JITTA

JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

THE IMPACT OF THE SARBANES-OXLEY ACT ON IT PROJECT MANAGEMENT

MICHAEL J. LEIH, Claremont Graduate University

School of Information Systems and Technology, 150 E. 10th St., Claremont, CA, 91711,
E-mail: michael.leih@cgu.edu

ABSTRACT

This case study investigated the impact of the Sarbanes-Oxley Act (SOX) on IT project management within a large, nationwide retail corporation. Using the teleological motor as a framework to evaluate process change, this study observed three primary impacts the SOX mandates had on IT project management: (1) an increase in project management formalization, (2) an increase in project duration, and (3) the need to support project management and audit activities with project management software. The study also observed three secondary effects resulting from the changes made to IT project management practices to support SOX: (1) an increase in process maturity, (2) an increase in the size of the IT staff, and (3) a breaking down of larger projects into more, smaller projects. This dual iteration of the teleological cycle appeared to be a natural action / reaction process to the changes resulting from SOX requirements.

INTRODUCTION

The Sarbanes-Oxley Act (SOX) of 2002 was enacted in response to a number of major corporate accounting scandals that rocked the American business landscape. This Act dramatically raised the standards for financial reporting for all SEC registrants, including all U.S. public companies, some private companies registered with the SEC, and all foreign companies trading on a U.S. exchange (Cohen and Qaimmaqami 2005, Dietrich 2004, SEC 2003). Because of the tight integration between financial reporting and information technology (IT), SOX also requires significantly greater levels of auditing on process controls within IT governance (Damianides 2005). The Act requires auditors to publicly report on corporate control processes pertaining to financial reporting and to report to shareholders exactly what control processes are in place and to what extent they are being followed.

The ultimate impact of SOX on corporate governance will likely not be fully known until the new auditing processes have been in effect for several years. This period is required to allow organizations the time to assess how auditors are reviewing their new internal controls and how SOX audits from other public companies are being reported. In addition, the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB), the governing bodies controlling the auditing

Mihir A Parikh acted as the senior editor for this paper.

Leih, M. J., “The Impact of The Sarbanes-Oxley Act on IT Project Management,” *Journal of Information Technology Theory and Application (JITTA)*, 8:3, 2006, 13-30.

standards of SOX, have been revising the internal control auditing standards since the passage of the Act. Additional time is also needed to allow the auditing standards to stabilize.

The case study presented here contributes to the body of research evaluating how regulatory initiatives, such as SOX, are impacting IT governance (Armour 2005, Brown and Nasuti 2005, Haworth and Pietron 2006, Krishnan, Peters, Padman and Kaplan 2005). Specifically, this study documents how the SOX mandates impacted the procedures for IT project management at a single nationwide retailer. To allow sufficient time for any new policies or practices in IT project management to stabilize, the research into the subject corporation was conducted over a period of 30 months, starting in November, 2003. Although SOX is having significant impact to many areas of IT governance, such as IT operations, IT security, and general IT policies and procedures (Damianides 2005, IT Governance Institute 2004), this study is focusing on the specific impacts to IT project management.

The paper is organized as follows: First, a four part background section containing (1) a summary of the internal control mandates of SOX, (2) an overview of how the Committee of Sponsoring Organizations of the Treadway Commission (COSO) control framework is being used as a guide in adhering to SOX internal controls over financial reporting, (3) an overview of how the Control Objectives for Information and Related Technology (COBIT) framework is used to control IT governance, and (4) an introduction of an IT maturity model. Second, a theoretical foundation section describing the teleological theory used to provide a framework through which the data analysis was conducted. Third, a methodology section documenting the case study methodology used, an overview of the research site, and the data collection methods. Fourth, a case analysis section of the new SOX related control procedures implemented into the IT project management practices and an analysis of the impact those changes are having on IT project management. Fifth, a conclusion section summarizing the primary impacts of SOX and the secondary effects that occurred to IT project management practices. Finally, a future research section discussing possible future research questions that can be considered resulting from the observations made in this study.

Contribution

This paper makes a contribution to both the practice of IT project management and the application of the teleological motor as a framework in understanding how regulatory mandates impact IT policies and practices. Although there is a rich body of knowledge in the area of IT project management, there is little research in the area of how new regulatory mandates, such as SOX, are forcing organizations to adopt new IT governance practices when implementing or modifying information systems.

The primary contribution of this case study is threefold; (1) to explore how the passage of SOX has impacted the way a corporation has had to modify their IT project management practices to meet the mandates of the SOX requirements, (2) to contribute to the body of knowledge in the area of how regulatory initiatives impact IT governance, and (3) to use the teleological motor as framework to suggest that major changes to IT project management, resulting from regulatory mandates, pass through two or more iterations of the teleological cycle. This third contribution can be used by other researches as a model to evaluate if changes mandated by regulatory initiatives will have the two phase pattern of primary impact and secondary effect, as observed in this study.

Background

The 66-page Act, consisting of 11 titles and 61 sections, 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, the Act mandates that control processes are put into place over financial reporting and that the

CEO and CFO of the corporation must certify that they have reviewed these controls and assess to their effectiveness.

The Sarbanes-Oxley Act

Title 11 of the Act, Corporate Fraud and Accountability, mandates significant penalties if a company officer, either purposefully or by neglect, reports fraudulent information or omits information (U.S. Congress 2002). According to section 1106, penalties for financial reporting fraud can be as high as a $5,000,000 fine or imprisonment for no more than 20 years. These severe penalties are designed to provide an adequate deterrent for failure to implement proper internal controls that produce accurate and complete financial reporting.

With all its sweeping changes, much of the details of how to comply with the Act were left up to the Securities and Exchange Commission. Together with the PCAOB, the SEC has defined its opinion on how public companies should comply with SOX. On March 9, 2004 the PCAOB issued an updated briefing paper and proposed revised auditing standards, “Auditing Standard No. 2 - An Audit of Internal Control Over Financial Report Performed in Conjunction with an Audit of Financial Statements” (PCAOB 2004). This briefing helped to clarify what standards should be used when auditing a company’s internal controls.

Section 302 of the Act, Corporate Responsibility for Financial Repots, mandates that CEOs and CFOs attest to the accuracy of their company’s quarterly and annual reports (Dietrich 2004). They must certify to the following:

1. They have viewed the report.
2. To the best of their knowledge, the report contains no untrue statement of a material fact and does not omit any material fact that would cause a statement to be misleading.
3. To the best of their knowledge, the financial statements and other financial information in the report fairly present, in all material aspects, the company’s financial position, results of operation, and cash flow.
4. They accept responsibility for establishing and maintaining disclosure controls and procedures. They also accept responsibility that the annual report contains an evaluation of the effectiveness of these measures.
5. Any major deficiencies or material weaknesses in controls, and any control-related fraud, have been disclosed to the audit committee and external auditor.
6. The report discloses significant changes affecting internal controls that have occurred since the last report, and whether corrective actions have been taken (U.S. Congress 2002).

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 that:

1. States management’s responsibility for establishing and maintaining adequate internal controls over financial reports for the company.
2. Identifies the framework used by management to evaluate the effectiveness of this internal control.
3. Assess the effectiveness of this internal control as of the end of the company’s most recent fiscal year.
4. States that an auditor issued an attestation report on management’s assessment (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 are required to review IT internal controls to ensure that all control processes established by the organization are being followed (IT Governance Institute 2004).

While section 302 of the Act mandates that senior executives support internal control activities in the company, it is section 404 (which mandates these internal controls) that is having the greatest impact on corporate governance. These changes to corporate governance have in turn mandated the need to establish formal internal controls in regards to IT project management. In addition, because the auditors must certify that all internal controls are being followed during their annual audit of the company, the need to document each control process is also required. It is the combination of both the following of internal controls and the documentation that internal controls are being followed that is causing the significant impact to IT project management.

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

COSO 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 neither the SOX Act nor the SEC mandates the COSO framework, the SEC's June 2003 announcement recognized COSO as the preferred framework for SOX compliance (SEC 2003). Based on this statement from the SEC, the retail corporation participating in this study chose to adopt the COSO framework as the primary guideline in meeting SOX requirements. According to the COSO framework, internal controls consist of five interrelated components (COSO 2005). These are derived from the way management runs a business, and are integrated within the management process.

The components that make up the COSO framework are:

1. Control Environment – The control environment sets the tone of an organization by establishing attitude standardization. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the corporation's people, management philosophy and operating style.

2. Risk Assessment – Every entity faces a variety of risks from external and internal sources and those risks must be assessed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with that change.

3. Control Activities – Control activities are the policies and procedures that help ensure that management directives are carried out. They help ensure that the necessary actions are taken to address risks during the achievement of company objectives. They also ensure that control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

4. Information and Communication – Pertinent information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports containing financial related information that make it possible to control the reliability of financial reporting.

5. Monitoring – Internal control systems need to be monitored. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

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 is needed to create an environment that is prepared for the audits now mandated by SOX. Several IT internal control frameworks exist (Paulk 2004), however, the IT control objectives known as COBIT are considered particularly useful and aligned with the spirit of SOX requirements (IT Governance Institute 2004). The retail corporation participating in this study chose to adopt the COBIT framework because the consulting firm hired to assist with SOX audit preparations recommended the control objectives and the internal audit department agreed with the recommendation.

Control Objectives for Information and Related Technology (COBIT)

COBIT was developed by the IT Governance Institute (ITGI) as a standard for IT governance. Founded as a not-for-profit organization in 1998 by the Information Systems Audit and Control Association (ISACA), the ITGI is dedicated to creating and sharing better practices for IT governance (IT Governance Institute 2004). The COBIT framework establishes IT governance as a structure of relationships and processes to control the IT organization 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. Table 1 lists each objective in relation to its respective domain based on the IT Governance Institute's 3rd edition of the COBIT framework (IT Governance Institute 2000).

Table 1. COBIT Control Objectives by Domain

Planning and Organization	**Acquisition and Implementation**	**Delivery and Support**	**Monitoring**
PO1 – Define a strategic IT plan	AI1 – Identify automated solutions	DS1 – Define and manage service levels	M1 – Monitor the processes
PO2 – Define the information architecture	AI2 – Acquire and maintain application software	DS2 – Manage third-party services	M2 – Asses internal control adequacy
PO3 – Determine technological direction	AI3 – Acquire and maintain technology infrastructure	DS3 – Manage performance and capacity	M3 – Obtain independent assurance
PO4 – Define the IT organization and relationships	AI4 – Develop and maintain procedures	DS4 – Ensure continuous service	M4 – Provide for independent audits
PO5 – Manage the IT investment	AI5 – Install and accredit systems	DS5 – Ensure systems security	
PO6 – Communicate management aims and direction	AI6 – Manage changes	DS6 – Identify and allocate costs	
PO7 – Manage human resources		DS7 – Educate and train users	
PO8 – Ensure compliance with external requirements		DS8 – Assist and advise customers	
PO9 – Assess risks		DS9 – Manage the configuration	
PO10 – Manage projects		DS10 – Manage problems and incidents	
PO11 – Manage quality		DS11 – Manage data	
		DS12 – Manage facilities	
		DS13 – Manage operations	

Each control objective in the COBIT framework can be regarded as a separate process that can be established to assist in the overall IT governance within the corporation. These control objectives can be mapped to the COSO components to meet the internal control requirements of SOX. Figure 1 demonstrates how the COSO and COBIT frameworks can be overlaid to sections 302 and 404 of the Act (IT Governance Institute 2004).

The SEC and PCAOB have provided little guidance to the IT organization on exactly how to implement internal controls to meet the mandates of SOX beyond the recommendation of the COBIT framework. Given that the COBIT framework was developed to provide an overall IT governance structure, which goes far beyond the internal control requirements specified in the Act (IT Governance Institute 2004), the impact on the IT organization is worth researching. This case study begins to evaluate how the implementation of internal controls mandated by SOX are impacting IT project management.

Maturity Models

As IT controls are established, the ability to develop measures of those processes are important in tracking their effectiveness. Key to this measurement is the use of maturity models for self-assessment and benchmarking. Maturity models can be effective tools for determining the current status of the organization's processes and how they should evolve (Dietrich 2004). Carnegie Mellon's capability maturity model integration (CMMi) is defined with five levels of maturity (Carnegie Mellon Software Engineering Institute 2001) and is a good example of how most maturity models are organized. Table 2 lists each of the five maturity levels along with a description of what each level of maturity should produce.

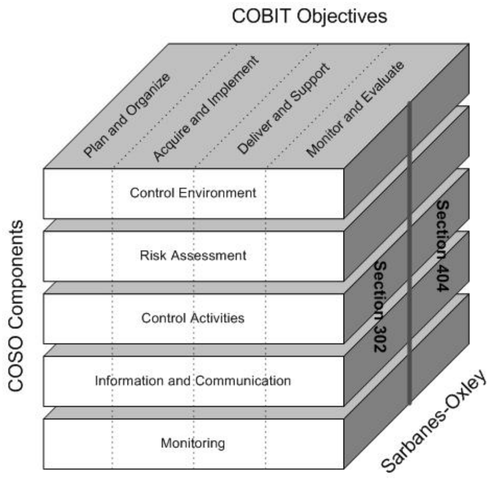

Figure 1. COSO/COBIT overlay matrix (Adapted from IT Governance Institute 2004)

Table 2. Maturity Model Level Definition and Descriptions

Level	Maturity	Description
1	Initial	Control processes are non-existent or ad hoc.
2	Repeatable	Basic project management processes are established to track cost, schedule and functionality.
3	Defined	The control process is documented, standardized, and integrated into a standard software process for the organization.
4	Managed	Detailed measurements of internal control processes and product quality are collected. Both process and products are quantitatively understood and controlled.
5	Optimizing	Continuous process improvement is enabled by quantitative feedback from the control processes.

For the purposes of establishing internal control, some organizations may be willing to accept IT controls that fall somewhat short of level 3. However, given SOX 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).

THEORETICAL FOUNDATION

Van de Ven and Poole (1995) have identified four theories, or "motors", that serve as building blocks for explaining the process of change in an organization: life cycle, teleology, dialectics, and evolution. Each of these theories describes different progressions of change events that are driven by different forces and operate at different levels within an organization. In addition, each of these theories is part of the larger family of process theory focusing on organizational transitions through events and activities that occur over time (Cule and Robey 2004).

Life cycle theory is adopted from the metaphor of organic growth and describes the continuous progression of change as an organization begins, develops, matures, and eventually terminates. Teleology theory is based on the philosophical premise that a defined purpose or goal is the driving force of change in an organization. Dialectics theory is based on the Hegelian assumption that organizations exist in a pluralistic context with competing ideas and values as the cause of change within an organization. Finally, evolution theory is used to explain the changes to an organization through a continuous cycle of mutation, selection, and retention. Of these four, the teleological motor appears to provide the most appropriate framework through which to analyze the organizational change caused by a regulatory mandate, such as SOX.

The teleological motor has been used in several case study research papers as a framework through which to interpret the changes an organization is experiencing (de Rond 2004, Doz 1996, Pare 2002). In addition, other papers have referenced teleology as an appropriate foundation for determining the cause of change and a model through which to evaluate the study of organizational transitions (Cule and Robey 2004, Hooker 2004). The mode of change associated with teleology is considered to be constructive. A constructive mode of change typically creates unique and innovative forms that are often considered to be unpredictable and discontinuous departures from past activities (Van de Ven and Poole 1995). This mode of change is not described as deterministic, but rather emergent as the change process unfolds. Van de Ven (1992) explains that the model incorporates the systems theory assumption of equifinality; that there are several equally effective ways to achieve the given goal.

Van de Ven and Poole (1995) define the teleological process of organizational development and change as a continuous cycle. In the case of satisfying a regulatory requirement, the initial stage of "dissatisfaction" is created by the new legislation. That is to say, the new law causes the state of dissatisfaction if the organization is not already compliant with the new mandate. The second stage of "search and interact" is the organization's response to determine what modifications to the organization are required to meet the new mandate. The third stage of "set / envision goals" is the process of defining the new business procedures to meet the new regulatory requirement. The final stage of "implement goals" is the execution of the business procedures defined in the previous stage. The rotation continues back to "dissatisfaction" if the subsequent cycle did not produce an adequate change in the business to meet the mandated behavior or the results of the initial change causes a secondary state of dissatisfaction. Figure 2 represents the teleological change cycle.

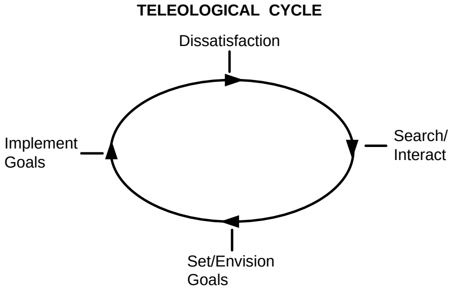

Figure 2: Teleological Cycle (Adapted from Van de Ven and Poole 1995)

METHODOLOGY

We selected a case study methodology to research the topic of this study because it is an appropriate method of research when "how" types of questions are being posed (Yin 2003). In addition, the research question of how SOX is impacting IT project management is relatively new and is not supported by a strong research base, providing more support for a case study approach (Benbasat, Goldstein and Mead 1987, Darke, Shanks and Broadbent 1998). Specifically, we conducted the study as an explanatory case study, with a positivist perspective. This approach allows the study to look for linkage between SOX compliance and changes to IT project management practices (Yin 2003).

This study was conducted at a publicly traded retailer. The company has retail locations located throughout the United States and is currently exceeding $1 billion in annual sales. The centralized IT department within the company uses an in-house project management methodology to manage over 100 projects per year. The software development practice within the company is to purchase commercial (and often customizable) off-the-shelf applications (COTS) and to configure and integrate these applications into the IT organization. Most projects last between four and twelve weeks, with a few projects lasting upwards of twelve months.

We conducted the study over a period of 30 months to evaluate the changes during the initial SOX compliance initiative and to evaluate subsequent changes during the first two years of SOX control audits. The study was initiated in November 2003, at the beginning of the company's SOX compliance process. At that time, the IT programming services department had four development project teams consisting of four project managers and twelve senior programmer analysts. The four project managers reported to a director of programming services. The study was concluded in May 2006 after the results of the second SOX control audit were published. By that time the IT programming services department had expanded to include the director of programming services, two senior programming managers, six programming managers (formally titled project managers) managing six development teams, four systems analysts, sixteen senior programmer analysts, two quality assurance (QA) analysts, and a technologies trainer.

We began our research by evaluating the company's internal control documentation relating to IT project management and the IT department's system development life cycle (SDLC). The SDLC is the primary document that governs the control processes used by the IT department for application development and change management as well as defines the IT project management methodology used by project managers. Next, we interviewed the company's newly appointed manager of internal audit to evaluate what control points, if any, were lacking in the IT project management process. The internal audit department was created in conjunction with SOX mandates and has the primary role to provide independent assurance to executive management and the board of directors that the system of internal controls are adequately designed and operating effectively. This assurance is accomplished through risk assessments, testing, and other activities that occur during the audit process. Finally, we interviewed the director of programming services and two project mangers to determine the state of the pre-SOX IT project management practices. The current state of IT project management was noted, along with what changes were going to be made to achieve SOX compliance.

In January 2005, towards the completion of the company's first annual SOX control audit, we conducted a second set of interviews with the manager of internal audit, the director of programming services, and the project managers. At that point, the company had fully documented and implemented the internal controls required by SOX for IT project management in the SDLC. We made a comparison between the 2003 SDLC and the 2005 SDLC and any changes to IT project management practices were noted. In addition, we reviewed the IT steering committee meeting minutes for any changes to IT project management policies. The IT steering committee, consisting of the CFO, the CEO, the VP of IS, and the manager of project planning, was created in early 2004 as a control mechanism to govern which project requests were to be worked on by the IT department. Furthermore, project status reports on major projects were given at steering committee meetings, as were any changes to IT control practices. Changes to IT project management practices were noted along with any comments relating to project management activities.

We completed data collection in May 2006 after the second SOX control audit was finished and published. We conducted interviews with the internal audit department and programming services and completed a final evaluation of the current SDLC and compared it with the versions from 2003 and 2005. In addition, we evaluated the project documentation for each of the 28 projects that were audited during 2005 and 2006 to validate that the controls documented in the SDLC were being followed. We reviewed the 2005 IT steering committee meeting minutes to provide further evidence and context to any changes made to the SDLC and project management practices. Table 3 provides a summary of the types and instances of data that were collected during the study.

Interviews were semi-structured, consisting of ten to fifteen open ended questions and lasting between 45 and 90 minutes. The initial interviews conducted in 2003 and 2005 were less structured than those conducted in 2006. Following the suggestions given by Yin (2003) and using an iterative approach as suggested by Glaser and Strauss (1967), interview questions in the final data collection phase were more focused and based on themes derived from information gathered in the first two years. We took notes during each of the interviews and the interviews (where the participants agreed to it) were recorded, transcribed, and loaded into the ATLAS.ti qualitative research software. Documents, interview notes and field notes were also entered into the software to provide a common place for data analysis. We coded and categorized the text data to provide analysis of common themes and an index was created for searching and retrieval activities. The data analysis was primarily inductive and relied on triangulation of different sources to build a set of theories on how SOX is impacting IT project management (Eisenhardt 1989, Glaser and Strauss 1967).

CASE ANALYSIS – OVERVIEW OF NEW CONTROL PROCEDURES

To achieve SOX compliance, and using the COBIT framework as a guide, key members of IT management and the internal audit department documented and evaluated the IT organization. This evaluation covered both IT project management and IT operations. Using a series of workflow documents, the internal audit department documented the major objective areas of the COBIT framework. 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.

The internal audit department determined that not all the control objectives defined in COBIT were necessary to meet SOX mandates. Therefore only those control objectives not already in place but found to be required were considered. 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 were evaluated and a set of control points were then added to the SDLC. These control points are explained in detail in the following sections and are summarized in Table 4.

Table 3. Summary of Data Collection

Data Type	Instances
Internal audit interviews	3
Director of programming services interviews	3
Project manager interviews	9
IT steering committee meeting minutes	18
SDLC and internal control documents	3
Project documentation	28

This adjustment to the SDLC follows a complete iteration of the teleological change cycle. The "dissatisfaction" was caused by the need to meet the SOX mandates. The "search and interact" phase was entered when the company began to evaluate the current SDLC with the control processes defined in the COBIT framework to meet the SOX regulatory requirements. The third phase of "set and envision goals" was completed when the necessary changes to IT project management practices were identified and documented. The final phase of "implement goals" was entered when the new IT project management practices were entered into the SDLC and adopted by project managers.

Most of the changes were initiated and implemented in 2004 for the 2005 controls audit, while a few were added or modified in 2005 for the 2006 controls audit. According to IT management, approximately five person-months of effort were required to complete the initial documentation process in 2004. An estimated effort of one person-month is required each year to maintain the documentation. The following is a summary, by COBIT domain, of the modifications to the SDLC.

Planning and Organization

PO1 – Define a Strategic IT Plan. Prior to SOX compliance, the company's strategic plan consisted of a few defined initiatives that were agreed upon year to year. The priorities for the initiatives routinely changed throughout the year and projects were initiated or cancelled as the need arose.

The company determined that two new control processes were required. The first was to create a formal strategic plan for the year and to establish priorities to the identified strategic initiatives. The strategic plan is created by IT management and approved by executive management. The second was to establish an IT steering committee to review each new project initiative to ensure it aligns with the strategic plan. Now every project request is reviewed and approved by the IT steering committee prior to the start of the project.

These control processes ensure that IT projects align with the company's strategic goals and that the projects have been evaluated with respect to their potential size and cost. It also ensures that executive management is aware of any system changes that could impact financial reporting. According to the IT management involved in this study, this is a welcomed process change. The management team feels this approach provides a better framework for long-range development planning and gives the project teams a better idea of what they will be working on in the next six to twelve months.

PO10 – Manage Projects. Prior to SOX compliance, each project manager had his or her own way of managing and documenting project tasks and activities. To ensure that each project is managed appropriately, IT project checklists were created to serve as a type of cognitive artifact (Bucklund 2004). A total of four project checklists were created containing various levels of pre-defined activities based on project size. Smaller projects had less formal analysis and design activities, while larger projects required more project documentation and project reviews. The project checklist is kept with the rest of the project's documentation and it is the project manager's responsibility to ensure that each activity on the checklist is executed and documented.

Most project managers agree that this level of formalization in project management is generally a good policy and helps ensure that projects follow the proper development life cycle. However, programmers and analysts felt that much of the additional documentation provided little value beyond process compliance and often expressed some frustration to the project managers regarding the extra paperwork.

PO11 – Manage Quality. The introduction of a formal user acceptance and testing procedure was added to the SDLC. Prior to moving any IT component of a project into a production mode, key users of the IT application must test, and attest to, the new system's completeness (meeting all functional requirements) and correctness. Although this process was completed in a less formal manner prior to SOX, the new process ensures that all aspects of the new IT system go through acceptance testing and meets the documented project requirements. It also requires that all tests are documented and that the project stakeholders sign-off on testing so auditors can review this control point in the SDLC process.

Most of the people involved in this study found value in the new testing procedures. However, according to one project manager, this new process sometimes creates a "bottle neck" with the software testing team if several projects are entering the testing phase at the same time. This causes frustration with users when there are delays of several days or weeks in project implementation because of testing constraints.

Acquisition and Implementation

A16 – Manage Change. A more formal and rigid change process was initiated to document and control any changes to a project's functional requirements. If a functional change is requested by anyone, a scope change document is created and the size and cost of the change is identified. The scope change is then reviewed and approved by the project management team and executive management before any aspect of the scope change is acted upon.

Prior to SOX, scope changes were often considered as a matter of course during development and the impact of the scope change was not formally evaluated. Now, scope change requests are more formal and can require significant effort to be approved.

The director of programming services finds this process change extremely helpful when trying to prevent scope creep. The director leverages the effort required to approve a scope change to motivate users to submit complete project requirements at the beginning of the development cycle. According to all the project managers, users typically attempt to "slip" in additional functionality during the testing phase of the SDLC, which can lead to significant delays in implementation and delay the start date of future projects. The process of change control helps to prevent scope changes from occurring and gives the project manager a greater level of control when completing a project.

Delivery and Support

DS7 – Educate and Train Users. Two tasks were added to the SDLC to address the training and education of users. If the implementation or modification of a system warrants new operational practices, then formal training and operational documentation is developed as part of the project requirements. In addition, a training task was added to the project checklist so any new operational practices can be communicated to both the user community and the IT operational and support teams.

According to the director of programming services, the requirement to add these tasks was the justification needed for a new technical writer and IT trainer. One project manager commented that these new team members helped improve morale with some of the programmers, as they no longer had to spend as much time creating operational and training documentation and could spend more time designing and developing software.

Monitoring

M2 – Assess Internal Control Adequacy. At the completion of each project, a senior programming manager reviews the project documentation to ensure that all control activities were completed and documented. In addition, a business analyst conducts a project review to ensure that project requirements were met and compares the time and cost estimates determined at the beginning of the project with actual time and cost values to evaluate estimation accuracies.

According to those interviewed during the case study, however, the project review is producing little value in its current implementation and will likely be reevaluated in future versions of the SDLC. Most project managers feel that the testing process ensures project requirements are being met and that by the end of the project, no one seems to care if project time and cost estimates were accurate.

Table 5 is a summary of the new controls that were added to the SDLC to meet SOX mandates for software implementation projects.

Table 4. Summary of New Controls added to the SDLC to meet SOX mandates

COBIT Control	Summary
PO1 – Define a Strategic IT Plan	The creation of a more formal and controlled strategic plan and the creation of an IT steering committee to authorize and monitor new projects.
PO10 – Manage Projects	The creation of project checklists to ensure each project addresses every required task in the SDLC.
PO11 – Manage Quality	The introduction of formal user acceptance testing with documented test plans and user sign-off.
A16 – Manage Change	The creation of a scope change document and the re-evaluation of the project when scope changes occur.
DS7 – Educate and Train Users	The addition of two tasks in the SDLC to create operational and user documentation and to train users in new functionality.
M2 – Asses Internal Control Adequacy	A final review of project tasks by a senior programming manager to ensure all activities in the SDLC are being followed.

CASE ANALYSIS – IMPACT OF SOX

The impact to IT project management at the company due to the process changes required by SOX can be classified into two categories, primary impacts and secondary effects. Primary impacts are those changes to IT project management that are directly associated with SOX compliance. Secondary effects are those changes to IT project management resulting more from the primary impacts rather than directly from SOX compliance mandates. These changes can be analyzed through two cycles of the teleological motor. The changes occurring in the first cycle of the teleological change process are associated with the dissatisfaction caused by the SOX mandates. The changes occurring in the secondary cycle of the teleological change process are associated with the dissatisfaction caused by the initial process change during the first cycle. This duel rotation of the teleological cycle appears to be a natural action / reaction sequence.

Primary Impacts

The primary impacts are evident in three major areas, an increase in process formalization, an increase in project duration, and a need to use project management software to support audit activities. First, IT project management has become more process centric and significantly more formalized. Every project over an estimated 80 hours of effort is reviewed by the IT steering committee. The addition of this formal project approval process to the SDLC has had both a perceived positive and negative consequence. Some project managers feel the formal approval process gives them greater consistency and stability while working on IT projects.

> *It was not uncommon for us to start a project, then a few weeks later, be told to put the first project on hold while we start a second project. After completing the second project, we would go back to continue on the first project, but found that most of the requirements had changed so we basically started over. Now that we have the strategic plan and project requests must be approved by committee, we have less switching of priorities. (Project Manager)*

Other project managers however, feel the approval process is too formal and delays the start of critical projects, reducing their ability to complete the project by the required deadline.

> *The project approval process can sometimes take more time than the project itself. It is frustrating knowing that a project is due in two months, but have to wait two or three weeks before we can start on it while it gets approved. (Project Manager)*

In addition to the project approval process, 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.

This new standard is also met with mixed opinions.

> *The project checklists have been useful in setting development standards, but most of the programmers don't like the amount of paperwork that is required to complete programming tasks. They feel it is a big waste of time. (Project Manager)*

Second, the time to implement and complete a project has increased. Prior to SOX requirements, there was no need to formally review every project by an outside committee. Now, additional time is required to prepare a project proposal with the necessary information, so the IT steering 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 a year.

> *Sometimes it takes a few weeks to review the paperwork after a project has been completed to be sure all the documents are there for the [SOX control] audit. Every time I find some piece of paper that's missing or a missing signature, I have to go hunt it down. If it wasn't for all the paperwork, we could get a few more projects done. (Senior Programming Manager)*

Third, the company is in the process of implementing software to support the SDLC and the documentation that is required for audit. This project management software will be configured to store all the related documents required for the SOX control audit, define the proper tasks required based on the project type and size (replacing the paper version of the project checklist), and log program modification activity related to each project. The application supports the ability to flag any missing elements of a project and to print out a project report for the auditors to review.

> *For the past two years, I spent almost 80% of my time during the [SOX control] audit chasing down paperwork and gathering data. The auditors wanted to review every line of the CMS [software change management system] log this year. With the new system, I can push a button and the auditors will have all the paperwork they need. (Director of Programming Services)*

These three primary impacts have significantly increased the cost of project management and implementation. The cost of purchasing and maintaining a software tool to support the SDLC and project related documentation is estimated by the director of programming services at $250,000 for the initial installation and $50,000 per year to license and maintain. Although this application does provide some level of return on investment though improving SDLC efficiency, it does not completely compensate for the additional costs of project implementation caused by the increase in labor required to complete a project.

The director of programming services estimates that after the company's third year of meeting SOX requirements, that fewer projects are being completed when compared to pre-SOX years. In addition, the added cost in payroll time from both developers and users to document SOX control activities so the company can pass audit procedures provides no value to the end product of the project. Project managers estimate that during 2005, nearly 20 man months of effort, out of the 144 man months of effort available through the programming staff, were used in preparation for the annual SOX audit and to document that SOX control processes are being followed.

Secondary Effects

In addition to the three primary impacts to IT project management, the company is experiencing three secondary effects, a perceived increase in process maturity, an increase in IT staff, and a breaking down of large projects into more, smaller projects. First, though a formal certification has not been undertaken, the IT project managers feel that the processes required by SOX have improved the company's software practices with respect to the standards specified by CMMi. Most of the project managers feel that they have moved from an initial or repeatable rating (level 1 or 2) to a defined process rating (level 3) or better.

> *I think the process makes development more predictable, even if it means it will always take longer than it should. Before we had the new SDLC, you never knew where the project really was. Now when a programmer says he is almost done, I know that there are still a few weeks of testing and user sign-off required before we can move it into production. Every project pretty much follows the same process now. (Senior Programming Manager)*

Second, the size of the IT department grew at a much faster rate during the first three years of the new SOX requirements than it did in the past. Two programming positions were added to support the implementation of new controls required by SOX in various business applications. A technical writer was added to support the new project training and user documentation requirements. Two quality assurance program testers were added to support the separation of duties requirement between the development of software and the testing of software. Finally, a person was added to manage and document all the new control procedures within the IT department. These additions were seen as a positive side effect of the SOX mandates.

> *I had been trying for years to get a technical writer and a QA team. I think SOX allowed us to accelerate the process of getting to the staffing levels we needed to support the company's growth. (Director of Programming Services)*

Third, some larger projects are now being broken down into smaller projects. With the increase in the number of activities required for larger programming projects, the users requesting programming changes have learned to ask for changes in smaller increments. The perception from the users is that smaller projects are approved more easily and will be completed more quickly.

> *Everyone knows that an 80 hour project can be squeezed in without the need to go through the IT steering committee. I actually like the smaller projects. We can get to them and get something back to the users more quickly. It's good to have these projects around when we have some down time waiting for QA to get back to us with the big projects. The problem is that we can get too many of these and if they are important we may not get to them fast enough because the bigger projects approved by the steering committee have priority. (Project Manager)*

The following table is a summary of the impacts to IT project management resulting from the required changes to the SDLC.

CONCLUSION

The findings from this case study have shown a set of primary impacts and secondary effects on IT project management resulting from the implementation of SOX control mandates. The study was conducted over a period of 30 months so that the pre-SOX IT project management process could be documented (year one) and the initial impact of the new control standards could stabilize (years two and three). The final set of interviews conducted as part of the study suggest that the ultimate impact of SOX may not be realized for several years as companies continue to adjust their control procedures as auditing practices become more standardized.

There were several comments during the final set of interviews stating that auditing practices changed from year one to year two, and that year three will likely bring new auditing practices requiring further modifications to the SDLC. Furthermore, it is likely that changes to the SDLC will continue as the software development team explores more effective and efficient ways to manage projects, regardless of any new changes to SOX auditing practices.

The primary impacts and secondary effects observed in this study suggest that SOX was, in this case, the catalyst to move towards a more mature development process in IT project management. Three of the more significant changes, the creation of an IT steering committee, the enforcement of a more ridged scope change management process, and the creation of the technical writing and quality assurance team in the IT department, are changes the IT management team has been asking for, but had not been able to get prior to SOX. Based on comments made during the interviews, the IT management team did feel these changes would have eventually occurred

Table 5. Summary of Primary Impacts and Secondary Effects from required SDLC changes

Type	Impact	Description
Primary Impact	Increase in Process Formalization	Through the creation of the IT strategic plan, the creation of the IT steering committee, the additions to the SDLC to document IT project management controls, and the creation of the project check list to ensure all project activities are followed.
	Increase in Project Duration	To allow for the review and approval by the IT steering committee, to allow for the documentation of all SDLC activities, and to allow for formal user testing and acceptance.
	Project Management and Audit Review Software	A centralized system to manage and track project documentation and activities to reduce documentation effort and simplify the audit processes.
Secondary Effects	Increase in Process Maturity	The IT project management process has become more repeatable and predictable.
	Increase in IT staff	The addition of more programmers to support SOX requirements and the addition of a QA team, a technical writer, and a process control person.
	More smaller projects	Because smaller projects require fewer control activities and are easier to get approved, some larger projects are being broken down into a series of smaller projects.

as the company continued to grow, but that SOX forced these changes to occur sooner.

Even though many aspects of the increase in process maturity are welcome, the perceived negative impacts were most often commented on. The software development teams feel the new process is less agile and reduces the number of projects that can be completed in a year. However, there were many differing views to these perceived negative impacts. While one project manager would see the extra time required for project approval to be an unneeded delay to the start of the project, another would see it as the means to avoid starting projects that would later be postponed or cancelled due to changing priorities. While one project manager would complain about all the formal procedures required to move an application into production, others would welcome the process to ensure the application was ready for production and that all the stakeholders related to the project were properly notified and trained. All, however, agreed that the amount of paperwork needs to be reduced, if possible, and that a project management system needs to be implemented to support auditing requirements.

In regards to how these impacts are viewed through a teleological framework of process change, there is evidence to show that process changes resulting from SOX compliance follows a two cycle pattern. The first iteration of the cycle begins with the dissatisfaction of being out of SOX compliance and ends with the goal of meeting compliance standards. This first cycle produced the process changes that were identified in this study as the primary impacts of SOX on IT project management. The second iteration of the cycle begins with the dissatisfaction of an increased workload to meet SOX standards and ends with the goal to improve IT project management efficiencies and of adding IT staff. This second cycle produced the process changes that were identified in this study as the secondary effects. There is evidence that additional iterations of the change cycle will continue as the company adjusts to changes in auditing standards and seeks to improve IT project management efficiencies. However, the first two iterations were more notable and more closely seen as a paired progression.

FUTURE RESEARCH

This research paper offers qualitative support that SOX has had a significant impact in the way IT project must be managed in a publicly held company. Based on this initial finding, additional questions should be considered in future research. Further research is required to establish if similar impacts to IT project management are being realized in other public corporations. Based on previous publications relating to maturity levels in small and medium sized enterprises (Baskerville and Pries-Heje 1999, Kautz, Westergaard Hansen and Thaysen 2000), we suspects that the changes to IT project management caused by SOX requirements are less pronounced in larger corporations and more pronounced in smaller ones.

In addition, research should consider the long term impact of SOX. That is, “will SOX require a constant review and upkeep of the software development process as auditing standards change?” or “will the processes used to manage IT projects eventually solidify as being SOX compliant with little or no changes in subsequent years?” Finally, “are the IT project management practices being adopted by public companies to meet SOX mandates, also being adopted by private organizations and government agencies as a set of best practices in IT project management?” Organizations, such as the ITGI, with their COBIT framework and the Project Management Institute (PMI), with their project management body of knowledge (PMBOK) standards base their existence on project management processes and control objectives. These standards organizations make a strong argument for the use of development standards, but will these standards be adopted by organizations as best practices that are not legally bound to follow them just because public companies are mandated to adopt them?

Appendix: Sox Relevant COBIT Controls for IT Project Management

Table 6 is a summarized list of all the COBIT controls that were determined by the company to be relevant for SOX compliance in regards to IT project management. This list is based on the state of the IT policies and practices at the conclusion of this study and includes both the COBIT controls that were already addressed in the SDLC documentation prior to SOX and those that were added over the course of this study. It should be noted that this list of COBIT controls is based on the subject company’s interpretation of COBIT controls and SOX compliance requirements as they relate to IT project management. Other organizations will likely have lists that differ in some aspects.

Table 6. SOX relevant COBIT controls for IT project management

COBIT Control	Comment
PO1 – Define a strategic IT plan	Control added to the SDLC
PO2 – Define the information architecture	The SDLC documentation already supported the concept of a data dictionary and the requirement to utilize a standard data architecture in the development and implementation of new applications.
PO5 – Manage the IT investment	The SDLC documentation already supported a standard ROI analysis at the beginning of each project and project managers were required to track project related expenses.
PO8 – Ensure compliance with external requirements	Although SOX requirements added IT project management activities to the SDLC documentation, the original SDLC did contain a requirement to ensure new application implementations met with existing regulations, such as privacy laws and security requirements.
PO10 – Manage projects	Control added to the SDLC
PO11 – Manage quality	Control added to the SDLC
AI1 – Identify automated solutions	The SDLC documentation already supported that every project be reviewed by IT management to ensure that user requirements are being met using appropriate automated solutions, including consideration of operability, performance, scalability and integration.
AI5 – Install and accredit systems	The SDLC documentation already supported a defined installation and acceptance process when implementing new applications. However, additional processes were added to the SDLC to support the education and training of users prior to implementation (See DS7).
AI6 – Manage changes	Control added to the SDLC
DS7 – Educate and train users	Control added to the SDLC
M2 – Asses internal control adequacy	Control added to the SDLC

REFERENCES

Armour, P. G., "Sarbanes-Oxley and Software Projects", *Communications of the ACM,* 2005, 48:6, 15-17.

Baskerville, R. and Pries-Heje, J., "Knowledge capability and maturity in software management", *The DATA BASE for Advances in Information Systems,* 1999, 30:2, 26-43.

Benbasat, I., Goldstein, D. K. and Mead, M., "The case research strategy in studies of information systems", *MIS Quarterly,* 1987, 11:3, 369-386.

Brown, W. and Nasuti, F., "What ERP systems can tell us about Sarbanes-Oxley", *Information Management & Computer Security,* 2005, 13:4, 31-327.

Bucklund, P., Introducing New IT Project Management Practices - a Case Study, Tenth Americas Conference of Information Systems, August 6-8, 2004, New York, NY, 785-792.

Burrowes, A. W., Kastantin, J. and Novicevic, M. M., "The Sarbanes-Oxley Act as a hologram of post-Enron disclosures: a critical realist commentary", *Critical Perspectives on Accounting,* 2004, 15:6-7, 797-881.

Carnegie Mellon Software Engineering Institute, Capability Maturity Model Integration, Version 1.1, 2001, Available at: www.sei.cmu.edu, last accessed 25 February 2005.

Cohen, A. F. and Qaimmaqami, D. J., "The US Sarbanes-Oxley Act of 2002: Summary and update for non-US issuers", *International Journal of Disclosure and Governance,* 2005, 2:1, 81-107.

COSO, Internal Control Issues in Derivatives Usage - Executive Summary, 2005, Available at: www.coso.org, last accessed 10 December 2005.

Cule, P. E. and Robey, D., "A Dual-Motor, Constructive Process Model of Organizational Transition", *Organization Studies,* 2004, 25:2, 229-260.

Damianides, M., "Sarbanes-Oxley and IT Governance: New Guidance on IT control and Compliance", *Information Systems Management,* 2005, 22:1, 77-85.

Darke, P., Shanks, G. and Broadbent, M., "Successfully completing case study research: combining rigour, relevance and pragmatism", *Information Systems Journal,* 1998, 8:4, 273-289.

de Rond, M., "On the Dialectics of Strategic Alliances", *Organization Science,* 2004, 15:1, 56-59.

Dietrich, R., Sarbanes-Oxley and the Need to Audit Your IT Processes - An MKS White Paper, 2004, Available at: www.mks.com, last accessed 27 February 2005.

Doz, Y. L., "The Evolution of Cooperation in Strategic Alliances: initial conditions or learning processes?" *Strategic Management Journal*, 1996, 17:Special Issue, 55-83.

Eisenhardt, K. M., "Building Theories from Case Study Research", *Academy of Management. The Academy of Management Review,* 1989, 14:4, 532-550.

Glaser, B. and Strauss, A., *The discovery of grounded theory: Strategies for qualitative research.,* Chicago, Aldine Transaction, 1967.

Haworth, D. A. and Pietron, L. R., "Sarbanes-Oxley: Achieving Compliance by Starting with ISO 17799", *Information Systems Management,* 2006, 23:1, 73-87.

Hooker, J. N., "Is Design Theory Possible?" *Journal of Information Technology Theory and Application,* 2004, 6:2, 73-83.

IT Governance Institute, COBIT 3rd Edition - Framework, 2000, Available at: www.isaca.org, last accessed 25 February 2005.

IT Governance Institute, IT Control Objectives for Sarbanes-Oxley, 2004, Available at: www.itgi.org, last accessed 25 February 2005.

Kautz, K., Westergaard Hansen, H. and Thaysen, K., Applying and adjusting a software process improvement model in practice: the use of the IDEAL model in a small software enterprise, International Conference on Software engineering, June 4-11, 2000, Limerick, Ireland, 626-633.

Krishnan, R., Peters, J., Padman, R. and Kaplan, D., "On Data Reliability Assessment in Accounting Information Systems", *Information Systems Research,* 2005, 16:3, 307-326.

Pare, G., "Implementing Clinical Information Systems: A Multiple-Case Study within a US Hospital", *Health Services Management Research,* 2002, 15:1, 71-92.

Paulk, M. C., "Surviving the Quagmire of Process Models, Integrated Models, and Standards", *ASQ World Conference on Quality and Improvement Proceedings,* 2004, 58:0, 429-437.

Public Company Accounting Oversight Board, Auditing Standard No. 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements, 2004, Available at: www.pcaobus.org, last accessed 25 March 2005.

Securities and Exchange Commission, Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 2003, Available at: www.sec.gov, last accessed 14 April 2003.

U.S. Congress "The Sarbanes-Oxley Act of 2002", 2002, House of Representatives 3763, Collection, 23 January 2002.

Van de Ven, A. H., "Suggestions for Studying Strategy Process: A Research Note", *Strategic Management Journal*, 1992, 13:Special Issue, 169-191.

Van de Ven, A. H. and Poole, S. M., "Explaining Development and Change in Organizations", *Academy of Management. The Academy of Management Review*, 1995, 20:3, 510-540.

Yin, R. K., *Case Study Research: Design and Methods,* (3rd ed.), Thousand Oaks, CA, Sage Publications, Inc., 2003.

AUTHOR

Michael Leih is a Ph.D. student at Claremont Graduate University and holds a M.S. in Computer Science from California State University, Fullerton. His research interests include IT governance, IT project management, and application development methodologies. Michael’s work has appeared in the Americas Conference in Information Systems proceedings 2005 and 2006. He has over 20 years of experience as an IT professional and over 10 years experience as an IT project manager.