https://doi.org/10.48009/2_iis_2006_24-28

THE IMPACT OF THE SARBANES-OXLEY ACT 2002 ON THE INFORMATION SYSTEMS OF PUBLIC COMPANIES

Monica C. Holmes, Central Michigan University, monica.c.holmes@cmich.edu
Darian Neubecker, Plante Moran, darian.neubecker@plantemoran.com

ABSTRACT

The Sarbanes-Oxley Act of 2002 has had a tremendous impact on large and small companies. The Act was intended to hold to accountability those individuals that were running the company. But the impact has trickled down through the accounting organizations and into the information systems that support those accounting activities. Some companies have been able to take advantage of the Act through consulting services, creating new systems that are Sarbanes-Oxley Act compliant or even creating new computer languages to handle the new regulations. For others the impact has been so great that some companies have opted to remove their stock from public trading in order to shield themselves from the high costs resulting from the massive systems changes they were facing. This paper highlights only those sections that impact the information systems of the companies.

Keywords: Sarbanes-Oxley, Auditing, Information Systems Controls

BACKGROUND

The Securities and Exchange Commission (SEC) acts of 1933 and 1934, while regulating public markets, allowed the accounting profession to largely regulate itself through the American Institute of Certified Public Accountants (AICPA) and various other accounting organizations like the Accounting Principals Board (APB), and later, the Financial Accounting Standards Board (FASB). There was a definite void in measures to prevent, detect, and punish fraud committed by corporate executives.

Enron filed for bankruptcy protection in 2001 after admitting overstated earnings by nearly $600 million since 1994. Shortly after, with $107 billion in assets, over $40 billion in debt and hiding $3.9 billion in expenses, the WorldCom bankruptcy filing was the largest in the US [10]. Filings by Adelphia and Tyco soon followed. The common variable was specifically fraud committed by those entrusted with running the company; (i.e., the executives at the very top—CEOs, CFOs, COOs and the like). Executive frauds have been shown to be 28 times more harmful to companies than frauds by those lower in rank [3]. The elevated stock price and other artificially inflated performance metrics also were tied to executive bonus and stock option plans. These compensation plans give executives $millions if their companies perform well. The most appealing aspect of using bonuses and stock options as executive compensation for companies is two-fold: (1) the stock option plans until recently were largely uncharged against earnings—depending on the structure and circumstances, most are still significantly unrealized in current earnings today; and (2) they supposedly align executive interests with those of the shareholder. What has become readily apparent is that this model is severely flawed—executives were motivated to cut corners and commit outright fraud in order to elevate performance metrics by which they were judged and compensated. The Enron and WorldCom bankruptcies caused billions of dollars in losses to pensioners and the loss of thousands of jobs to those both internal and external to the companies filing bankruptcy [3]. The result was the Sarbanes-Oxley Act of 2002, named after the two Congressmen that sponsored the bill.

THE SARBANES OXLEY ACT OF 2002

The Sarbanes-Oxley Act of 2002 (the "Act") requires substantial changes in corporate governance, corporate structure and corporate reporting. There are, also, changes in the regulation of public accounting firms and enforcement. Section 906, adopted by the SEC in June of 2003, also deserves immediate mention since it criminalizes any Section 302 violations. In general, the Act applies to all reporting companies (companies that have registered equity or debt securities under the Securities Act) whether U.S. or foreign. This paper highlights only those sections that impact the information systems of the companies.

Section 101 establishes the creation of a public company accounting oversight board (PCAOB). The board is composed of five full-time members—two CPAs and three non-CPAs. All must be financially literate and prohibited from receiving any compensation by any public accounting firms.

Section 302 requires that each officer is certifying that, to the best of their knowledge, the financial statements and other financial information presented in the report, fairly represent in all material aspects, the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report. The officers certify that they are responsible for the development of, disclosure and internal controls that the financial statements are prepared according to GAAP.

Section 401 covers disclosures of 'off-balance sheet' financing in the Management's Discussion and Analysis section of SEC disclosure documents. These 'off-balance sheet' arrangements were the exact transactions used by Enron. This practice is now illegal. A company must now present a table summarizing certain contractual commitments over time. Investors thus can get an accurate insight over the company's short-term and long-term liquidity and capital resource requirements.

The definition of internal control over financial reporting is: a process designed by, or under the supervision of, the CEO and CFO and implemented by the company's board of directors, management, and other personnel in order to provide reasonable assurance for the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principals [8]. Everything from dual reviews to check signers to passwords to locks on storage facilities can be considered internal controls over financial reporting.

One item to note is that a company must evaluate the effectiveness of both the design *and* operation of the controls. This is one major reason why internal control over financial reporting must be evaluated on an on-going basis (quarterly by regulations). The SEC wanted the report to be tailored to the particular industry or situation a company operates although they do require certain statements pertaining to the internal control over financial reporting.

Section 406 requires the codes of ethics; specifically: (1) honest and ethical conduct; (2) full, fair, accurate, timely, and understandable disclosure in reports and documents issued to the SEC and to the general public; (3) compliance with applicable laws, rules, and regulations; (4) prompt internal reporting to the appropriate person identified in the code of violations of the code; (5) and accountability for adherence to the code [7].

IMPACT OF THE SARBANES-OXLEY ACT ON IT INFRASTRUCTURE

A direct relationship now exists between IT effectiveness and operational effectiveness at large corporations. Transactions from inception to disposition are now in an automated process. The importance of IT management and the role of the CIO are now critical if a company plans on meeting the requirements of the Act.

The CIO and IT management are charged with data analysis and design as well as systems development and maintenance. They must focus a long-term, value-creating IT initiative with an effective ERP system fully integrated with a CRM front-end system and SCM back-end system as the IT infrastructure. Security from hackers and viruses as well as disaster recovery programs is critical along with programs critical to business objectives residing on one platform. Critical financial information must have the ability to be extracted at any time from any place. Defined policies, procedures, and processes must be fully integrated across all entities. Application standards and procedures must be developed in target processes, everyday work, problem resolution, system controls, and risk management at every level throughout the entire organization and related entities [11]. The critical points will be the junctions where information passes from one system to the next and from outside entities (customers and suppliers) to the systems. Effective controls must be in place to ensure that each transaction is authorized and accurate. These controls must be audited continuously and exceptions examined in a timely manner.

The IT costs associated with compliance activities have far outpaced the expenses associated with Y2K. However, CIOs now have the opportunity to create an IT infrastructure that is truly integrated, leading to significant value-creating opportunities in operations, planning, and decision-making. The following paragraphs identify a few systems, technologies, and processes for maintaining an IT infrastructure to comply with the Act.

Project Manager

A project manager with IT expertise and a finance background is necessary to coordinate the compliance activities. This allows for a response that is organized and timely. This manager should have knowledge across many functions to smooth coordination and communication with every business area. Communication skills are critical to this position. A likely schedule of cycle of activities

performed will include (1) defining business strategies and objectives; (2) define business process; (3) organizing people and assignments; (4) devising management reports; (5) developing methodologies; and (6) developing and implementing data systems [11].

Data Storage Systems

The Act requires companies to maintain systems to store and access enormous amounts of data in real-time. The strain of these requirements have proven to be too much for many data storage systems resulting in vast upgrades to these systems by companies who wish to meet and maintain compliance. The scalability of storage systems is a must, especially for entities in high-transaction industries with the automated capture and storage of data. The compliance certification of storage systems is balanced with the difficulty in maintaining data in its original form as it passes through different systems and processes. Communication between IT management and executives will become critical while compliance requirements and reporting requirements will force a tighter integration between mainframes, open systems, and data store entities [11].

IT Solutions

Sarbanes-Oxley Act compliance is serving as a huge business opportunity for many parties. Software vendors are providing fully integrated IT systems that claim to be able to provide compliance. These vendors will also provide consulting services for their IT platforms. New languages are also at the forefront. XBRL appears to be the future business language. IT system design architectures like ITIL and COBiT are now being examined and used extensively by companies seeking compliance.

IT System Outsourcing

Most major software companies and consulting firms are offering their tailored platforms that claim to provide compliance in simple and shortened timeframes. BWise, a European market leader in internal control software and short-listed by the international public accounting firm Ernst & Young, offers its ICSO (Internal Control Sarbanes Oxley) software platform. BWise claims that this platform is fully auditable, web-based with extensive security measures built-in, and can achieve compliance in as little as 3-4 weeks [6]. IBM offers a full and flexible lineup of Sarbanes-Oxley related services ranging from software applications, systems, data libraries, consulting services, and workflows. IBM with KPMG will develop a Lotus Workplace solution specifically designed to handle compliance with the Act. The first in a series of IBM offerings is IBM's Lotus Workplace for Business Controls and Reporting, a web-based, collaborative application designed to allow for automation of significant aspects of business controls framework [12]. HP is offering its own customized consulting services aimed toward compliance. HP offers 'risk-management' consulting that accesses a company's IT controls in relation to the Act's requirements [2]. The Act has created a lucrative market for software and consulting firms.

XBRL

XBRL is a language consisting of XML elements that allows data to be tagged and then manipulated in any possible way imaginable [9]. Businesses will be able to take financial statements and trace the amounts in those statements all the way back to the individual transaction level. On February 14, 2005, the SEC formally announced that it would begin accepting financial reports using XBRL (developed in 1999) [9]. Many experts believe it is only a matter of time before XBRL is required for all reports submitted to the SEC.

COBiT

The COBiT framework was designed by the Information Systems Audit and Control Association in conjunction with the IT Governance Institute. This framework, which follows COSO closely, provides a set of high-level control objectives for IT processes grouped into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring [14]. COBiT provides management guidelines giving managerial advice on best practices when managing information systems, achieving organizational objectives, and monitoring IT operations.

ITIL (Information Technology Infrastructure Library)

ITIL is a customized framework of best practices that promotes quality computing services in the IT sector [5]. Specifically, ITIL addresses the organizational structure and employee skill requirements for an organization's IT function through a comprehensive set of managerial procedures for a company wishing to develop and maintain an effective IT system. ITIL has been commonly known as the world standard in IT service management [5]. For example, service

delivery refers to the services that the data center must provide to the business to adequately support it (i.e., IT Financial Management, Capacity Management, Availability Management, IT Continuity Management, and Service-level Management).

COSTS AND BENEFITS OF COMPLIANCE

Some studies show that the costs for compliance have been too high for smaller public companies to handle and drastic measures are resulting. The first study, with 147 responses from high-level executives, was a multi-tiered review of the costs of compliance and executive opinions on issues concerning the Act [4]. The study shows that the average audit fees have increased by a range of 55% for S&P 500 companies to 84% for S&P Small-Cap companies. The subject of IT controls was a top issue among the respondents. They felt that IT controls will need to be built into business process similar to the way engineers build tolerance into stamping machines [8]. The challenge is developing an auditing/accounting system that will have the ability to detect when IT controls are not operating as designed and signal evaluation activities and monitor corrections [8]. Another common thought regarding IT controls was the need for more IT auditors. The five most mentioned needed enhancements to IT controls were (1) improved information system security; (2) better understanding and improvement of segregation of duties; (3) improved access controls and access monitoring; (4) improved testing procedures and program change management; and (5) improvement processes to document policies, procedures, and controls [8].

RISE OF PUBLIC COMPANIES "GOING DARK"

"Going dark" is a term referring to public companies that remain corporations but delist from stock exchanges and cease their SEC filings. This is both a legal and viable option for small public companies as long as they have fewer than 300 to 500 listed shareholders (often times corporations have many more shareholders that are not on the records). Between 1999 and 2003 the number of public companies "going dark" increased from 30 in 1999 to over 200 in 2003 [8].

Companies like Bluefly, an online discount retailer based in New York with 75 employees and annual revenues of roughly $44 million, faced audit costs that could quadruple (audit fees before compliance totaled $150,000) [10]. Studies have shown that compliance costs are 11 times more burdensome for public companies with annual revenues under $100 million compared with public companies making over $2 billion annually [10].

The advantages of going dark over becoming a private company are numerous: cheaper, easier, and approval from shareholders is not needed. In addition, these companies can cease their SEC filings and do not have to deal with nearly as many formerly mandated shareholder responsibilities. However, these firms often see the value of their shares drop (their shares can only be traded through far less active channels like trading on Pick Sheets), they cannot get additional capital funding, and face increased costs for funding (higher interest rates on debt). One result from "going dark" is the possibility of the company's stock rising to a level higher than ever before as Sport Supply Group experienced.

CONCLUSION

The Act is, without question, a significant set of laws affecting public companies, probably the most significant piece of legislation concerning market regulation since the Exchange Acts of 1933 and 1934. The regulations are both vast and complex. The costs are significant, as are the potential benefits if the compliance activities are oriented towards achieving efficiencies and not just meeting and maintaining compliance. The effects of this piece of legislation will be long-lasting. We have only cracked the surface concerning the impact on the marketplace this legislation will have. The only certainties concerning the Act is that it was dictated by market activities prior to its enactment, it is not going away, and its impact on businesses and the marketplace is only beginning to be understood.

REFERENCES

1. COBiT: Executive Summary. *Information Systems Audit and Control Association.* August 2005. http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/COBIT_Publications/COBIT_Components.htm
2. Frauenheim, E. (June 9, 2005. August 2005). Relief from Sarbanes-Oxley on the way? *CNet News.* http://news.com.com/Tangled+up+in+SOX--relief+from+Sarbanes-Oxley/2100-1014_3-5737846.html
3. Green, S. (2004). *Manager's Guide to the Sarbanes Oxley Act : Improving Internal Controls to Prevent Fraud.* New Jersey: John Wiley & Sons, Inc.

4. Hartman, T. E. (June 2005). The Cost of Being Public in the Era of Sarbanes-Oxley. Foley & *Lardner, LLP*. Accessed August 2005. http://www.foley.com/files/tbl_s31Publications/FileUpload137/2777/2005%20Cost%20of%20Being%20Public%20Final.pdf#search='The%20costs%20of%20being%20public%20in%20the%20era%20of%20Sarbanes%20Oxley'.htm
5. Information Technology Infrastructure Library. *Wikipedia.* Accessed August 2005. http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library.htm
6. Internal Control Sarbanes Oxley. *Scandent Solutions*. Accessed September 2005. http://www.scandentsolutions.com/03_InternalControl_Services.htm
7. Lander, G. (2004) *What is Sarbanes-Oxley*. New York: McGraw-Hill.
8. Miller, P. K. & Rittenberg, L. E. (January 2005). Sarbanes-Oxley Section 404 Work: Looking at the Benefits. *The Institute of Internal Auditors*. Accessed August 2005. http://www.theiia.org/?doc_id=5161
9. Extensible Business Reporting Language (XBRL). *Cover Pages*. (August 31, 2005). Ed. R. Cover. Accessed September 2005. http://xml.coverpages.org/xbrl.html
10. Rosen, E. (June 20, 2005). Smaller Firms Foresee Huge Audit Costs. *The New York Times*. Accessed August 2005. http://www.indystar.com/apps/pbcs.dll/article?AID=/20050620/BUSINESS/506200318/1003
11. Sarbanes Oxley Group.(2004). *The Sarbanes Oxley Guide for Finance and Information Technology Professionals.* Ed. S. Anand. Booksurge/CLA.
12. Sarbanes Oxley Solutions. *IBM*. Accessed September 2005. http://www-1.ibm.com/service/us/index.wss/offering/bcs/a1002618
13. SEC Release No. 33-8545. (October 2005). *Securities and Exchange Commission*. Accessed October 2005. http://www.sec.gov/rules/final/33-8545.htm
14. Waschke, M. (August 2005). Changing the DNA of IT: Sarbanes-Oxley and Service Management. *ComputerWorld.* Accessed August 2005. http://www.computerworld.com/printthis/2005/0,4814,101050,00.html