Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

The Impact of the Sarbanes-Oxley Act on IT Project Management: A Case Study

Michael Leih
Claremont Graduate University, michael.leih@cgu.edu

The Impact of the Sarbanes-Oxley Act on IT Project Management A Case Study (Research in Progress)

Michael Leih
Claremont Graduate University
michael.leih@cgu.edu

ABSTRACT

In 2002, the Sarbanes-Oxley Act was passed into law requiring all U.S. based, publicly traded companies to report on the status of their internal controls governing the reporting of financial information. Because of the close relationship between financial reporting and IT, the requirements of the Sarbanes-Oxley (SOX) Act has also greatly impacted IT Governance and the way IT projects are managed. This study is investigating the impact of SOX on IT Project Management within a large corporation. The study is evaluating three areas of impact: 1) The introduction and formalization of internal controls as defined by the COBIT framework, 2) The positive and negative effects on IT project implementation, and 3) The additional costs to an IT project to maintain compliance to the SOX requirement. In addition, the study also considers if the introduction of internal controls has impacted the organization's development maturity when evaluated against standard maturity models.

Keywords Project Management, Sarbanes-Oxley Act, COBIT, Internal Controls, System Development Lifecycle, Maturity Model

INTRODUCTION

The Sarbanes-Oxley (SOX) Act of 2002 was enacted in response to a number of major corporate accounting scandals that rocked the American business landscape. This act dramatically heightened the standards for financial reporting for US public companies with market capitalization over $75 million (Dietrich 2004). Because of the tight integration between financial reporting and IT, Sarbanes-Oxley also requires significantly greater levels of auditing on process control within IT governance (Damianides 2005). The act requires auditors to publicly report on corporate control processes pertaining to financial reporting and to show shareholders exactly what control processes are in place and to what extent they are being followed.

The ultimate impact of Sarbanes-Oxley on corporate governance will likely not be fully known until the new auditing processes have been in effect for more than a year, sometime in late 2005. This will provide organizations the ability to assess how auditors reviewed their new process controls and how audits from other public companies reported on their internal controls. This study will review the current literature on the possible impact of Sarbanes-Oxley on IT project management as well as report on how this new act is impacting IT project management at a specific public corporation. It will review how the IT governance standards, COBIT (Control Objectives for Information and Related Technology) is being used to satisfy control standards to meet SOX requirements and how these new processes are impacting an IT organization's maturity rating.

BACKGROUND

The 66-page act is arguably the most sweeping and important collection of federal securities laws since the passing of the Securities Exchange Act in 1934 (Burrowes, Kastantin and Novicevic 2004). In short, the legislation centers on ensuring the accuracy, consistency, transparency, and timeliness of financial results and reports. To do this, SOX mandates that control processes are put into place over financial reporting procedures and that the CEO and CFO must attest to the accuracy of financial statements.

The Sarbanes-Oxley Act

SOX mandates significant penalties if company officers purposefully or by neglect, report fraudulent information, but with all its sweeping changes (U.S. Congress 2002), much of the details on how to comply with the act were left up to the Securities and Exchange Commission. Together with the Public Company Accounting Oversight Board (PCAOB), the SEC has slowly defined its opinion on how public companies should comply with Sarbanes-Oxley.

Section 302 of the act, Corporate Responsibility for Financial Reports, mandates that CEO's and CFO's attest to the accuracy of their company's quarterly and annual reports (Dietrich 2004). They must attest that they have viewed the report, that the report contains no untrue statements, that the financial information fairly represents the company's financial position, and that control procedures have been put into place and are working to insure the accuracy of financial information. Section 404 of the act, Management Assessment of Internal Controls, mandates that each annual report issued by a company under the Exchange Act is to contain an internal control report. This report must state management's assessment of internal controls over financial reporting, identifies the internal control framework used, and that the auditors attest to the effectiveness of internal controls (U.S. Congress 2002).

The added challenge of section 404 is the auditor's attestation report. Not only must organizations ensure that appropriate controls are in place, they must also provide their independent auditors with documentation supporting management's assessment of internal controls, including IT controls. This means that auditors will be reviewing IT project documentation to ensure that all control processes established by the orginziation are being followed (IT Governance Institute 2004).

COSO

COSO (The Committee of Sponsoring Organizations of the Treadway Commission) is a voluntary, private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal control and corporate governance (IT Governance Institute 2004). Although Sarbanes-Oxley or the SEC mandates the COSO framework, the SEC's June 2003 announcement recognized COSO as the preferred framework for Sarbanes-Oxley compliance (Securities and Exchange Commission 2003). The COSO framework components establish the overall guidelines for corporate governance to ensure reliable and complete financial reporting, but it does not provide the actual processes that IT organizations can use to establish effective internal controls in preparation for IT audits (Dietrich 2004). An IT internal control framework must be used to create an environment that is prepared for the audits now mandated by Sarbanes-Oxley. Several IT internal control frameworks exist (Paulk 2004), but the IT control objective known as COBIT is considered particularly useful and aligns with the spirit of the Sarbanes-Oxley requirements (IT Governance Institute 2004).

COBIT

COBIT establishes IT governance as a structure of relationships and processes to control the IT origination in order to achieve the business objectives of the corporation. COBIT provides the structure that links IT processes, IT resources, and information to enterprise strategies and objectives. The COBIT framework identifies 34 control objectives, which have been classified into four domains. The four domains are 1) Planning and Organization, 2) Acquisition and Implementation, 3) Delivery and Support, and 4) Monitoring (IT Governance Institute 2000). Each control objective in the COBIT framework can be regarded as a separate process that can be established to create the overall IT governance within the corporation. The management guidelines given by COBIT are governed by a generic maturity model that allows managers to map where the organization is today and where it stands in relation to the best-in-class in its industry.

Maturity Models

As IT controls are established, the ability to develop measures of these processes are important in tracking their effectiveness. Key to this measurement is the use of maturity models for self-assessment and benchmarking. One example would be Carnegie Mellon's Capability Maturity Model Integration, which defines five levels of maturity, starting with level 1, initial, and ending with level 5, optimizing (Carnegie Mellon Software Engineering Institute 2001). Given Sarbanes-Oxley requirements for independent attestation of controls by external audit, controls will more than likely require the attributes and characteristics of level 3 or higher for key control activities (IT Governance Institute 2004).

CASE OVERVIEW AND METHODOLOGY

This study is being conducted at the IT department of a publicly traded retailer over a period of 26 months. The company has retail locations located throughout the United States and is currently exceeding $1 billion in annual sales. The IT department uses an in-house project management methodology to manage over 100 projects per year. Most projects last between two and 12 weeks, but a few projects will last up to nine months.

The study was initiated in November 2003, at the beginning of the company's SOX compliance process. At that time, the research began by evaluating the company's internal control documentation relating to IT project management and the IT department's System Development Life Cycle (SDLC). In addition, an interview with the company's newly appointed manager of internal audit was conducted to evaluate what control points, if any, were lacking in the IT project management process. The current state of IT project management was noted, along with what changes were going to be made to meet SOX compliance. The second evaluation was conducted in January 2005, towards the completion of the company's first annual audit under the new regulations. At that point, the company had fully documented and implemented the internal controls required for IT project management needed to comply with SOX. Data was collected regarding the current state of IT project management by conducting interviews with IT project managers, evaluating the current SDLC document, and other relevant information (Table 1). The final evaluation will be conducted in January 2006 to evaluate if any additional changes to IT project management are made resulting from the company's 2005 audit on internal controls and from audit reports of other public companies.

Object	**Instances**
Project Manager Interviews	4
IT Steering Committee Meeting minutes	12
SDLC and Internal Control Documents	2

Table 1 Data Collection Types and Quantities

DISCUSSION AND ANALYSIS

The company has experienced significant growth over the past 10 years. Less than five years ago, the applications development team consisted of 10 programmers and a director. IT project management processes were informal and each project adopted its own development life cycle based on general policies. By early 2005, the applications development department had grown to 28 programmers with six project managers. The SDLC documentation that governed IT project management was fully compliant with SOX requirements and was being followed, in detail, by every project manager.

To achieve SOX compliance, and using the COBIT framework as a guide, the company began to document and evaluate the IT organization. This evaluation covered both IT project management and IT operations. Using a series of workflow documents, the major objective areas of COBIT were identified. The process objectives were established, the risks associated with each objective were identified, and a process flow listing various control activities along with their control points were documented. Extracting those control activities relating to IT project management from the workflow documentation, a series of control points that impact the IT project management process was evaluated and the following control points were added to the SDLC.

1. Planning and Organization – the company added a review, by the IT Steering Committee, of every project request with a time estimation greater than 80 hours. This control process ensures that IT projects align with the company's goals and that the projects have been evaluated as to their potential size and cost. It also ensures that executive management is aware of any system changes that could impact financial reporting.

2. Acquisition and Implementation – the company expanded the use of a number of SDLC documents and modified some of its practices. First was the introduction of an IT project checklist. This document serves as a cognitive artifact (Bucklund 2004) to ensure all the control points of an IT project development are executed and documented. Second was the rigid practice of requiring scope change documentation and sign-off when ever the functional requirements of a project were altered. Finally the company introduced formalized test scripts and user test sign-off documents prior to system implementation.

3. Delivery and Support – the company added a policy to create formal operations and support documentation to be handed over to the IT operations department and users at the completion of every project.

4. Monitoring – there were no major changes made regarding IT project management.

Results of change

The impact to IT project management at the company due to the process changes required by SOX are evident in three major areas. First, IT project management has become significantly more formalized. Every project has a checklist that must be followed and will be audited. In the past, the applications development team had the flexibility to include only those processes that contributed to the development of the product. Now that IT project management has become more process centric, every project must adhere to the SDLC guidelines and document that each control point has been followed. Second, the time to implement and complete a project has increased. Prior to SOX requirements, the need to formally review every project by an outside committee was not needed. Now, additional time is required to prepare a project proposal with the necessary information, so an outside committee will be able to evaluate the merits of the request. In addition, the project managers feel that the significant increase in paperwork and sign-off documentation typically adds 10 – 20% to the project implementation time line, which reduces the number of projects that can be implemented in year. Thirdly, the company is seriously considering moving towards process automation. The company is actively seeking IT project management tools to assist in the management of the SDLC and required documentation with the hopes that it will be able to recover some of the time being lost maintaining SOX compliance.

In addition to the three primary changes to IT project management, the company is experiencing some secondary impacts. First, the IT project managers feel that processes required by SOX have improved the company's rating on a standard maturity model. Most of the project managers feel that they have moved from an initial or repeatable rating to a defined process rating or better. Second, some developers have expressed increased frustration with the added paperwork required by SOX, which might lead to a decrease in job satisfaction. This could mean that IT project managers must spend additional effort keeping the programmers and systems analysts content in their jobs or risk higher levels of turn over.

RESEARCH PROGRESS AND REMARKS

The data collection for this case study will be completed in January 2006 after the second internal controls audit is complete. An updated review of relevant documents will be made and any supporting information will be added to literature review and background section of the study. Another series of interviews will be conducted with the project management team to evaluate if any additional changes were adopted.

REFERENCES

1. Bucklund, P. (2004) Introducing New IT Project Management Practices - a Case Study, Tenth Americas Conference of Information Systems, August 6-8, New York, NY, 785-792.
2. Burrowes, A.W., Kastantin, J., and Novicevic, M.M. (2004) The Sarbanes-Oxley Act as a hologram of post-Enron disclosures: a critical realist commentary, *Critical Perspectives on Accounting*, 15, 797-881.
3. Carnegie Mellon Software Engineering Institute (2001) Capability Maturity Model Integration, Version 1.1, www.sei.cmu.edu, accessed: 2/25/2005
4. Damianides, M. (2005) Sarbanes-Oxley and IT Governance: New Guidance on IT control and Compliance, *Information Systems Management,* 22, 1, 77-85.
5. Dietrich, R. (2004) Sarbanes-Oxley and the Need to Audit Your IT Processes - An MKS White Paper, MKS, www.mks.com, accessed: 2/27/05
6. IT Governance Institute (2000) COBIT 3rd Edition - Executive Summary, www.isaca.org, accessed: 2/25/2005
7. IT Governance Institute (2004) IT Control Objectives for Sarbanes-Oxley, www.itgi.org, accessed: 2/25/05
8. Paulk, M.C. (2004) Surviving the Quagmire of Process Models, Integrated Models, and Standards, ASQ: Annual Quality Congress Proceedings, Toronto, Canada, 429-437.
9. Securities and Exchange Commission (2003) Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. 33-8238, June 5, 2003
10. U.S. Congress (2002) The Sarbanes-Oxley Act of 2002. House of Representatives 3763, Public Law 107-204, 107th Congress.