

December 2006

IT Governance and the Sarbanes-Oxley Act

Michael Leih
Claremont Graduate University

Follow this and additional works at: <http://aisel.aisnet.org/amcis2006>

Recommended Citation

Leih, Michael, "IT Governance and the Sarbanes-Oxley Act" (2006). *AMCIS 2006 Proceedings*. 129.
<http://aisel.aisnet.org/amcis2006/129>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2006 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

IT Governance and the Sarbanes-Oxley Act

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 internal controls requirement of the Sarbanes-Oxley (SOX) Act has also greatly impacted IT governance. This paper is the result of a grounded theory research study that evaluated written submissions from the public, to the SEC, and the experiences and opinions about how the Act's internal controls requirement has impacted publicly held companies. The grounded theory study resulted in seven propositions that theorize how the implementation of mandatory and auditable internal controls within the IT organization has affected IT governance. The propositions were derived from both considering the primary impact of implementing internal controls and the secondary response from the IT organization and management on how to reduce the perceived negative impact the new regulatory requirements have.

Keywords IT Governance, Sarbanes-Oxley Act, COBIT, Internal Controls, Regulatory Requirements

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 followed.

In an effort to understand the impact SOX has had on public corporations, the U.S. Securities and Exchange Commission (SEC) hosted an all day roundtable discussion on April 13, 2005 about the implementation of the internal control reporting provision. In addition, the SEC invited written submissions from the public regarding the internal controls requirement that are mandated by Section 404 of the Act.

Since the implementation of SOX, there has been extensive research published in the area of accounting and auditing, but limited research published in the area of information systems and impact the legislation is having on IT governance. Publications in IS have included papers on the following topics: addressing the data reliability in accounting systems (Krishnan, Peters, Padman and Kaplan 2005), how ERP systems can support the mandates of SOX (Brown and Nasuti 2005), and what impact SOX has had on IT project management (Leih 2005). The goal of this paper is to begin to build a theoretical base by reporting on a grounded theory research study based on how the internal control requirements mandated by SOX are affecting IT governance.

The study uses a multitude of statements from corporations, associations, and individuals who have commented on their experiences implementing SOX's internal controls requirements. The theoretical base provided in this paper should help in the development of future studies as the research community begins to investigate how regulatory initiatives impact IT governance. This paper will provide an overview of the Sarbanes-Oxley Act and its key sections mandating internal controls, provide an overview of the COSO and COBIT frameworks (which provide guidance in implementing internal controls), and report on the results of a grounded theory research study analyzing the written submissions from the public to the SEC on the implementation of internal controls.

BACKGROUND

The Sarbanes-Oxley Act

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 report. To do this, the Act mandates that control processes are put into place over financial reporting and that the CEO and CFO must attest that they have reviewed these controls and that they are working.

Section 302 of the Act, Corporate Responsibility for Financial Reports, mandates that CEOs and CFOs attest to the accuracy of their company's quarterly and annual reports (Dietrich 2004). 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. Asses 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).

With all its sweeping changes, much of the details on how to comply with the Act were left up to the Securities and Exchange Commission. The SEC, together with the Public Company Accounting Oversight Board (PCAOB), has defined its opinion of how public companies should comply with Sarbanes-Oxley. Most organizations considered the original internal audit standards provided by PCAOB in 2003 to be vague, but 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" (Public Company Accounting Oversight Board 2004). This briefing helped to clarify the standards that should be used when auditing a company's internal controls.

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 that supports 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 followed (IT Governance Institute 2004).

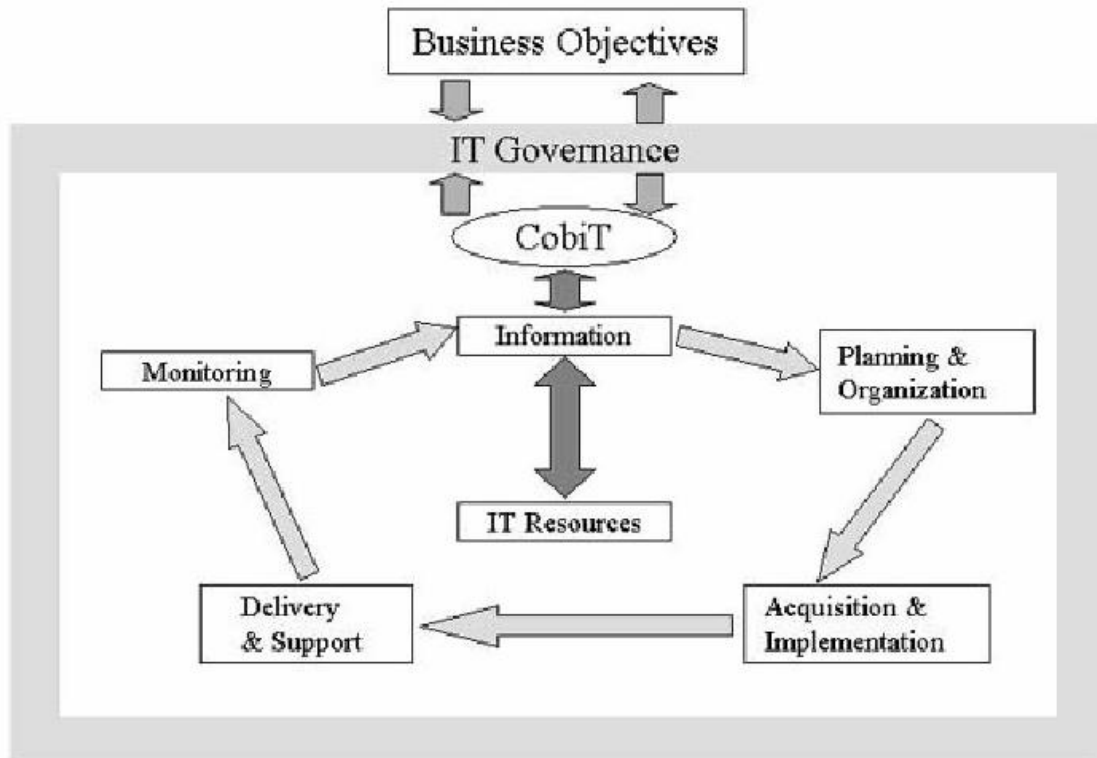
COSO

The Committee of Sponsoring Organizations of the Treadway Commission (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 Sarbanes-Oxley nor 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). According to the COSO framework, internal controls consist of five interrelated components: 1) Control Environment, 2) Risk Assessment, 3) Control Activities, 4) Information and Communication, and 5) Monitoring (COSO 2005).

The components of the COSO framework establish the overall guidelines that enable 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 should 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). However, the IT control objective know as COBIT is considered particularly useful and aligns with the spirit of the Sarbanes-Oxley requirements (IT Governance Institute 2004).

COBIT

Control Objectives for Information and Related Technology (COBIT) were developed by the IT Institute as a standard for IT governance. Founded as a not-for-profit organization in 1998 by the Information Systems Audit and Control Associations (ISACA), the IT institute is dedicated to creating and sharing better practices for IT governance (IT Governance Institute 2004). COBIT establishes IT governance as a structure of relationships and processes that controls 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 (see Figure 1). The four domains are 1) planning and organization, 2) acquisition and implementation, 3) delivery and support, and 4) monitoring (IT Governance Institute 2000).



Source: ISACA

Figure 1: The COBIT framework

Each control objective in the COBIT framework can be regarded as a separate process that is established to create the overall IT governance within the corporation. These control objectives can be mapped to the COSO components to meet the internal control requirements of Sarbanes-Oxley. Figure 2 demonstrates how COSO and COBIT frameworks can be overlaid to sections 302 and 404 of the Sarbanes-Oxley Act (IT Governance Institute 2004).

The SEC and PCAOB have provided little guidance to an 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 controls requirements specified in Sarbanes-Oxley (IT Governance Institute 2004)) the impact to the IT organization is worth researching. The propositions presented in this paper will address how the implementation of internal controls mediated by Sarbanes-Oxley impacts IT governance.

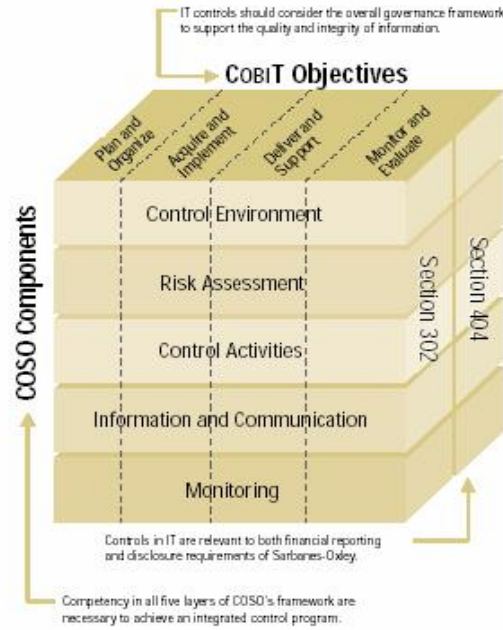


Figure 2: COSO/COBIT overlay matrix

METHODOLOGY

Grounded theory (GT) is a qualitative research method used to develop theory that is based on data systemically gathered and analyzed in an iterative fashion (Strauss and Corbin 1998). The GT approach has gained popularity and acceptance in the information systems research field since Glaser and Strauss published their work in 1967 (Glaser and Strauss 1967). Most grounded theory research studies follow a traditional approach of gathering field data through an iterative process by using surveys, observation notes, and directed interviews (Creswell 1998). According to Creswell, the data that is gathered needs to be of sufficient amount to saturate the area of analysis. This technique derives one or more theories or propositions around the research topic. The analysis of data is completed through an iterative coding process consisting of three coding steps.

The first step, open coding, is an analytical process in which concepts, and their corresponding properties and dimensions, are discovered and identified in the data. Sufficient review of the data during open coding is required to refine each category and property until no further insights are obtained. The second step, axial coding, is the process of relating categories and properties to the central phenomenon in order to derive causal relationships and the context and conditions in which these relationships occur. The term “axial” is used because coding occurs around the axis of a category. The final step, selective coding, is the process of intergrading and refining the relationships discovered in axial coding to form a “story line” and to derive one or more propositions (Creswell 1998).

Studies of the traditional grounded theory approach in information systems research, where data is gathered through directed interviews, have been used to analyze the impact of CASE tools (Orlikowski 1993), the development of requirements documentation (Power and Moynihan 2003), and the use of electronic data interchange (Crook and Kumar 1998). However, there are examples of published GT research that have used data collected from other sources besides the directed interview approach. Goede and De Villiers’ study, “Methodologies in IS practices” primarily used observation notes from a field study (Goede and De Villiers 2003). Sarker, Lue and Sahay’s study, “Virtual Team Development” used communication transcripts and interview notes (Sarker, Lau and Sahay 2001). Fitzgerald, Simon and Thomas’ study, “Strategies students use to trace code” used written transcripts of students thinking aloud while they performed problem solving exercises when evaluating program source code (Fitzgerald, Simon and Thomas 2005). This study follows the less traditional approach by using statements sent to the SEC from a multitude of corporations and associations. These statements regarded their experiences and reactions to the implementation of internal controls to meet SOX mandates.

Data Collection

In February 2005, the SEC announced that it would be holding a public roundtable to discuss the implementation of the internal control requirements mandated by Section 404 of the Sarbanes-Oxley Act. Several members of the SEC and PCAOB, along with representatives from publicly held corporations and accounting organizations, contributed to this roundtable that was held on April 13, 2005. The full transcript of the roundtable is available on the SEC's website at www.sec.gov/spotlight/soxcomp/soxcomp-trans.txt. In addition to this roundtable, the SEC solicited written statements from the public on the implementation of Section 404. The collection of these statements is also available on the SEC's website at www.sec.gov/news/press/4-497.shtml. At the time this study was conducted, there were 248 written submissions that were sent to the SEC and posted on the website. These written submissions provided the data used to develop theories on how the mandatory implementation of internal controls in IT organizations is changing IT governance.

Data Analysis

Of the 248 submissions posted on the SEC's website, an analysis revealed that 36 of them had specific statements referring to the implementation of internal controls in the IT organization. These 36 submissions were from a wide variety of corporations, associations and individuals. To provide an idea of the diversity of organizations that submitted the 36 statements, a summarization of the distribution is provided in figure 3. Some of the companies that submitted statements that were used in this study included PepsiCo, Pfizer, Ernst & Young, Intel, Microsoft, and Price Waterhouse Coopers.

Size of the Organization		Type of Organization		Business Sector	
24	Large	22	Corporations	2	Manufacturing
8	Small and Medium	10	Associations	6	Financial
4	Individual	4	Individuals	4	Utility
				2	Food
				1	Health Care
				8	Auditing
				3	Technical
				10	Services

Figure 3: Summary of submission distribution

Open coding

In open coding, statements from the 36 submissions were copied into the ATLAS.ti software tool and coded into major categories. In total, 171 statements (typically paragraphs) were identified and coded into one or more categories. Each category was refined and appropriate properties were then assigned and dimensionalized as suggested by Strauss and Corbin (1998). A total of four categories were identified: Internal Controls, Implementation Impacts, Operational Responses, and Managerial Responses. Figure 4 provides a summary of these categories and their respective properties and dimensions.

Internal Controls represents the implementation of key controls and the frameworks that define them and assesses whether they meet the requirements mandated by the Act. Properties of the category include 1) the broad scope of impact the internal controls have, 2) the limited implementation guidance by auditors, and 3) the detailed level of abstraction in which key controls are being defined. An example of a statement coded to this category is: *“Our auditors applied the full and literal CobiT framework to our information technology (“IT”) internal controls. This approach was excessive and resulted in unnecessary utilization of internal resources and higher external costs.”*

Implementation Impacts represents the type of effect the implementation of the internal controls has on the IT organization. The properties for this category are 1) the increase in costs, 2) the increase in testing, 3) the increase in documentation, 4) the high effort required to implement internal controls, 5) the new maintenance activities required, and 6) the disproportionate level of impact on small and medium sized corporations. An example of a statement coded to this category is: *“Effort required to achieve compliance is significant and beyond initial expectations. The efforts expended will improve the operations on the company in some ways, but the estimated benefit would be in the range of 15% to 20% of the total cost incurred.”*

Operational Responses represents those adjustments to current activities that the IT organization had to make or intends to make to meet SOX requirements. Properties of this category include 1) simplifying operational complexities, 2) centralizing operations, 3) consolidating system architectures, 4) delaying implementation of new systems or system upgrades to allow new controls to mature prior to annual audits, and 5) automating controls with IT. An example of a statement coded to this category is: *“Many companies are delaying the implementation of significant IT projects by six to nine months solely because of the documentation and testing requirements of Section 404. They also expect this problem to persist, and predict that they will be able to make major systems changes only in the first half of their fiscal years going forward.”*

Managerial Responses represent those reactions or changes that management has made as a result of the new internal controls requirements. Properties of this category include 1) the greater level of project management now required, 2) the perceived low return on investment to implement internal controls, and 3) the greater level of management’s awareness of existing internal controls and their effectiveness. An example of a statement coded to this category is: *“We have learned that we have historically relied upon experienced individuals with integrity to prepare and review financial statements. Under SOX, we have learned that “if it isn’t documented, it isn’t done.” Our documentation has improved significantly; however, we suspect that the increased cost is not worth the benefit to be received.”*

Category	Properties	Dimensions
Internal Controls	Scope of Impact	Broad ... Narrow
	Implementation Guidance	Extensive ... Limited
	Level of Abstraction	Abstract ... Detail
Implementation Impact	Cost	Increase ... Decrease
	Testing	Increase ... Decrease
	Documentation	Increase ... Decrease
	Implementation Effort	High ... Low
	Maintenance Effort	High ... Low
	On Small Companies	High ... Low
Operational Responses	Operational Complexity	Simple ... Complex
	Organization Architecture	Centralize ... Decentralize
	Systems Architecture	Consolidate ... Expand
	System Implementation / Upgrade	Facilitate ... Delay
	Automate Controls with IT	Increase ... Decrease
Managerial Responses	Project Management	Greater ... Lesser
	Perceived ROI	High ... Low
	Management Awareness	Greater ... Lesser

Figure 4: Summary of open coding

Axial Coding

In axial coding, the categories and their dimensionalized properties were evaluated and assigned to various relationships. Several iterations were performed to determine how the categories related to one other and how best to represent these relationships to derive proposition during selective coding. To help organize how the categories interrelate, a causal model was developed to assist in the integration and organization of the data (Strauss and Corbin 1998). Each property within a category was evaluated within the context of the statements which were used in open coding to determine how the property best fit into the causal model. Four groupings were defined within the causal model, and the properties within each category were assigned to the grouping that best represented the relationship that it had with other properties. Figure 5 is a graphical representation of the results of axial coding.

The first group is the Causal Conditions. No properties identified during open coding were assigned to this group. Rather, this group represents the focus of the study: “How is the mandatory implementation and auditing of internal controls affecting IT governance?” The specific elements of this group are 1) the mandatory implementation of internal controls, 2) the mandatory internal auditing of internal controls, and 3) the mandatory external auditing of internal controls.

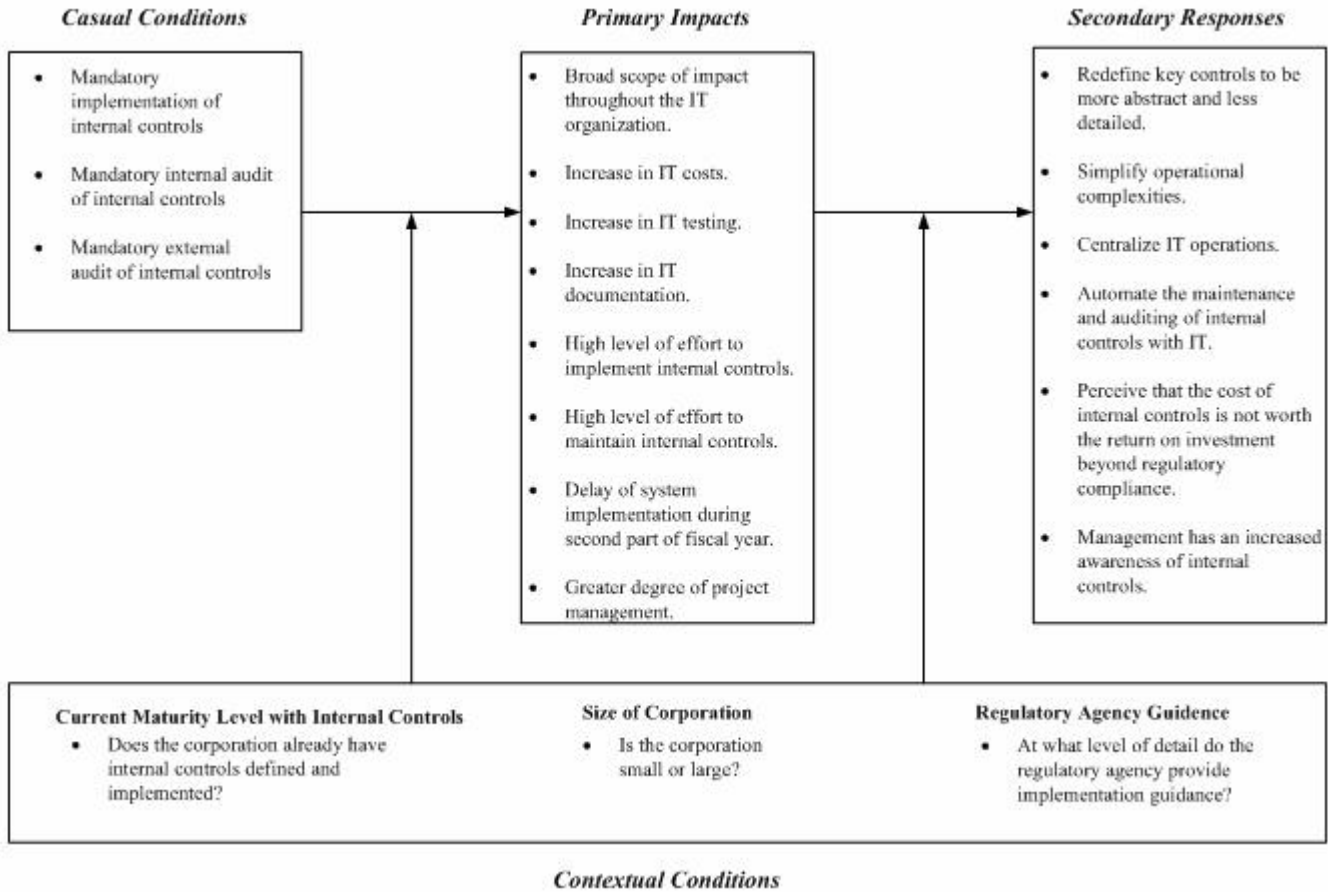


Figure 5: Axial coding: Primary impacts and secondary responses of mandatory internal control implementation

The second group contains the properties that were identified as Primary Impacts resulting from the implementation of mandatory internal controls. These properties are 1) the scope of the impact throughout the IT organization, 2) the increase in cost to implement and manage IT operations, 3) the increase in testing required to implement new IT, 4) the increase in documentation required for internal and external auditing, 5) the high level of effort required for the initial implementation of internal controls, 6) the high level of effort required to maintain the establishment of internal controls, 7) the delayed implementation of new systems during the later part of the fiscal year, and 8) the greater degree of project management that is required to ensure internal controls are being followed.

The third group contains the properties that were identified as Secondary Responses to primary impacts. These secondary responses were identified and isolated apart from the primary impact properties because the data supported the notion that these properties had a higher causal relationship with the primary impact properties than with the initial casual conditions. These secondary responses were 1) the need to redefine key controls to be more abstract and less detailed, 2) the need to simplify operational complexities, 3) the need to centralize IT operations, 4) the need to automate the maintenance and auditing of internal controls, 5) the perception that mandated internal controls have a low return on investment, and 6) the increased awareness of management of what internal controls are in place and how effective they are.

The fourth group contains the properties that were identified as Contextual Conditions because of their contextual influence on the relationship between the “initial casual conditions and the primary impacts” and “the primary impacts and the secondary responses.” That is, these properties influenced the degree of impact or response that the properties in groups two and three had to the dimensions identified in the categories. These properties were identified as 1) the maturity level of internal controls the IT organization had prior to the implementation of mandatory internal controls, 2) the size of the corporation, and 3) the guidance provided by the regulatory agency that is mandating the implementation of internal controls.

Selective Coding

In selective coding, the relationships identified in axial coding were reviewed and placed into a storyline narrative as a set of propositions as suggested by Creswell (1998). The propositions were again refined through an iterative process and evaluated against the original statements to provide additional rigor and to ensure that they are grounded in the data. This step resulted in the development of seven propositions that can be used in future research as theories and hypotheses.

RESEARCH RESULTS

The following are the propositions that suggest how implementing mandatory internal controls affect IT governance based on the coding process. In addition to each proposition are quotes extracted from various statements that support the propositions.

P1: Even though the implementation of internal controls mandated by SOX is limited to the financial reporting processes, the scope of impact will affect a broad range of IT processes.

P1-1: The breadth of the scope of impact is inversely proportional to the regulatory agency's guidance in the implementation of the internal controls. That is to say, the less guidance provided by the regulatory agency, the greater the breadth of impact.

There has been little to no guidance issued surrounding the implementation of the Standard's references to IT controls by the SEC or PCAOB. Control Objectives for Information and related Technology ("COBIT"), issued by the IT Governance Institute, and now in its third edition, is increasingly accepted internationally as generally sound practices for control over information, IT and related risks. However, the framework for COBIT, which was largely recommended and imposed by consulting and auditing firms, extends beyond the scope of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission framework for financial reporting. This has resulted in an expansion of the scope of general IT controls into IT operational areas and details probably not envisioned by the Sarbanes-Oxley Act.

P2: The implementation of both mandatory and auditable internal controls will increase the cost to implement and maintain systems, increase the amount of testing to implement and maintain systems, and increase the amount of documentation to implement and maintain systems.

P2-1: The increase in cost, testing, and documentation will be inversely proportional to the organization's maturity level with internal controls before the implementation of the mandatory internal controls. That is to say, if an organization has experience with internal controls and already has them implemented, additional internal controls will have a lesser impact than if an organization has no experience with internal controls and does not have any implemented.

External auditors are requiring companies to document and test controls that do not impact the financial statements. For example, many companies are now required to document every call that their help desks receive for technical support and auditors are now ensuring that every employee has a personnel performance evaluation. Having those procedures in place may be good business practice, but they do not ensure the accuracy of a company's financial statements. The all-inclusive approach applied by external auditors to IT controls has resulted in massive cost for little value. It is clear that in the area of IT controls, auditors have spent most of their time on controls that have a very tangential, if any, impact on the financial reporting process and have focused on business risk decisions that do not impact the accuracy of the financial statements.

P3: Mandatory and auditable internal controls will require a high level of effort to implement, a high level of effort to maintain, and a greater degree of project management.

P3-1: The effort required to implement and maintain internal controls will be inversely proportional to the organization's maturity level with internal controls before the implementation of the mandatory internal controls. That is to say, if an organization has experience with internal controls and already has them implemented, it will require less effort than if an organization has no experience with internal controls and does not have any implemented.

It was a massive effort by people throughout the company. We need to work on a sustainable process to reduce the required annual effort.

P4: The implementation of mandatory and auditable internal controls on new systems will delay the implementation of the new system until the first part of the organization's fiscal year.

Because COSO requires an internal control to be "mature" to be considered effective, it is not practical to implement major new IT systems in the third and fourth fiscal quarters because the control will not be mature. Additionally, with new systems there are always post-implementation bugs to be fixed, and if they are implemented late in the year, then there will not be enough time to remediate any bugs that are discovered, and have the new control mature before year end.

P5: The high level of effort required to implement and maintain mandatory internal controls will cause IT management to simplify operational complexities, centralize IT operations, and automate the maintenance and auditing of internal controls with IT systems.

The cost of compliance is exacerbated in a decentralized financial and IT environment.

P6: The smaller the organization, the smaller perceived return on investment to implement and maintain internal controls.

In practice, the standards being implemented by the PCAOB and the "Big 4" do not differentiate between the stages of a company's development, resulting in a massive and disproportionate burden for small companies.

P7: The greater degree of project management required to implement and maintain internal controls, the greater awareness management will have on internal controls.

The primary benefits to the Company from implementation of the Act have been significantly increased attention to information technology general controls, increased definition of business processes, creation of updated desk procedure documentation that can be used for training purposes, the creation of a more entity-wide awareness level as to design, operation and importance of internal controls over financial reporting and the specific identification of our "portfolio" of controls that we can look to on an ongoing basis to evaluate, update and strengthen controls.

RESEARCH REMARKS

This grounded research study has attempted to derive a series of propositions on how regulatory requirements, like the internal controls requirement mandated by the Sarbanes-Oxley Act, affect IT governance. This study can benefit researchers because it creates a theoretical foundation to support future research in this area. The propositions will need to be tested in a much broader population to further verify their validity. Empirical analysis through surveys and directed interviews can verify whether the primary and secondary impacts are in fact resulting from the introduction of mandatory and auditable internal controls. In addition, future research should consider whether the impacts revealed in this study are impacting IT governance in private and government organization not held under Sarbanes Oxley. That is to say, "Are the internal controls mandated by Sarbanes Oxley in public corporations being adopted as best practices in private and government organizations?"

This study can also benefit practitioners by providing a context in which to evaluate their own experiences with internal controls implementation. If the propositions in this study are found to be generalizable to other regulatory initiatives, practitioners can implement secondary responses more quickly in order to reduce the influence of the primary impacts. In addition, regulatory agencies can use these findings to create legislation in such a way as to minimize some of the perceived negative impacts realized in the implementation of the Sarbanes Oxley Act.

This study may have its limitations, as it deviated from the traditional data collection method of directed interviews at a specific site or sites. Directed interviews allow the researcher to derive initial concepts, re-interview informants and refine concepts in an iterative manner until no new concepts are realized. The limitation of this study is the researcher's inability to interview the corporations and associations with refined questions to determine if the data contribution has truly been saturated. The approach used in this study, however, has been used in other published research, and by obtaining a large initial data base of information, the need for iterative data collection is diminished. In addition, the propositions derived by

this study may not be generalizable to internal controls requirements that will not be audited. It is likely that the auditing and public reporting requirement of SOX is the key reason internal controls have such a great impact on IT governance.

REFERENCES

1. Brown, W., and Nasuti, F. (2005) What ERP systems can tell us about Sarbanes-Oxley, *Information Management & Computer Security*, 13, 4, 31-327.
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. COSO (2005) Internal Control Issues in Derivatives Usage - Executive Summary, www.coso.org, www.coso.org/publications/executive_summary_derivatives_usage.htm, accessed: 12/10/05
4. Creswell, J. *Qualitative inquiry and research design: Choosing among five traditions* Sage Publications, Thousand Oaks, California, 1998.
5. Crook, C.W., and Kumar, R.L. (1998) Electronic data interchange: a multi-industry investigation using grounded theory, *Information & Management*, 34, 2, 75-89.
6. Damianides, M. (2005) Sarbanes-Oxley and IT Governance: New Guidance on IT control and Compliance, *Information Systems Management*, 22, 1, 77-85.
7. 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
8. Fitzgerald, S., Simon, B., and Thomas, L. (2005) Strategies that Students Use to Trace Code: An Analysis in Grounded Theory, ICER '05, October 1-2, 2005, Seattle, Washington, 69-80.
9. Glaser, B., and Strauss, A. *The discovery of grounded theory: Strategies for qualitative research.*, Chicago: Aldine., 1967.
10. Goede, R., and De Villiers, C. (2003) The Application of Grounded Theory as Research Methodology in studies on the use of Methodologies in IS Practices, Proceedings of SAICSIT, 2008-2217.
11. IT Governance Institute (2000) COBIT 3rd Edition - Executive Summary, www.isaca.org, accessed: 2/25/2005
12. IT Governance Institute (2004) IT Control Objectives for Sarbanes-Oxley, www.itgi.org, accessed: 2/25/05
13. Krishnan, R., Peters, J., Padman, R., and Kaplan, D. (2005) On Data Reliability Assessment in Accounting Information Systems, *Information Systems Research*, 16, 3, 307-326.
14. Leih, M. (2005) The Impact of the Sarbanes-Oxley Act on IT Project Management - A Case Study, AMCIS 2005, August 11-14, 2005, Omaha, NB, 854-857.
15. Orlikowski, W.J. (1993) CASE tools as organizational change: Investigating incremental and radical changes in systems development, *MIS Quarterly*, 17, 3, 209, 232.
16. Paulk, M.C. (2004) Surviving the Quagmire of Process Models, Integrated Models, and Standards, ASQ: Annual Quality Congress Proceedings, Toronto, Canada, 429-437.
17. Power, N., and Moynihan, T. (2003) A Theory of Requirements Documentation Situated in Practice, SIGDOC, October 12-15, 2003, San Francisco, California, 86-92.
18. Public Company Accounting Oversight Board (2004) Auditing Standard No. 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements. Auditing Standard No. 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements
19. Sarker, S., Lau, F., and Sahay, S. (2001) Using an Adapted Grounded Theory Approach for Inductive Theory Building about Virtual Team Development, *The DATA BASE for Advances in Information Systems*, 32, 1, 38 - 56.
20. 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
21. Strauss, A., and Corbin, J. *Basic of qualitative research: techniques and procedure for developing grounded theory, second edition* Sage Publications, 1998.
22. U.S. Congress (2002) The Sarbanes-Oxley Act of 2002. House of Representatives 3763, Public Law 107-204, 107th Congress