Sarbanes-Oxley and IT Control

Robert Freeman
BADM 559

Introduction
The issue of IT control, although prevalent for the past several years, has not always been a major concern for many businesses and industries across the United States. The reason for this is due in part to the ever-increasing reliance of businesses upon information technology to provide easier access and control of critical company data/information. As electronic data becomes more mainstreamed throughout the globe, this information also becomes easier to access, as well as manipulate. Consequently, it is not only essential, but required by law for public companies to demonstrate an effective and cohesive plan for utilizing internal IT controls. The Public Company Accounting Oversight Board (PCAOB), created by the Sarbanes-Oxley Act (2002), helps clarify the importance for companies to not only demonstrate effective internal controls over accounting methods, but over IT processes as well, as outlined by the PCAOB’s Auditing Standard No. 2, which states that, “The nature and characteristics of a company’s use of information technology in its information system affect the company’s internal control over financial reporting.”¹

The Sarbanes-Oxley Act, passed by the United States Congress in the wake of major accounting scandals on Wall Street, was designed to address and correct many of the perceived problems that existed with previous legislation concerning the regulation of internal controls for public companies. The issue really at stake, however, is not just internal controls of IT, but trust. Information technology, through technological innovations such as the Internet, has allowed companies to expedite financial information across the world to both investors, stakeholders, and

other users. However, without proper controls regulating the internal use of the financial information that users will eventually see (and rely upon for financial decisions), the trust between stakeholders and a business could be broken. It is crucial that in order for a market to function properly, differing parties must be able to work with one another and be able to use relevant and reliable information. IT now, and in the future, will continue to play a crucial role in easing or hindering these important market interactions.

The purpose of this paper is to analyze the background and subsequent reaction to legislation such as Sarbanes-Oxley, and examine the impact that this legislation has had upon the world of IT controls, with an additional accounting perspective. How have companies responded to these changes since 2002, and what have been the impacts of the mandates for increased IT control? Can businesses find value beyond compliance with the law, and realize further benefits from greater IT control? By having an understanding of the laws that have driven companies to their current point, users will be better able to determine whether Sarbanes-Oxley, and the methods and controls that have followed, have been of benefit or hindrance to American businesses. Additionally, it is crucial to examine whether these new regulations have created greater trust and confidence between investors and corporations in the marketplace.

The Origins of Sarbanes-Oxley and IT Auditing

The Sarbanes-Oxley Act, passed in July of 2002, was defined as the most important legislation approved by Congress to change the market since the Security and Exchange Acts of 1933 and 1934 (where greater regulations and accounting standards were placed upon public businesses). The passage of the Act stems from the accounting scandals that broke headlines in both 2001 and 2002. These well-known scandals, coming from such previously respected companies such as Enron, WorldCom, Tycho International, and several other major businesses, had not only the
consequence of bankrupting the organizations, and bringing down major accounting firm Arthur Anderson, but also severely disrupting investor trust and confidence in the financial market. How were investors to know, based upon the annual and quarterly financial statements produced by companies such as WorldCom, that a serious fraud was taking place? To renew confidence, what investors needed was an improved commitment towards accountability, which the U.S. government believed could only come through new regulation.

From an accounting perspective, not only did Sarbanes-Oxley create a new regulatory committee, (the PCAOB) capable of passing new auditing standards and mandates, but the Act has further tried to modify corporate behavior, by holding executives personally responsible for signing off their company’s financial statements, and carrying out their company’s codes of ethics and conduct. Most importantly, the Act has largely taken the concept of self-regulation and control out of the hands of the private sector, and into the control of the government. However, despite Sarbanes-Oxley’s attempt to further alter corporate codes of conducts, the reality is that a company and its executives are only as good as they allow themselves to be, and having a code of ethics will not change those circumstances. Before the passage of the Act, 90% of the Fortune 500 American businesses already had in place a code of ethics, or codes of corporate governance. Additionally, Enron’s code of ethics had, before 2001, been lauded by analysts as one of the most sound and responsible codes amongst the company’s competitors. During the investigation into the reasons behind Enron’s collapse, one of the principal conclusions made by the Special Committee was that, “There was an absence of forceful and effective oversight by Senior Enron Management and in-house counsel, and an absence of

---

2 http://www.sarbanes-oxley.cc/the-history-of-the-act.html
objective and critical professional advice by outside counsel or auditors,”
Act looked to correct this mistake, by forcing top-level executives to disclose pertinent
information surrounding the creation and execution of a company’s codes of conduct, allowing
stakeholders to better determine the validity and honesty in the internal governance of their
invested companies.

The increased regulation of behavior and controls over executives and
accounting/auditing procedures is important within the context of this analysis, as these changes
also reflect the attitudes that needed to change within the IT world as well. IT auditing and
control issues have their history dating as far back as 1973, during the Equity Funding
Corporation of America scandal. From 1964 until 1973, this mutual funds and life insurance
firm engaged in fraudulent practices, utilizing a computer-based system that created and
maintained fictitious insurance policies, consequently inflating the firm’s value to investors. At
one point during the fraud, over 80 employees were involved in the scandal; subsequent
investigations and court rulings revealed that computer technology, left in the hands of only a
few individuals without oversight and control, could be easily used to manipulate earnings and
hide illegal activities. Another important event in the history of IT controls, before the advent of
Sarbanes-Oxley, was the 1998 AT&T computer collapse, when a software failure forced a global
communications blackout for AT&T users, preventing them from using credit cards or accessing
bank funds for a period of time. Beyond confirming the reliance of users upon IT-based systems
for daily activities, the crisis also introduced the need for greater oversight when designing and

4 http://www.jstor.org.proxy.lib.muohio.edu/stable/1342755?seq=8&Search=yes&term=sarbanes-
oxley&list=hide&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Dsarbanes-
oxley%2BAND%2BInformation%2BTechnology%2BControl%26Search%3DSearch%26hp%3D25%26wc%3Don&item=2&ttl=87&returnArticleService=showArticle&resultsServiceName=doBasicResultsFromArticle
implementing systems, as well as the necessity of creating back-up IT systems in times of emergency, or during events involving critical loss of data.

To serve as a parallel to the IT-based crises that have occurred in the past several decades before the passage of Sarbanes-Oxley, published forms of IT control have been recognized as important first steps in the evolution of IT governance. Beginning in 1968, the American Institute of Certified Public Accountants (AICPA) required the larger accounting firms to actively engage in new forms of Electronic Data Processing (early forms of IT) auditing and control development, ultimately documenting more formalized methods of control and review. By 1977, a new version of documented IT controls was released from the Electronic Data Processing Auditors Association (EDPAA); this initial version was called Control Objectives, but later became known as Control Objectives for Information and Related Technology (CobiT), with the purpose of creating a set of generally accepted set of accounting IT objectives for auditors. There have been over four versions of CobiT released, with the latest, 4.1, released in May of 2007. Sarbanes-Oxley has encouraged companies to adopt either CobiT, or a companion form of IT control procedures known as COSO. An additional IT control guide, released by the IT Governance Institute in 2006 after Sarbanes-Oxley, directly address issues raised by the legislation, and offers insightful requirements for change and improvement. For the purposes of this paper, the IT Governance Institute document, which has not been officially endorsed by the SEC or PCAOB, will be used as an alternative document apart from CobiT and COSO, and act as a guide towards better understanding the importance and use of IT controls within a business.

Examining IT Governance Controls

The IT Governance Institute document serves as an important guideline and form of documentation against lack of formal IT controls, and thus, should be analyzed in order to

---

5 http://ilurbana.library.ingentaconnect.com/content/bpl/abac/2005/00000041/00000001/art00003?crawler=true
determine what kinds of controls businesses should be placing within IT departments. What is important to recognize is that most companies already have some form of IT control in place, and have the needed staff to implement new policies and changes. However, what many of these businesses are lacking is more formal sets of control procedures, as well as adequate employee IT control training. The skills and basic structure are there, but the execution of needed critical elements is missing. Consequently, because of the importance of personal responsibility that Sarbanes-Oxley has placed upon executives in every department of a business, including IT, all companies must take steps to move current IT controls into compliance with Sarbanes-Oxley standards; for some companies, the time and modifications required to make this change will be dependent upon where the company’s IT controls currently stand\(^6\).

Regardless of how much progress in IT control a company has made, there are several objectives that must be reached in order for an organization to be in compliance with Sarbanes-Oxley. These objectives include: Understanding the organization’s internal control program and its financial reporting process, identifying risks related to these IT systems, designing and implementing controls designed to mitigate the identified risks and monitoring them for continued effectiveness, and monitoring IT controls for effective operation over time. Further, it is also important for a company to formally document these risks and controls, and add to that documentation as updates or new policies are implemented over time. In particular, an effective IT governance policy must have satisfactory IT controls controlling computer programs, access to data and information, and changes in programs, including, for example, accounting software packages such as Microsoft’s Great Plains. Further, having a properly functioning control environment (a process that monitors and reports on IT governance activities and progress) is

\(^6\)http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=12383
also needed, and if found to be inadequate, may contribute to having a material weakness appear in an auditor’s report to the public. Additionally, an effective IT control environment will not only help a company meet regulatory compliance standards, but it may help bring further value to the company in the future, in the form of increased returns on investments, and better alignment of IT goals with the objectives of the general business.

Two of the most important IT controls that must be used during the control process include entity-level controls, and activity-level controls. The purpose of the entity-level control is to better understand how a company operates, and the culture that it has adopted. Consequently, an entity-level control may not test specific software or IT applications, but instead entire subsystems or processes. Entity-level assessments should help enable an effective dialogue between the differing design elements in the process, and inquiries should be more advanced than simple, “yes” or “no” answers. Such questions may first be structured towards understanding the strategic, “tone-at-the-top” management style, and should then move down towards how the style may impact the IT organization, the relationships, and management of human resources. In contrast, the activity-level control is much more specific, in that it tests the effectiveness and reliability of application systems that specialize in data processing, and collecting and compiling information that will ultimately be used by management and external stakeholders. These may include activities pertaining to the general ledger, recording journal entries, and other critical accounting procedures. Tests should subsequently determine whether these systems are flexible to changes without being vulnerable to fraud, as well as reliable in their execution.

Following IT control procedures will often depend upon the company itself, and the unique characteristics present within its IT architecture. Nevertheless, each company may be
able to adhere to the basic outline constructed by the Sarbanes-Oxley IT Compliance Road Map (Please See Exhibit 1). Starting with planning the scale and scope of an IT control project, and moving towards assessing IT risk and building sustainability are all important steps within the Road Map. When first constructing an IT control program, it is first essential to construct areas of accountability and responsibility, called an IT control sub-committee. The role of this sub-committee should be to monitor progress with regards to Sarbanes-Oxley compliance, as well as help facilitate and guide external auditors through the new IT controls. This sub-committee would directly report to the Compliance Steering Committee, which would in turn direct the overall process. Regarding issues of responsibility, for each level of controls over both IT applications and processes, documentation must clearly state who is in charge of the application, how that responsibility is delegated, and what risks are present in the system. Without having in place several layers of accountability over critical systems, an IT process leaves itself vulnerable to manipulation.

For addressing the issue of IT risk in the road map, an organization must first examine and document any inherent risk present within the system. What this means is that without controls, there are dangers within a system’s fundamental design and procedure that may leave a company vulnerable. Lacking certain necessary features such as access controls into sensitive database files is an inherent risk. To assess the severity of the risk, a company should first understand the probability and impact of the risk. The higher the probability and impact, the more important it will be for a company to focus control efforts on containing that problem. Other factors used to determine the extent of a risk include the complexity of the technology, the experience of the people handling the control process, whether the process is centralized or distributed, and whether the risk would have a material impact upon the financial statements.
Upon the completion of the risk assessment, a company should be able to increase or decrease the scope of the project, as well as eliminate certain IT applications in order to help streamline the IT control process. Documenting control procedures and methods should then follow from this phase.

Evaluating and updating the process controls present in the IT control system are two important initial steps leading up to the final point in the Road Map; building sustainability. These evaluations look at both detective and preventive IT controls, and report on their capabilities. Having managed and measured awareness and documentation of a system’s IT controls, as well as having a measurable, if not optimized IT control effectiveness, is essential for success. Signs of deficiency include ad hoc to non-existent awareness and efficiency of IT controls, which would indicate a serious lack of understanding by management and employees over differing areas of responsibility. Testing must be carried out on these systems to make a proper determination of understanding, including inspection of documentation, inquiries into procedures, observation and re-performance of the IT control process. Sample-size and timing should also be taken into consideration. Upon completion of these tasks, a company may now head towards sustainability, turning IT controls into a fundamental and permanent process of the company. This process should involve evaluation and reviews of progress made, and suggestions for what could be done in the future to move IT controls out of simple compliance, and into the area of value creation for the company. Control rationalization, or the elimination of unnecessary or redundant controls, should also be reviewed and implemented.

As Sarbanes-Oxley changes and regulations surrounding it alter over time, a company must remain aware of any new legal requirements, and make appropriate alterations as necessary. Over the long-term, the automation of processes, and further installation of program change
control software (making it easier for new IT controls to be removed or added) should be the continued goal of the IT process.

Although the human factor is often overlooked during the IT control process, it is also one of the most important components for success. Complying with Sarbanes-Oxley is not just about assessing risk and changing control procedures; changing methods is also about working with and challenging corporate cultural assumptions and attitudes. Building up a vision, and pushing top-level management on a path towards commitment to change and improvement is needed before any IT control project can begin. In a corporate culture that already has a pre-disposition towards flexibility and innovation among employees, this change will come more easily than with a corporate culture that is much more rigid in its management-style. A company must first understand the impact that the change will have upon employees, and instead of forcing a new control program upon the employees, management must work to turn their staff into “agents of change”. Communication, training, and motivation are three key tenants that must be used in order to push past cultural obstacles, better understand the “pain points” among employees, and build a dialogue towards sustainable development. When this occurs, the process of following the IT Road Map becomes much simpler and less time-consuming.

Creating Value

After examining some of the documentation and IT controls that has arisen since the passage of the Sarbanes-Oxley Act, it is important to examine the impact of this change. As mentioned throughout this paper, many companies look towards Sarbanes-Oxley for not only guidance in areas of compliance, but also to enhance value within the company, and re-foster trust between management and stakeholders. Has Sarbanes-Oxley succeeded in this fundamental goal? Reaction since 2002 has been mixed, and the benefits and consequences stemming from the Act
vary. From an expense-based perspective, complying with Sarbanes-Oxley has been very costly for many businesses. Pre-Sarbanes, the cost of running a public business making revenue of under $1 billion was on average $1.25 billion. After Sarbanes, however, the cost has moved to $2.86 billion, representing an increase of 130%.\(^7\) According to Michael Hughes, one of KPMG’s leading partners, “Costs [from Sarbanes-Oxley] were often driven by the steep learning curve, condensed timeline, additional regulatory guidance issued late in the year, the extent of deferred maintenance of controls and related processes, along with the inability to fully achieve an integrated audit and efficiently use the work of others.”\(^8\) This cost has become a roadblock for many companies on the way towards compliance.

Other experts have argued that given the same processes that are in place today over IT controls, not all frauds that perpetuated the creation of the Sarbanes-Oxley Act could have been prevented. For example, although current IT controls would have been able to detect bank frauds such as the Allied Irish Bank/Allfirst fraud case in 2002, where employees were using computer-systems to conceal mass amounts of data, insider frauds such as the cases of Enron and WorldCom would probably still have happened. The remedy to this, as noted by the previous section outlining IT governance, lies not within the changing of IT processes, but instead within a change of corporate culture and attitude.\(^9\) Another critique against Sarbanes-Oxley is that the requirements for controls and change have become too stringent, making it very difficult for companies to catch up and comply. In January of 2007, a survey of more than 200 IT managers, taken by the Oracle Applications Users Group, indicated that 61% of companies had self-reported that they had not yet met Sarbanes-Oxley requirements, and that out of the companies that had complied, 64% of those organizations had found subsequent flaws and deficiencies.

---

\(^7\) [http://knowledge.emory.edu/article.cfm?articleid=882](http://knowledge.emory.edu/article.cfm?articleid=882)  
\(^8\) [http://knowledge.emory.edu/article.cfm?articleid=882](http://knowledge.emory.edu/article.cfm?articleid=882)  
\(^9\) [http://www.securityfocus.com/columnists/322](http://www.securityfocus.com/columnists/322)
within their controls\textsuperscript{10}. An overriding concern is that compliance with Sarbanes-Oxley is forcing many smaller, entrepreneurial companies to close their doors before they can even get off the ground (cost of compliance can cost $500,000 per year, regardless of employee size), consequently destroying innovative technologies and business practices within the United States.

It is the reduction of innovation in the face of expensive compliance regulations that have convinced many other organizations within America that they must convert expenses into more positive valuations of their business. One benefit of increased IT controls is that Sarbanes compliance has forced many executives and managers to rethink how IT controls fit within a business and for what purpose those controls can be utilized for. A new, risk-based perspective has been developed that challenges older processes, and ferments new knowledge, as well as further develops new techniques for lessening risk and increasing control. Both the quantity and quality of information reported to investors on the financial statements have been improved, giving stakeholders greater insight into how well their company is performing. Further, comparability between financial statements have increased, and companies that only comply with regulations, rather than taking the extra step of giving investors more value, may be undercut by superior financial statements produced by competitors.

Additionally, other publications such as the CPA Journal, have recommended that businesses use Sarbanes-Oxley to push another step further in creating value, by investing in programs such as Enterprise Risk-Management (ERM), and aggressively tackling ethical and human cultural corporate attitudes\textsuperscript{11}. Methods for being able to stop managers and employees from rationalizing fraudulent behavior in the face of uncertain regulatory and ethical decisions must be strengthened throughout a company. Defining and maintaining core values, both

\textsuperscript{10} http://www.itconsulting.com/news/sarbanes-oxley-oaug-jim-clark-011807/
\textsuperscript{11} http://www.nysscpa.org/cpajournal/2004/604/perspectives/p11.htm
personally, and professionally, is critical to success. Finally, a company must not become bogged down in compliance regulations, and must make fundamental structural changes to its governance process in order to seek further value from greater IT controls. Using documentation of controls as a tool for improvement, rather than a club for punishment, will help make actual improvements in the system easier, and less expensive in the long-term. An effective ERM system would be very helpful for a company, as an ERM would tackle risks on a comprehensive basis across the system, from IT risks to legal risks, and ties those risks into the overall goal of strategic management, ensuring that every department, most especially IT, was aligned with the strategy, operations, reporting, and compliance of the entire organization. In this way, Sarbanes-Oxley can become a benefit, not a hindrance, towards greater company returns.

**Assessing Trust**

As IT controls have become an essential component in producing and managing a corporation’s financial statements, the ability of Sarbanes-Oxley to restore public trust in the market through the strengthening of these controls is critical towards evaluating the overall success of the Act. One of the initial concerns after the passage of the Act was that instead of trying to build up confidence, companies would instead have a “race to the bottom”, where companies would look to take advantage of lack of consumer trust. However, the opposite has proven true, as companies such as General Electric have spent over $35 million world-wide to ensure compliance with Sarbanes-Oxley. At a U.S. Chamber of Congress panel in August, 2008, addressing the importance of trust in the business world, and how Sarbanes-Oxley has impacted it, Timothy Munoz, senior vice president of brokerage house Legg Mason stated, “Trust equals a personal sense of engagement. Companies do a poor job of showing what value they

---

create. Trust takes time. Companies have to do a consistent, ongoing job over time. Trust takes work and requires personal relevance."\textsuperscript{14} Consequently, in order to continue to re-establish trust and confidence in the marketplace, companies must find value out of Sarbanes-Oxley, and not just move through the motions of compliance. Complementing this statement, another study has found that increased expenditures on controls do not necessarily automatically increase investor confidence in a company\textsuperscript{15}. Alternatively, investors want to see larger returns, regardless of whether the governance process that created those returns is a compliant or not. While this finding does cast doubt on the ability for Sarbanes-Oxley alone to change the outcome of confidence in the markets, the act of improving quality control, and improving value returns beyond compliance may go a long ways towards increasing returns, as well as confidence. Trust will continue to be an important issue in the development of internal controls within a company, and in changing the cultural attitudes of a company’s management and employees.

Conclusion

Sarbanes-Oxley has done much to impact the changes that the IT world has seen when it comes to personal responsibility and management over IT controls in the business. Information technology is continuing to become an essential element of communication and control over the most sensitive areas of corporate governance, thus making it crucial for continual updates and testing on IT controls used today. Are IT controls perfect? The answer is no, as they cannot alone prevent the occurrence of fraud within a company. Further, Sarbanes-Oxley alone cannot force change within a company, as we have seen that compliance with the law is not enough to restore public trust and confidence in the system. IT control is not just about technological changes, but is more fundamentally about the people who use, manage, and document IT.

\textsuperscript{14} http://www.ethics.org/ethics-today/0808/us-chamber.asp
\textsuperscript{15} http://news-info.wustl.edu/tips/page/normal/6708.html
Change needs to begin in this area, with the improvement among both employees over management of innovation, flexibility, and use of IT technology. This change must not occur simply within the IT department, and as shown in the IT governance process, must begin from a top-down level, facilitated by executives from each different segment of the business. IT control is not just an IT issue, but a corporate issue as well. Sarbanes-Oxley has been the first stage of change, but it will not necessarily drive American businesses towards less risk and greater success into the future. This improved value must come from within the company, challenging both attitudes, controls, and consequently, external stakeholders as well.
Exhibit 1

Source: http://www.inforica.com/consult-compliance.html
Works Cited
