importance of segregation of duties as a control concept. Developing a process for identifying segregation of duties controls and evaluating them is something that IT professionals can do as well as internal audit staff. Many times, companies have systems that were constructed internally without adequate controls. When these systems are used for financial information processing, they become potential sources of SOA violations. Even companies that purchase packaged applications can be vulnerable. When the purchased software is modified, built-in controls can be neutralized or eliminated in the customization process. Very few organizations have procedures in place that provide for an automatic review of controls in modified systems.

The costs of failed IT projects are legendary (Wallace & Keil, 2004). A leading cause of IT project failure is poor project management. Thus, project management methods and systems become key elements in a good system of internal control. IT professionals must develop processes that monitor the selection and implementation of systems that affect the financial processing or reporting of the company. If they fail to do so, they subject the company to SOA sanctions.

IT also can be deeply involved in records management (Kubilus, 2003). Whether it is maintaining copies of current e-mail messages and instant messaging files, or retention of backup information regarding old transactions that might have been fraudulent. The IT professional is often in a position to enforce controls that have a bearing on SOA-related concerns. Lanza (2004) notes that two of the most important elements of any SOA compliance program is the proper use of data analysis tools and data mining software. Data analysis functions include the use of query tools that allow users to ask questions of the enterprise-wide information system (Gelinas, 2002). In large organizations such as those subject to SOA, this system will, in most cases, have been designed and implemented by the company's IT staff. It will definitely be maintained by IT staff. The people who know the most about the enterprise-wide information system will always be IT professionals. Many companies have undertaken major knowledge management initiatives in recent years (Angus, 2003; Awad and Ghaziri, 2003). These initiatives have, in most cases, been designed and implemented by IT professionals. As SOA requirements become part of the fabric of large companies, they will be included as part of these companies' knowledge management systems (Lanza, 2004).

AN IT ACTION PLAN

IT industry analysts such as Johnson (2003) recommend a series of steps that IT professionals should include in an SOA compliance action plan. First, they recommend that IT professionals do some research. IT professionals are not accountants and they are not auditors. They do not know about basic control concepts such as segregation of duties. They seldom understand the significant differences between financial systems and other company IT systems.

The second step is to do some benchmarking. Find out what other IT professionals are doing to comply with SOA. In many companies, CIOs are sitting on the sidelines while the accountants and lawyers scramble to meet the challenges of the SOA (Hoffman, 2004b). IT is an integral part of the control landscape in any company. The CIO and senior IT managers must be proactive in pushing the importance of IT processes and the risks inherent in ignoring IT controls.

Step three is to become familiar with software vendor and consultant offerings. Some software vendors are offering upgrades that include documented controls. Some of these products are even keyed to specific SOA elements. Vendors of software reporting tools, supply chain management tools, and document management systems are also working to offer systems that can help with internal control documentation.

Step four is analyze ongoing IT projects for control weaknesses and failure risks. If the software project has any financial implications, the risk of failure of the system implementation effort can be a control weakness in itself, under SOA.

CONCLUSION

IT professionals have been left out of the scramble to comply with SOA provisions. As the deadlines for compliance approach, more and more companies will find that they need to turn to their IT professionals to document controls, and to develop processes that will allow them to identify and evaluate controls. Proactive CIOs and senior IT managers can help their companies by taking the initiative and moving forward with an action plan that will help them be ready when the other members of the management team wake up and realize the important resource they have in the IT function.

REFERENCES

Angus, J. (2003). Rethinking knowledge management. *InfoWorld*, 25(17), March 17, 32-35.

Awad, E. and H. Ghaziri (2003). *Knowledge management*. Upper Saddle River, NJ: Prentice-Hall.

Day, K. (2003). SEC sues HealthSouth, CEO over earnings: Former CEO pleads guilty to fraud, *The Washington Post*, March 20, E1.

Eichenwald, K. (2002). Andersen guilty in effort to block inquiry on Enron, *The New York Times*, June 16, 1.

Gelinas, U. and S. Sutton (2002). *Accounting information systems*, fifth edition. Cincinnati: South-Western..

Hall, J. (2004). *Accounting information systems*, fourth edition. Cincinnati: South-Western.

Hardesty, D. (2004). *Practical guide to corporate governance and accounting: Implementing the requirements of the Sarbanes-Oxley Act*. Boston: Warren, Gorham & Lamont.

Hoffman, T. (2004a). IT Auditors Seek Sarb-Ox Guidance, *Computerworld*, April 12. (http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,92100,00.html)

Hoffman, T. (2004b). IT oversight gets attention at board level, *Computerworld*, May 17. (http://www.computerworld.com/industrytopics/transportation/story/0,10801,93178,00.html)

Johnson, M. (2003). Sarbanes action plan, *Computerworld*, June 2. (http://www.computerworld.com/managementtopics/management/story/0,10801,81667,00.html)

Kubilus, N. 2003. Sarbanes-Oxley: Where IT and finance meet, *Computerworld*, June 30. (http://www.computerworld.com/governmenttopics/government/legislation/story/0,10801,82523,00.html)

Lanza, R. (2004). Making sense of Sarbanes-Oxley tools, *Internal Auditor*, 61(1), February, 45-49.

Laudon, K, and J. Laudon (2004). *Management information systems*, eighth edition. Upper Saddle River, NJ: Prentice-Hall.

Moules, J. and P. Larsen (2003). Reports condemn culture of fraud at WorldCom, *Financial Times*, June 10, 1.

Oz, E. (2004). *Management information systems*, fourth edition. Boston: Course Technology.

Romney, M. and P. Steinbart (2002). *Accounting information systems*, ninth edition. Upper Saddle River, NJ: Prentice-Hall.

Schwartz, N. (2001). Enron fallout: Wide, but not deep, *Fortune*, 144(13), December 24, 71-72.

Sorkin, A. (2002). Tyco figure pays $22.5 million in guilt plea, *The New York Times*, December 18, 1.

United States Code (2002). *Sarbanes-Oxley Act of 2002*, Public Law No. 107-204, codified at 15 U.S.C. §7201

Wallace, L, and M. Keil. (2004). Software project risks and their effect on outcomes, *Communications of the ACM*, 47(4), April, 68-73.

Winters, B. (2004). Choose the right tools for internal control reporting, *Journal of Accountancy*, 197(2), February, 34-40.