JOURNAL OF INFORMATION SYSTEMS
Vol. 25, No. 1
Spring 2011
pp. 185–211

American Accounting Association
DOI: 10.2308/jis.2011.25.1.185

Information Security and Sarbanes-Oxley Compliance: An Exploratory Study

Linda Wallace
Virginia Polytechnic Institute and State University

Hui Lin
DePaul University

Meghann Abell Cefaratti
Northern Illinois University

ABSTRACT: The Sarbanes-Oxley Act of 2002 (SOX) created a resurgence of organizational focus on internal controls. In this study, we examine the extent to which the information technology (IT) controls suggested by the ISO 17799 security framework have been integrated into organizations' internal control environments. We collected survey data from 636 members of the Institute of Internal Auditors (IIA) on the current usage of IT controls in their organizations. In addition to identifying the most and least commonly implemented IT controls, the survey results indicate that control implementation differences exist based on a company's status as public or private, the size of the company, and the industry in which the company operates. Training of internal auditors and/or IT personnel is also associated with significant differences in implemented controls. We discuss the implications of our research and offer suggestions for future research.

Keywords: information security; internal control; ISO 17799; Sarbanes-Oxley.

Data Availability: A complete copy of the survey and the data collected are available upon request.

I. INTRODUCTION

The Sarbanes-Oxley Act (SOX) was enacted in 2002 by Congress to protect shareholders and the general public from fraudulent corporate practices and accounting errors and to maintain auditor independence. SOX raised the standards for financial reporting in public companies to increase transparency, accountability, and reliability of financial information. It has

We thank the anonymous reviewers for their constructive suggestions and the Editor, Paul John Steinbart, for the time and effort he put into helping us improve our original manuscript. We acknowledge Donna Batten for her assistance in distributing the survey electronically and thank the members of the IIA for their participation. We acknowledge the summer grant program through the Pamplin College of Business at Virginia Polytechnic Institute and State University for partial funding of this project.

Published Online: March 2011

become strategically important for organizations who are striving to meet SOX requirements to select and implement appropriate information security procedures in order to manage internal controls effectively.

Information security refers to all of the steps taken to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (United States Code 2008). Information technology (IT) is a vital component of information security. IT refers to any technology that helps to manage, process, or disseminate information, such as some combination of computer hardware, software, and associated communications systems. Because of the close link between financial reporting, information security, and IT, most organizations have implemented a variety of IT controls to comply with SOX regulations (Damianides 2005).

Although the primary focus of SOX is the accuracy of an organization's financial information and the effectiveness of internal controls, SOX does not explicitly address how IT should be incorporated into the SOX compliance process. Furthermore, the SEC offers little guidance on the use of IT, allowing for inconsistent interpretation of the scope and nature of IT involvement in SOX compliance (Brown and Nasuti 2002). A 2003 Gartner survey showed that most organizations do not require personnel with IT experience to participate in compliance efforts (Leskela and Logan 2003). Others suggest that even if IT professionals are involved in the compliance process they may not be well-versed in the intricacies of internal control, leading to communication, implementation, and effectiveness issues (ITGI 2006).

ISO 17799, the International Standard for the Code of Practice for Information Security Management, provides a detailed list of controls that can be used for establishing an information security program. As a result of the lack of formal guidance regarding how to incorporate IT into a SOX compliance effort, ISO 17799 has been adopted by many organizations as a framework for implementing and maintaining information security. Prior research has suggested that organizations who implement the controls outlined by ISO 17799 will be "well on their way" toward complying with the security mandates of SOX (Haworth and Pietron 2006).

Researchers have noted that information security is implicit in the requirements of SOX, and that the relationship between information security and SOX compliance is likely to strengthen over time (Anand 2008). Prior research, however, has not examined the IT controls that organizations are using in order to achieve SOX compliance. This is an important first step before we can determine how best to use an information security framework to support SOX compliance.

The objective of this exploratory study is to empirically investigate the IT controls that organizations have implemented. To accomplish this objective, we developed and administered a survey to internal auditors to identify which specific IT controls are used in their organizations. Six-hundred-thirty-six internal auditors responded. We identified the ten most and ten least commonly implemented controls and found that organizations may differ in their implementation of certain IT controls based on whether they are a public or private organization, how many employees they have, the industry to which they belong, and the level of training administered to IT and audit personnel. The results presented can be used as the foundation for future research to link IT controls, information security, and SOX compliance in a larger theoretical context.

The remainder of this article is organized as follows. In the next section, we provide an overview of SOX and ISO 17799. In the third section, we describe the research method. The fourth section presents the results, and the article concludes with a discussion of the implications of our research and opportunities for future research.

II. SARBANES-OXLEY COMPLIANCE AND ISO 17799

Sarbanes-Oxley Compliance

Prior research has identified several sections of SOX for which IT has the highest relevance. These include Sections 302, 404, 409, and 802 (Brown and Nasuti 2002; Garcia 2004; Weidenmier and Ramamoorti 2006). Section 302 requires corporate officers to make representations related to internal controls, company policies, and fraud procedures. Because CEOs and CFOs rely on information prepared by others, it is common for them to request information and certification from those individuals (e.g., CIOs) who are directly responsible for preparing it (CIOInsight 2004). As a result, employees and managers with IT expertise are often involved with SOX compliance, as they are asked to provide proof that the automated portions of financial reports have appropriate controls and that computer-generated reports are accurate and complete (Kaarst-Brown and Kelly 2005).

Section 404 requires companies listed on the U.S. stock exchange to use an internal control framework and to perform an annual assessment of the effectiveness of these controls. Many of these frameworks suggest controls that may be implemented via IT.

Section 409 addresses the critical need to disclose information regarding a firm's financial condition on a "rapid and current basis" to ensure that changes, particularly negative ones, are immediately reported to shareholders (U.S. House of Representatives, Committee on Financial Services 2002). The accuracy and timeliness of financial reporting often relies on a well-controlled IT environment that facilitates the reliable communication of information to interested parties (Lazarides 2007).

Section 802 requires authentic and immutable record retention. Organizations must create and maintain corporate records in a cost-effective manner in order to satisfy the SOX requirement that all business records, including electronic records and electronic messages, must be saved for not less than five years. This has a direct impact on IT in terms of data management, data and system security, and business recovery practices (Brown and Nasuti 2002).

Therefore, organizations face the challenge of integrating IT practices with SOX compliance efforts (Damianides 2004; Weidenmier and Ramamoorti 2006). Organizations need guidance to help them develop the appropriate strategies for integrating IT controls in their SOX compliance efforts. This research, which reports on the IT controls that have been implemented in organizations, is a first step in building these strategies.

Information Security Frameworks

Some organizations choose to use an information security management framework in an attempt to structure their efforts to protect their systems and data. Research has shown that applying a security framework can be an effective way to protect an organization's information assets (e.g., Da Veiga and Eloff 2007; Ma et al. 2008; Tang 2008). Common frameworks include the COSO framework, COBIT, and ISO 17799.

In this study, we chose to focus on the ISO 17799 framework of IT controls in order to examine current security practices for the following reasons. First, ISO 17799 directly focuses on information security, while other frameworks have a broader focus. COSO is a model for corporate governance (Harris 2006) that establishes a general framework for how organizations can control and manage their internal processes, specifically financial processes. Although COSO can be applied to IT, it is not designed to focus on controls specific to IT (Linkous 2008). COBIT was intended to be a high-level governance framework (Greenfield 2007) and focuses on many areas of IT governance, not just on information security (von Solms 2005). ISO 17799, on the other hand, is an international standard that contains best practices specifically for implementing information security management controls (ISACA 2005).

Second, the ISO framework is very detail oriented. While COSO and COBIT outline requirements for various security structures and controls, ISO 17799 provides the details on how to develop and implement these components (Harris 2006). COBIT suggests to organizations "what" they should monitor and control (Greenfield 2007), but is not very detailed in terms of providing guidelines for "how" to implement security to achieve control (von Solms 2005).

Third, Haworth and Pietron (2006) mapped the 124 components of ISO 17799 to SOX guidelines and focused on identifying the IT controls that were relevant to SOX. They suggested that almost all of the 124 IT controls described by ISO 17799 have direct relevance for companies striving for compliance with SOX and they called for future research to further develop a set of guidelines that could help to bring companies into reasonable compliance with the mandates of SOX.

In 2005, ISO 17799 was updated and re-released as two related standards: ISO 27001 and ISO 27002. ISO 27001 contains a list of management controls that an organization needs to address in order to audit and certify their Information Security Management System (Carlson 2008). ISO 27002 is analogous to the original ISO 17799 in that it contains a list of operational controls that an organization should consider in order to develop a comprehensive Information Security Plan (Carlson 2008). The content of ISO 27002 has remained largely the same as the original content of ISO 17799 (Praxiom Research Group Limited 2008). We based our survey on ISO 17799 in order to build on the previous research by Haworth and Pietron (2006); however, future research may follow the terminology of ISO 27002.

In summary, because the objective of our study is to better understand the current state of practice regarding which IT controls organizations are using, we chose to use the ISO 17799 framework as a basis for developing our survey instrument and to guide our efforts in examining the IT controls that may eventually help companies achieve SOX compliance. The next section provides more detail about the components of ISO 17799 and the IT controls that it recommends organizations use for information systems security.

ISO 17799

ISO 17799 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. Specifically, it addresses ten areas of security in an organization: Security Policy, Organizational Security, Asset Classification and Control, Personnel Security, Physical and Environmental Security, Communications and Operations Management, Access Control, Systems Development and Maintenance, Business Continuity Management, and Compliance (ISO 2005). The ten categories focus on different security control areas and are decomposed into 124 recommended IT controls. Each of the ten categories are shown in Table 1 and explained in more detail in the following paragraphs.

The focus of Security Policy is the creation of implementable security policies that are applicable to the organization and its information security needs. Organizational Security emphasizes the level of management's awareness and activity to establish an overall information security infrastructure for the organization. To successfully address the area of Asset Classification and Control, an organization must "maintain appropriate protection of organizational assets" (Calder and Watkins 2002, 91). Controls over organizational assets include identifying the owner of both physical assets as well as information assets (i.e., databases, data files, and financial and accounting information). To achieve compliance with Personnel Security, the organization should strive to reduce the risks of loss of information through error, fraud, or misuse of facilities (Calder and Watkins 2002). The area of Physical and Environmental Security focuses on the controls necessary to protect physical assets and emphasizes planning for the protection of critical information assets by physically securing information-processing facilities.

The section of ISO 17799 entitled Communications and Operations Management is extensive; encompassing operational controls such as segregation of duties, planning for forecasted capacity requirements, managing the network, properly disposing of media, and electronic commerce and electronic mail security. The Access Control section of ISO 17799 outlines controls to properly protect access to an organization's information, such as controls required to combat hacker attempts and other malicious attempts to access organizational networks and information.

TABLE 1

ISO 17799 Category Descriptions[a]

Category Number	Category Name	Category Description	Number of Survey Items
3	Security Policy	Create implementable security policies.	0
4	Organizational Security	Establish an overall information security infrastructure for the organization.	1
5	Asset Classification and Control	Protect organizational assets, including maintaining an inventory of organizational assets.	2
6	Personnel Security	Reduce the risks of loss of information through human error, fraud, or misuse of facilities.	5
7	Physical and Environmental Security	Plan for the protection of critical information assets and other physical assets.	20
8	Communications and Operations Management	Implement operational controls such as segregation of duties, planning for forecasted capacity requirements, managing the network, properly disposing of media, and electronic commerce and electronic mail security.	38
9	Access Control	Protect access to the organization's information.	25
10	Systems Development and Maintenance	Incorporate information security procedures, such as encryption and digital signatures, into the information system from the beginning.	13
11	Business Continuity Management	Develop a plan to address the business's ability to function with minimal interruption when a major disaster occurs.	0
12	Compliance	Avoid breaches of any criminal or civil law, as well as any statutory, regulatory, or contractual obligations, and of any security requirements.	4

[a] The first two sections of 17799 discuss the scope of the Standard (Haworth and Pietron 2006). Beginning with Section 3, the Standard addresses ten categories of controls.

Systems Development and Maintenance focuses on the approach necessary to design information security procedures that should be incorporated into the information system from the beginning. Such controls include encryption, digital signatures, and evaluation of software products prior to usage. The section labeled Business Continuity Management addresses planning issues for major disasters that may result in a disruption to the business's activities. The items outlined in this section are intended to minimize the impact of disasters on the business's activities. The last section of ISO 17799, the Compliance section, "is intended to ensure that the organization avoids breaches of any criminal or civil law, as well as any statutory, regulatory or contractual obligations, and of any security requirements" (Calder and Watkins 2002, 271). The organization must identify applicable legislation with which it must comply. Areas to consider include legislation such as the Sarbanes-Oxley Act of 2002. The ten categories of ISO 17799 provide a comprehensive framework of controls and activities intended to help organizations properly and effectively protect their information systems.

III. RESEARCH METHOD

Survey Development

To better understand how organizations are using IT controls, we developed a survey to gauge the participants' perceptions of the prevalence of specific IT controls, as outlined by ISO 17799, in their organizations. To develop the questions, each of the authors independently reviewed the components of ISO 17799 and composed items that captured the intent of each of the 124 controls. The questions were designed to assess the many ways that IT may be used to implement the ten areas of information security described by ISO 17799. Duplicate questions were deleted and the remaining items were reworded in an iterative manner through discussions between the authors in order to develop a list of 108 questions that clearly and comprehensively covered the breadth and depth of the ISO 17799 components. Table 1 shows the number of items developed for each ISO 17799 category.

Two of the categories do not have any survey items because the concepts addressed by ISO 17799 for these two categories did not relate to controls that could be implemented using IT. Rather, the concepts in these categories related to policies and non-technical procedures (e.g., business continuity planning, etc.) that the organization should have in place in order to manage their security procedures. For example, while business continuity planning certainly has an IT component, category 11 of ISO 17799 is limited to a discussion of management's development of these plans. The IT concepts related to business continuity planning (i.e., backups, etc.) are covered by other ISO sections. Therefore, our survey does include IT controls related to business continuity planning even though they are not specifically identified as category 11 controls in Table 1.

For the remaining categories, we constructed items relating to areas where IT could be used to address security. The resulting list of 108 items was reviewed by five subject-matter experts with extensive experience in IT research and survey design and their feedback was used to further refine the items. Appendix A contains a sample of the items used in the exploratory survey and demonstrates how the IT items map to ISO 17799.

In addition to asking questions about IT controls, we asked several questions about employee training. Previous research has indicated that IT employees involved in the SOX compliance process may not always be trained in compliance issues (ITGI 2006). Therefore, we asked the participants to indicate the extent to which the IT personnel in their organizations had received training on SOX compliance and the extent to which their auditors had received IT training. We also asked the participants about the extent to which their organization had achieved SOX compliance. Finally, we asked the participants to answer several questions about their organizations, since it is possible that certain organizational characteristics (industry, number of employees, etc.) could be related to their choice in the IT controls and we wanted to explore possible trends or relationships.

Participants

Emails were sent to members of the Institute of Internal Auditors (IIA) to request their participation in the web-based survey. The IIA has approximately 160,000 members worldwide, although the email survey request only went out to 18,408 members due to language barriers and privacy issues (e.g., members who did not wish to receive emails regarding surveys). Approximately 30 percent of the emails were undeliverable due to normal technological issues (nonworking email addresses, spam filters, etc.), resulting in approximately 13,000 email invitations. A total of 881 members responded to the survey, of which 636 provided complete responses. There were 424 male respondents and 212 female respondents.

Response bias occurs if there are differences in nonrespondents when compared to respondents. Ideally, we would have contacted some of the IIA members who did not respond to the survey in order to assess whether response bias was a problem. Unfortunately we were not able to obtain access to those who did not respond. However, nonrespondents have been shown to resemble late respondents in previous research (Armstrong and Overton 1977), so each respondent was categorized by response time in order to distinguish between the early and late respondents. The first 25 percent of the replies were considered to be early responders, while the last 25 percent were classified as late responders. We used a one-way ANOVA to compare the two groups. We found that there were no significant differences in the early and late respondents in terms of their age, gender, organization size, industry, or response to the question regarding the extent to which their organization had achieved SOX compliance.

The average participant was between 41 and 50 years old and had been employed by their current organization between three and five years. The participants were asked to indicate any certifications that they possessed. The majority of the participants had some type of professional certification. The most common certifications were: Certified Internal Auditor (CIA), Certified Public Accountant (CPA), and Certified Information Systems Auditor (CISA). Table 2 shows the frequency of the certifications possessed by the respondents.

Table 3 shows that Finance/Banking/Accounting, Insurance/Real Estate/Legal Services, and Manufacturing were the industries most commonly represented by the participants. The respondents consisted of 305 employees of publicly traded companies and 331 employees from private organizations. Table 3 also displays the size of the organizations to which the participants belonged, as measured by number of employees.

TABLE 2

Participants' Professional Certifications

Certification	Respondents with This Certification	Respondents with This Certification and No Other Certifications	Respondents with This Certification in Addition to Other Certifications
CPA (Certified Public Accountant)	220	91	129
CFE (Certified Fraud Examiner)	75	11	64
CIA (Certified Internal Auditor)	257	84	173
CFM (Certified Financial Manager)	3	0	3
CMA (Certified Management Accountant)	17	3	14
CISA (Certified Information Systems Auditor)	238	91	147
CISSP (Certified Information Systems Security Professional)	37	3	34
CCP (Certified Computing Professional)	4	0	4
CITCP (Certified IT Compliance Professional)	1	1	0
None	108		

TABLE 3

Industries Represented and Company Size by Number of Employees

	Frequency
Industry	
Business Services/Computer/Network Consulting	15
Education	33
Finance/Banking/Accounting	123
Government Agencies	64
Health/Medical/Dental Services	43
Insurance/Real Estate/Legal Services	79
Manufacturing	75
Not-for-Profit	12
Retailer/Wholesaler/Distributor	39
Transportation	16
Utilities	27
Number of Employees	
Less than 100	26
100 to 499	88
500 to 999	52
1,000 to 4,999	186
5,000 to 9,999	85
10,000 or more	198
Not Sure	1

IV. RESULTS

The results of this study describe the extent to which organizations are implementing IT controls and identify the organizational differences (size, industry, etc.) that might lead to differences in control choices. We also examine the extent to which organizational training of IT employees and/or auditors may influence IT control implementation and/or SOX compliance success.

Most and Least Commonly Implemented Controls

Table 4 presents the ten most commonly implemented controls, while Table 5 presents the ten least commonly implemented controls, according to the respondents. In order to identify the most commonly implemented controls, we combined the "strongly agree" and the "agree" responses for each control because both answers indicate the presence of a control. The controls with the ten highest frequency counts of "strongly agree" and "agree" are shown in Table 4. A similar process was followed to identify the ten least commonly implemented controls, except that we combined the "strongly disagree" and "disagree" responses. The frequency results for the ten least commonly implemented controls are shown in Table 5, with the least commonly implemented control displayed at the top of the table.

Controls such as deploying antivirus software and authenticating remote users accessing the network were ranked as the most commonly implemented controls. Protecting equipment from unauthorized access and tracking the location of removable computer media using IT were ranked as the least commonly implemented controls. It should be noted that although the controls represented in Table 5 were ranked as the least commonly implemented, this does not mean that the controls do not exist in some form within the organization. The organization may have such a control, but may not use IT to support that control.

TABLE 4
Ten Most Commonly Implemented Controls

ISO #	Control Description	Frequency of "Strongly Agree" and "Agree" Responses	Ranking for Finance/ Banking/ Accounting Industries	Ranking for Insurance/Real Estate/Legal Services Industries	Ranking for Manufacturing Industry	Ranking for Government Agencies
10.5.4	Our organization uses IT to deploy antivirus software on workstations.	608	1	6	1	1
9.4.3	Our organization uses IT to authenticate remote users accessing the network.	606	2	9	3	9
8.5.1	Our organization uses IT to protect networks from unauthorized access.	604	7	4	7	4
8.5.1	Our organization uses IT to maintain network security.	603	8	5	—	2
10.5.4	Our organization uses IT to keep antivirus software updated.	602	3	2	8	5
9.5.2	Our organization uses IT to enforce a secure log-on process when providing access to information services.	601	4	1	5	6
9.3.1	Our organization uses IT to enforce security procedures regarding password selection and use (e.g., minimum length of six characters, frequency of password change).	598	6	—	4	3
9.6.1	Our organization uses IT to restrict access rights to applications.	597	—	8	6	7
8.4.1	Our organization uses IT to regularly back up essential business information and software.	592	5	3	2	—
9.2.2	Our organization uses IT to restrict and control system privileges.	590	10	10	9	8

TABLE 5

Ten Least Commonly Implemented Controls

ISO #	Control Description	Frequency of “Strongly Disagree” and “Disagree” Responses	Ranking for Finance/ Banking/ Accounting Industries	Ranking for Insurance/Real Estate/Legal Services Industries	Ranking for Manufacturing Industry	Ranking for Government Agencies
7.2.1	Our organization uses IT to protect equipment from unauthorized access.	235	1	1	1	3
8.6.1	Our organization uses IT to track the location of removable computer media.	191	2	2	4	10
7.1.3	Our organization uses IT to secure offices and rooms.	184	3	3	2	2
7.1.1	Our organization uses IT to secure the physical perimeter of our buildings.	166	5	6	—	1
7.1.2	Our organization uses IT to manage visitor access to secure areas within our buildings.	161	6	4	5	5
7.1.5	Our organization uses IT to restrict access to the facility from the delivery or loading area.	152	7	—	3	7
8.1.6	Our organization uses IT to measure security compliance at a third-party facility.	147	4	5	6	—
10.3.3	Our organization applies digital signatures to protect the authenticity and integrity of electronic information.	141	—	7	7	6
12.3.2	Our organization uses IT to record each use of software audit tools.	130	8	—	10	—
7.2.5	Our organization encrypts confidential information taken off-site.	129	—	9	9	—

Tables 4 and 5 also contain information about which of these controls were also ranked in the top ten and bottom ten by respondents from each of the four largest industry groups. These rankings provide insight into the security priorities of different industries. For example, Table 4 shows that authenticating remote users accessing a network is much more important to organizations in Finance/Banking/Accounting and Manufacturing industries than it is to Government Agencies or organizations in Insurance/Real Estate/Legal Services industries. It also shows that even though maintaining network security was the fourth overall most commonly implemented control, it did not make the top-ten list for the Manufacturing industry. Table 5 shows that although the other industries did not often use IT to measure security compliance at a third-party facility, the respondents from Government Agencies did not rate this control as one of their top ten least implemented. The differences and similarities shown in Tables 4 and 5 offer an interesting look into the security strategies of each industry.

"Not Applicable" and "Not Sure" Responses

Participants were given the option to choose "not applicable" or "not sure" during the survey, when answering questions about the use of each IT control in their organization. "Not sure" and "not applicable" responses were filtered out for much of the analysis we performed (e.g., Table 4 and Table 5 above) so that we could focus on controls whose implementation could be assessed on the "agree/disagree" scale. However, reviews of both the "not applicable" and "not sure" responses were performed to be sure that the "not applicable" response was used appropriately, and to see if we could gain any insight into why a respondent might have selected "not sure" as their response.

In the survey instructions we indicated that a "not applicable" response should be used if the control did not apply to their organization (see Appendix A). For example, perhaps the organization does not have third-party vendors that they work with; so instead of disagreeing that they use IT to implement a control related to third-party vendors, they should select that the control is "not applicable." Table 6 contains a list of the controls most frequently listed as "not applicable." Although we do not have organizational data to verify the appropriateness of the responses, it

TABLE 6

Controls Most Frequently Listed as "Not Applicable"

ISO #	Control Description	Frequency of "Not Applicable" Responses
7.1.5	Our organization uses IT to restrict access to the facility from the delivery or loading area.	73
8.1.6	Our organization uses IT to measure security compliance at a third-party facility.	65
8.7.3	Our organization uses IT to protect electronic commerce activities.	65
12.3.2	Our organization uses IT to restrict access to organizational system audit tools.	31
8.7.7	Our organization uses IT to protect information that is exchanged using voice and video outputs.	31
12.3.2	Our organization uses IT to record each use of software audit tools.	27
8.7.5	Our organization uses IT to secure electronic office systems (e.g., an organizational document management system).	25

seems likely that respondents who selected a "not applicable" response for the questions shown in Table 6 may have done so because their organization did not have a loading dock, use system audit tools, etc.

The "not sure" responses reveal which controls the participants were unable to assess. Table 7 contains a list of the IT controls for which at least 150 participants responded "not sure" regarding the use of the control in their organization.

The item referring to the usage of IT to deploy routing controls had the highest number of "not sure" responses. We conducted further analysis on the "not sure" responses to see if we could determine if there were certain characteristics of the individual respondents (i.e., certifications) or the organization (i.e., size) that increased or decreased the likelihood of a "not sure" response. For each potential covariate we ran a Chi-square difference test to test if the number of responses that received a rating on the "strongly agree" to "strongly disagree" scale were significantly different from the number of "not sure" responses. We removed the "not applicable" responses from the data before this analysis.

The analysis revealed that organizational size did not have a significant influence over whether a respondent could provide an "agree/disagree" response to the survey questions as opposed to a "not sure" response. However, when we analyzed the certifications possessed by the respondents there were two interesting findings. First, there were 91 individuals who had a CPA certification and no other certification. When the responses of these individuals were compared to the 416 individuals who did not have a CPA certification (the 129 individuals with CPA certification in addition to other certifications were eliminated from the analysis in order to avoid confounding the findings), the CPAs selected "not sure" *more* frequently ($p < 0.05$) than non-CPAs for 43 of the 108 controls.

Second, there were also 91 individuals who had Certified Information Systems Auditor (CISA) certification and no other certification. When the responses of these individuals were

TABLE 7

Controls Most Frequently Listed as "Not Sure"

ISO #	Control Description	Frequency of "Not Sure" Responses
9.4.8	Our organization uses IT to deploy routing controls requiring origin and destination address checking.	208
8.2.1	Our organization uses IT to monitor power capacity demands.	175
8.4.3	Our organization uses IT to analyze fault logs for trends.	175
12.3.2	Our organization uses IT to record each use of software audit tools.	169
9.5.1	Our organization uses IT to deploy automatic terminal identification to authenticate connections.	169
9.5.8	Our organization uses IT to limit connection time for high-risk applications.	166
8.7.7	Our organization uses IT to protect information that is exchanged using voice and video outputs.	165
8.6.1	Our organization uses IT to track the location of removable computer media.	164
9.4.5	Our organization uses IT to control access to diagnostic ports.	159
8.1.6	Our organization uses IT to measure security compliance at a third-party facility.	157
8.4.3	Our organization uses IT to maintain a fault log.	157

compared to the 398 individuals who did not have CISA certification (the 147 individuals with a CISA certification in addition to other certifications were eliminated from this analysis), the individuals with CISA certification selected "not sure" significantly *less* frequently ($p < 0.05$) than those without a CISA certification for 48 of the 108 controls. These results imply that perhaps the CPAs' knowledge of IT and IT controls within an organization was limited. Instead, CISAs were more likely to be able to provide an "agree/disagree" response to the questions regarding the implementation of IT controls, rather than a "not sure" response.[1]

Public versus Private Organizations

Table 8 presents the results of a comparison of control implementation means for public versus private companies.[2] In all, 41 controls were implemented at significantly different levels ($p < 0.05$), based on the company's status as public or private. For each control, the respondents from the public organizations more strongly agreed (i.e., the mean response was closer to a positive response ("4.5")) that the control was implemented in their organization as compared to the private organizations. It is encouraging that publicly traded companies may be addressing SOX compliance and taking their responsibilities to their shareholders seriously by taking many of the necessary steps to protect their information systems.

Large versus Small Organizations

When we compared IT controls based on company size (large versus small), 11 controls were implemented at significantly different levels ($p < 0.05$). For purposes of our analysis, we defined a large company as having 500 or more employees and a small company as having 499 or fewer employees. A 500-employee threshold is commonly used for defining small organizations (e.g., National Institute of Standards and Technology 2007; U.S. Small Business Administration 2006; Ford 2009). Table 9 shows the results of this analysis. For eight of the 11 controls, participants from large organizations indicated that they more strongly agreed that the control was used in their organization. This result is consistent with expectations of what one would see in organizations that may have more resources than their smaller counterparts.

However, for three controls, smaller organizations received ratings that indicated higher levels of control implementation: becoming aware of patches and fixes to current software, protecting mobile computing equipment, and ensuring that data are backed up to servers rather than individual PC hard drives. For each of these three controls, the more users there are in the organization, the more of a burden each of these tasks becomes. Thus, it is reasonable that smaller companies report higher levels of success in implementing these controls.

Our finding is consistent with prior research that also found that large organizations had higher-quality implementations for many of their security controls (Baker and Wallace 2007). Although other security studies have captured information about organizational size (i.e., Richardson 2008), none of them appear to have used that information to examine a relationship between organizational size and control implementation decisions.

[1] Although there were 84 individuals who possessed only a Certified Internal Auditor (CIA) certification, only six controls were significantly different at a level of $p < 0.05$ from the non-CIA respondents, and none of the controls were significantly different at a level of $p < 0.01$. Therefore, the results of this analysis are not reported.

[2] Keeping with our previous approach of combining the "strongly agree" and "agree" responses to collectively represent a positive indication of an IT control, and combining the "strongly disagree" and "disagree" responses to represent a negative indication of an IT control, we averaged the value of the subject's response in these categories. Specifically, a value of "5" originally indicated that the participant "strongly agreed" that the IT control was in place in their organization and a "4" indicated that they selected an "agree" response. These values were changed to "4.5" to collectively represent a positive response. The "strongly disagree" responses ("1s") and "disagree" responses ("2s") were all changed to "1.5s" for this analysis.

TABLE 8
Mean Comparisons of Public to Private Companies

ISO #	Control Description	Public	Private	Sig.
6.3.2	Our organization uses IT to report security weaknesses in systems or services.	4.09	3.93	0.000
7.1.1	Our organization uses IT to review and update access rights to secure physical areas.	4.15	3.94	0.000
7.1.3	Our organization uses IT to detect unauthorized access to physical facilities.	3.74	3.44	0.000
7.2.1	Our organization uses IT to monitor equipment for adverse environmental conditions.	4.06	3.87	0.000
7.2.5	Our organization password protects equipment taken off-site.	3.98	3.58	0.000
8.1.3	Our organization uses IT to recover from errors resulting from incomplete/inaccurate data input.	4.11	3.96	0.000
8.1.3	Our organization uses IT to generate an audit trail of security incidents.	4.22	3.97	0.000
8.1.5	Our organization uses IT to separate access to development, testing, and operational environments.	4.28	4.17	0.000
8.4.1	Our organization uses IT to regularly test backup restoration.	4.15	3.90	0.000
8.4.2	Our organization uses IT to create operator logs.	4.27	4.11	0.000
8.7.4	Our organization uses IT to secure electronic mail.	4.35	4.25	0.000
8.7.5	Our organization uses IT to secure electronic office systems (e.g., an organizational document management system).	4.01	3.79	0.000
9.2.1	Our organization uses IT to implement a formal user registration procedure for access to multi-user information systems.	4.34	4.16	0.000
9.3.1	Our organization uses IT to enforce security procedures regarding password selection and use (e.g., minimum length of six characters, frequency of password change).	4.43	4.34	0.000
9.4.5	Our organization uses IT to control access to diagnostic ports.	4.26	4.12	0.000
9.5.8	Our organization uses IT to limit connection time for high-risk applications.	4.01	3.74	0.000
10.4.3	Our organization uses IT to control access to the program source libraries.	4.42	4.32	0.000
12.3.1	Our organization uses IT to create logs of all system audit activities.	3.91	3.58	0.000
6.3.4	Our organization uses IT to periodically analyze security incident logs for trends.	3.97	3.80	0.001
8.7.2	Our organization uses IT to secure media in transit from unauthorized access, misuse, or corruption.	3.91	3.72	0.001
9.5.7	Our organization uses IT to shut down inactive terminals in high-risk areas after a defined period of inactivity.	3.90	3.72	0.001
10.5.4	Our organization uses IT to deploy antivirus software on workstations.	4.47	4.43	0.001
7.2.2	Our organization uses IT to ensure uninterrupted power to equipment running critical business applications.	4.38	4.31	0.002

(continued on next page)

TABLE 8 (continued)

ISO #	Control Description	Public	Private	Sig.
7.1.1	Our organization uses IT to secure the physical perimeter of our buildings.	3.56	3.28	0.003
7.1.2	Our organization uses IT to provide an auditable trail of access to physical facilities.	3.80	3.60	0.003
7.1.3	Our organization uses IT to control access to internal phone directories.	3.74	3.58	0.003
7.2.4	Our organization uses IT to track the maintenance of information-processing equipment.	4.06	3.92	0.003
9.7.2	Our organization uses IT to monitor the use of information-processing facilities.	4.25	4.14	0.003
8.7.3	Our organization uses IT to protect electronic commerce activities.	4.31	4.22	0.004
10.2.3	Our organization uses IT to ensure the authenticity of electronic messages.	4.03	3.87	0.004
9.7.1	Our organization uses IT to create access event logs.	4.23	4.12	0.005
12.1.5	Our organization uses IT to require users to agree to policies regarding appropriate use of information-processing facilities when logging on to a system.	4.09	3.99	0.006
8.2.2	Our organization uses IT to become aware of upgrades available for currently installed software.	4.26	4.17	0.007
8.1.4	Our organization uses IT to support the segregation of duties.	4.16	4.06	0.013
8.1.1	Our organization uses IT to make information security operating procedures available to staff and/or third-party contractors.	4.08	3.98	0.026
9.5.5	Our organization uses IT to restrict the use of system utilities.	4.27	4.21	0.030
7.1.2	Our organization uses IT to manage visitor access to secure areas within our buildings.	3.55	3.46	0.031
8.3.1	Our organization uses IT to implement corrective controls in response to malicious software.	4.27	4.20	0.043
8.5.1	Our organization uses IT to protect data passing over networks.	4.32	4.26	0.044
10.3.3	Our organization applies digital signatures to protect the authenticity and integrity of electronic information.	3.53	3.34	0.046
10.2.2	Our organization uses IT to detect corruption during data processing.	4.13	4.05	0.049

Training

Research has shown that organizations may not require their IT personnel to participate in compliance efforts (Leskela and Logan 2003) or, if IT professionals are involved in the compliance process, they may not be well-versed in the intricacies of internal control (ITGI 2006). As research has shown that IT training and experience is important for making sure that auditors can properly evaluate controls (Curtis et al. 2009), it seems likely that IT training and experience would be important for those who are deciding which controls to implement as well. Because SOX compliance should be a cross-functional effort between audit employees and IT employees, we asked the participants whether IT personnel in their organization were involved in SOX compliance activities and/or had received SOX training, as well as whether their auditors had received IT

TABLE 9

Mean Comparisons of Large to Small Companies

ISO #	Control Description	Large	Small	Sig.
9.5.8	Our organization uses IT to limit connection time for high-risk applications.	3.84	3.48	0.000
10.3.5	Our organization uses IT to support an encryption key management system.	3.83	3.54	0.001
9.8.1	Our organization uses IT to protect mobile computing equipment (e.g., laptops, mobile phones, and PDAs).	3.85	4.11[a]	0.005
8.1.3	Our organization uses IT to respond to information systems failures (e.g., loss of service).	4.26	4.17	0.005
10.2.1	Our organization uses IT to validate data input to application systems.	3.94	3.76	0.006
8.7.6	Our organization uses IT to prevent unauthorized modification of information that is to be made public.	3.89	3.80	0.006
8.4.1	Our organization uses IT to ensure that data are backed up to servers and not individual PC hard drives.	3.77	3.98[a]	0.010
7.2.1	Our organization uses IT to monitor equipment for adverse environmental conditions.	3.85	3.74	0.013
8.2.1	Our organization uses IT to monitor the utilization of key system resources (e.g., file servers, domain servers).	4.19	4.09	0.015
8.2.2	Our organization uses IT to become aware of patches and fixes to current software.	4.24	4.26[a]	0.015
8.1.4	Our organization uses IT to support the segregation of duties.	3.99	3.83	0.035

[a] The average rating for these three items had a significantly higher agreement rating for smaller companies than they did for larger companies.

training. We then compared the means for each control implementation based on levels of auditor training, IT employee involvement in SOX compliance, and levels of SOX training for IT personnel.

The results are summarized in Table 10. In all cases, if the respondent indicated that their organization provided training or had IT involvement in SOX compliance, they were more likely to agree that the IT control was present. Companies who indicated that they provided auditor training had 35 controls that were more likely to be implemented than those who did not provide auditor training. If IT personnel were involved in SOX compliance, then 55 controls were significantly more likely to be implemented. Finally, the level of SOX training for IT personnel positively affected the likelihood of implementation for 65 of the 108 controls.

The results indicate that training and/or IT involvement can make a highly significant difference in control implementation strategies. When the participants strongly agreed or agreed that their organizations had IT employees who were involved in SOX activities, or that their IT personnel had received SOX training, over half of the 108 controls were implemented significantly more often than if they disagreed with the statements regarding IT employees. Although previous studies have indicated that IT employees may not be involved in SOX compliance activities, we have evidence that organizations may benefit from IT employee involvement.

TABLE 10

Count of Significantly Different Controls Based on Presence of Training/Involvement

Item	Count of Significantly Different Controls[a]
Our auditors have received IT training.	35
Our organization has IT employees who are involved with Sarbanes-Oxley compliance activities.	55
Our IT personnel have received Sarbanes-Oxley compliance training.	65

[a] This count represents the number of controls that were significantly different for participants who indicated their organizations provided training/involvement ("strongly agree" or "agree") versus those who did not provide training/involvement ("disagree" or "strongly disagree").

Because of the overwhelming differences in control implementation in organizations that had some type of IT involvement or training, we ran a regression using the training/involvement questions as independent variables and the respondents' answer to the question "Our organization has achieved SOX compliance" as the dependent variable. Although the dependent variable measure we used can only provide a general measure of SOX compliance, it may still serve as an indication of a relationship between auditor and IT training/involvement and the respondents' assessment of their organizations' level of SOX compliance. The results of the regression are shown in Table 11. The R^2 value is 0.126 and all three independent variables were significant at the $p < 0.10$ level.

V. DISCUSSION

As stated earlier, this research was designed to be an exploratory study that would provide us with a better understanding of the types of IT controls that organizations are currently implementing. Establishing baseline knowledge of the current state of organizational controls is essential to achieving the ultimate goal of developing and testing a model linking IT controls to SOX compliance success. The results of this research can serve as a basis for future research and have revealed a research stream with great potential.

Our findings provide insight into the current state of support provided by IT controls and the impact of training both on an organization's choice of controls and the likelihood that they will

TABLE 11

Regression Results for Achieving SOX Compliance (Public Companies Only)

Variable Description	B	Std. Error	t	Sig.
Constant	0.946	0.125	7.545	0.000
Our organization has IT employees who are involved with Sarbanes-Oxley compliance activities.	0.172	0.054	3.187	0.002
Our auditors have received IT training.	0.083	0.044	1.894	0.059
Our IT personnel have received Sarbanes-Oxley compliance training.	0.109	0.047	2.340	0.020
Adjusted $R^2 = 0.126$.				

achieve SOX compliance. In general, we found that most participants agreed that each of the IT controls was in place within their organizations to at least some extent. However, we noticed some differences in certain types of organizations and the controls on which they chose to focus. Table 12 summarizes our findings and suggests areas for future research. These suggestions are discussed below.

Half of the ten most commonly implemented controls consisted of controls from the ISO category, Access Control, while more than half of the ten least commonly implemented controls came from the Physical and Environmental Security category (see Tables 4 and 5). This suggests that organizations have prioritized IT controls related to protecting their informational assets, while giving less attention to IT controls that can protect their physical assets. Future research could investigate whether organizations are leaving themselves vulnerable by not using IT to protect their physical assets and if so, could suggest specific controls that would improve their physical security. The results also reveal that although the largest number of survey questions were from the ISO category of Communications and Operations Management, only three controls in this category showed up in the ten most commonly implemented controls list, suggesting that these controls are not a top priority for many organizations. This category refers to controls that help with incident management, segregation of duties, capacity planning, and electronic commerce and email security. Future research should investigate if there are IT controls related to these areas that organizations should be considering more seriously in their implementation strategies or if they are wisely making them a lower priority.

There were also some differences among the industry groups in our study. For example, Table 4 shows that most industry groups rated the use of IT to deploy antivirus software as the most commonly implemented control, but organizations in the Insurance/Real Estate/Legal Services industries rated this control much lower in the list. The Insurance/Real Estate/Legal Services industries also rated most of the controls in the Access Control category (category 9) much lower than the other industry groups did, including the selection and use of passwords, which did not even make it into their top-ten list. Future research could investigate whether these low rankings are due to a lack of concern for appropriate information access controls in these industries and whether these industries need to change their security strategies to better address these vulnerabilities.

Table 4 also reveals that controls related to backing up business information and software did not make the top-ten list for Government Agencies, while it was in the top five most commonly implemented controls for the other industries in the table. Given the often-publicized reports of government laptops that are stolen or go missing, it seems that the government may want to consider stronger controls in this area. Future research could investigate the reasons for the lack of backup controls among Government Agencies and recommend appropriate strategies to help them better secure their information assets.

Participants from publicly traded companies agreed more strongly than participants from private organizations that 41 controls were in place in their organizations (see Table 8). This result implies that there may be a link between SOX compliance (which is relevant only for publicly traded companies) and the effort put into the implementation of certain IT controls. Publicly traded companies may be more aware of the importance of particular IT controls for protecting their data and business systems, although private companies may benefit from these same controls.

Table 8 indicates that the differences between public and private companies span almost all the ISO categories of controls, although half of the survey questions dealing with Physical and Environmental Security (category 7) were significantly different, as were half of the questions from the Compliance category (category 12). This suggests that publicly traded organizations may

TABLE 12

Summary of Findings and Future Research Ideas

Findings	**Future Research Ideas**
10 most common controls: • 5 from Access Control • 3 from Communications and Operations Management • 2 from Systems Development and Maintenance	• Investigate the lack of top-ranked controls from the Communications and Operations Management category.
10 least common controls: • 6 from Physical and Environmental Security • 2 from Communications and Operations Management • 1 from Systems Development and Maintenance • 1 from Compliance	• Investigate the lack of controls in the Physical and Environmental Security category.
Industry differences: • Access Control—not as highly ranked by the Insurance/Real Estate/Legal Services industries. • Information Backup Controls—not in top ten rankings by Government Agencies.	• Investigate the reasons for lower-ranked Access Control by certain industries and develop strategies to increase controls in this area if necessary. • Investigate the reasons for lower ratings of controls related to information backups by Government Agencies and recommend strategies for securing information assets.
Public versus private organizations: • 41 controls were more likely to be implemented in public organizations. • The controls spanned all ISO categories, although half of the controls from Physical and Environmental Security were significantly different, as were half of the controls from Compliance.	• Investigate control strategies of public organizations as compared to private organizations, particularly as they relate to protection of physical assets and logging system activities. • Investigate IT investment decisions of companies that were public but chose to go private after SOX.

(continued on next page)

TABLE 12 (continued)

Findings	**Future Research Ideas**
Certification differences: • CPAs were more likely to select a "not sure" response. • CISAs were less likely to select a "not sure" response. • Respondents with CISA certifications were significantly more likely ($p < 0.05$) to agree with the statement "Our auditors have received IT training" than the non-CISA respondents. • There was no significant difference in the frequency of "agree" responses regarding auditor training between CPAs and non-CPAs.	• Future researchers should be aware that a person's certifications could affect their ability to assess controls. • Investigate whether providing additional training to certain groups of employees (e.g., CPAs) could improve their ability to assess organizational controls and develop appropriate implementation strategies.
Large versus small organizations: • 8 controls were more likely to be implemented in large organizations. • 3 controls were more likely to be implemented in small organizations.	• Investigate whether there are strategies that smaller companies should follow in order to implement certain controls, given that they may have limited resources. • Investigate whether there are strategies that larger companies can follow in order to reduce the complexities of implementing certain controls that are more difficult with large numbers of employees.
Training: • 60% of controls were more likely to be implemented in organizations where IT employees had been trained in SOX compliance issues. • 50% of controls were more likely to be implemented in organizations where IT employees were involved in SOX compliance activities. • 32% of controls were more likely to be implemented in organizations where auditors had received IT training. • Training of IT employees and internal auditors was significantly more likely to result in an "agree" response to the statement "Our organization has achieved Sarbanes-Oxley compliance."	• Investigate the best practices for including IT personnel in an organization's SOX compliance activities and the impact that their training can have on the selection of controls. • Investigate the relationship between IT personnel and internal auditors and the impact that the training provided to each group can have on an organization's control implementation strategies. • Develop recommendations for how IT personnel and internal auditors can work together to improve SOX compliance efforts.

(continued on next page)

TABLE 12 (continued)

Findings	Future Research Ideas
Other future research:	• Further investigate the relationships between information technology, organizational characteristics, and the quality and effectiveness of internal controls. • Consider an organization's selection of controls from a risk assessment or cost-benefit viewpoint. • Develop a top-down, risk-based approach to assessing the effectiveness of controls and implementing risk mitigation strategies.

be better at using IT to protect their physical assets and to log system activity than private organizations. Future research should further identify and investigate differences in the control implementation strategies of public and private organizations.

There have also been a number of organizations who have chosen to go private as a result of SOX because they felt that the cost of compliance exceeded the benefits (Engel et al. 2007). These organizations provide a unique opportunity for study, as they have operated both as public and private organizations. Future research could investigate organizations that were previously public but went private after SOX and compare their IT security strategies both before and after their decision to go private.

Another interesting finding from this research was that the certification that an individual possessed had an impact on the likelihood that they would select a "not sure" response when asked if their organization used a particular control. Participants with only a CPA certification were significantly more likely to select "not sure" than non-CPAs. Therefore, even if an organization had a control in place, the CPAs may not have been aware of its existence. On the other hand, participants with only a CISA certification were less likely to select "not sure" as their response than non-CISAs. Almost no differences were found among participants with only a CIA certification versus non-CIAs. Future research should further investigate possible differences due to certifications and researchers conducting survey research should be aware of the possibility that even if their respondents have identical job titles, the certifications they possess could affect their ability to answer certain questions.

For example, training may play a role in the number of "not sure" answers that a respondent selected. Further analysis showed that the respondents with CISA certifications were significantly more likely ($p < 0.05$) to agree with the statement "Our auditors have received IT training" than the non-CISA respondents. However, there was no significant difference in the frequency of "agree" responses regarding auditor training between CPAs and non-CPAs. This result implies that perhaps the CISA respondents were more likely to have received IT training than non-CISAs or CPAs and thus were less likely to select a "not sure" response. Providing IT training to CPAs may enhance their ability to identify and assess organizational controls, resulting in a more effective control environment within the organization. Future research could determine if training sessions focused on employees with certain certifications would be beneficial for organizations who are building their security programs.

Future research should also look at the relationship between certifications and control strategies within an organization. Perhaps, if CPAs are unaware of the existence of certain controls, there would be more gaps and security problems in organizations that predominately employ CPAs. On the other hand, research could determine if there are better controls in place within organizations that have more CISAs. Similarly, there may be a relationship between employee certification and ability to achieve SOX compliance.

The number of employees that an organization had was also shown to have a relationship with the controls that the organization chose to implement. Generally, participants from larger organizations indicated higher levels of agreement with the statements regarding control implementation. However, there were some controls that smaller organizations may be better able to handle due to the reduced complexity of managing fewer employees. Table 9 shows that more than half of the controls that were significantly different for organizations of different sizes were from the ISO category dealing with Communications and Operations Management. Future research could further investigate this link and determine if there are strategies that smaller companies could follow in order to implement controls in this area, given that they may have more limited resources than larger organizations. Research could also be used to help larger organizations reduce the complexity associated with implementing controls in the areas where they were not as likely to have coverage as smaller organizations that have fewer employees (i.e., protecting mobile computing equipment, backing up data to servers, and becoming aware of software patches and fixes).

Perhaps most importantly, the results indicate that employee training can have a very significant impact on both the selection of IT controls in an organization as well as its ability to achieve SOX compliance. Table 10 shows that 60 percent of the controls were significantly more likely to be implemented in organizations where IT employees had been trained in SOX compliance issues. Additionally, 50 percent of the controls were more likely to be implemented in organizations where IT employees were involved in SOX compliance activities. Furthermore, Table 11 shows that organizations that trained their IT employees on SOX compliance issues and involved them in SOX compliance activities were more likely to agree with the statement that their organization had achieved SOX compliance. These findings are an indication that when IT employees are educated on SOX issues and included in the SOX compliance process, they are able to realize the value of certain controls in helping their organization achieve its SOX compliance objectives. Future research should investigate the best practices for including IT personnel in an organization's SOX compliance activities and the impact that their training can have on the selection of controls. Similarly, almost one-third of the controls were more likely to be implemented in organizations where auditors had received IT training. This finding could indicate that training auditors on IT issues may increase their awareness of the usefulness of certain IT controls. Future research should further investigate the relationship between personnel training and IT control implementation strategies.

For example, future research could study the relationship between IT personnel and internal auditors and the impact that the training provided to each group has on an organization's control implementation strategies. The structure and type of auditor and IT training and involvement that would be beneficial to SOX compliance have been largely unexamined in previous research efforts. Because of the exploratory nature of our study, we did not have comprehensive measures of training/involvement or SOX compliance, so the results related to training have limitations on their interpretability. IT personnel and internal auditors should work together to achieve SOX compliance. Therefore, a better understanding of the nature of their interaction and the best strategies for combining each of their strengths and weaknesses would be beneficial to organizations striving for the most effective and efficient strategies for SOX compliance. Our research indicates that organizational control systems may benefit if IT personnel have accounting/audit knowledge and internal auditors have IT knowledge. Future research should develop recommendations for how the two groups can work together more effectively, possibly through the development of cross-functional teams and interdisciplinary training. Future research could identify the training strategies that would be most beneficial for each category of employee.

A natural next step in this research stream is to further investigate the relationship between IT controls and SOX compliance. With a better understanding of the current state of practice regarding IT controls, future research can utilize the results from this study to identify categories of IT controls in order to develop and test a research model that continues to investigate the link between IT controls and SOX compliance. Future research could consider relationships between IT and organizational characteristics and the quality and effectiveness of internal controls. Such research could focus on whether the presence or absence of controls in organizations with certain characteristics could lead to stronger or weaker internal control environments and successful SOX compliance.

The selection and implementation of IT controls should also be considered within the larger context of risk assessment, risk management, and IT governance. Assessing the appropriateness of the use of technology for control implementation should be one part of an organizational risk assessment process within an IT governance strategy. McCuaig (2006) suggests that organizations should ask “What are the known risks, what steps have proven effective in mitigating the known risks, how should conformance to those mitigating activities be measured, and what should be reported to the public?”

Previous research has shown that, in response to SOX legislation, many companies are realizing the importance of their IT governance strategies and the impact that their governance strategies can have on their organization’s success (Bowen et al. 2007). Although we report on the IT controls currently used by companies, we do not consider the choice of controls from a risk assessment or cost-benefit viewpoint. Many controls may not be implemented using IT because the cost of implementation would outweigh the benefit of the control. We only asked participants about the controls actually in place and not about any cost considerations that were used to make decisions. By collecting data on the “why,” researchers may find that some controls are cost prohibitive or might have other risks that would limit their appropriateness.

Our research focused on uncovering the current state of internal controls in organizations, but other researchers have attempted to measure the effectiveness of internal controls (e.g., Mock et al. 2009) and have shown how IT plays a role in determining control effectiveness (e.g., Klamm and Weidenmier-Watson 2009). The results of our research could be used in conjunction with these other research efforts in order to develop a top-down, risk-based approach to assessing the effectiveness of controls and implementing risk mitigation strategies.

VI. CONCLUSION

IT controls are an important component of an organization’s internal control structure. Safeguarding and monitoring a company’s financial data are an essential part of IT controls and SOX requirements. Information security management is a complex task and if governed effectively, helps organizations to not only achieve SOX compliance but also maintain that compliance. The results of this research not only provide a description of the IT controls used in current practice, but also suggest how future research can build on the current findings to develop strategies to aid organizations in implementing information security controls that support and maintain compliance with SOX.

APPENDIX A
SAMPLE INSTRUCTIONS AND ITEMS FROM CURRENT SURVEY

Please use the scale to indicate the extent to which you agree with each of the statements below. If you do not know how to answer the question, you should select “not sure.” If a control is not applicable to your organization, you should select “not applicable” for that item. For the purposes of this survey, “IT” refers to any technology that helps to manage information, such as some combination of computer hardware, software, and associated communications systems.

Please use the following scale to indicate the extent to which you agree with each of the statements below:

1. Strongly Disagree
2. Disagree
3. Neutral
4. Agree
5. Strongly Agree
6. Not Sure

7. Not Applicable

Likert Scale Questions

ISO 17799 Component[a]		Survey Item
A.4.2.1	Identification of risks from third-party access	Our organization uses IT to ensure that third-party access to our systems is authorized.
A.5.1.1	Inventory of assets	Our organization uses IT to maintain an inventory of assets.
A.5.1.1	Inventory of assets	Our organization uses IT to maintain an inventory of information assets (e.g., data files).
A.6.2.1	Information security education and training	Our organization uses IT to educate employees on information security policies.
A.6.3.1	Reporting security incidents	Our organization uses IT to report security incidents (e.g., electronic notification).
A.6.3.2	Reporting security weaknesses	Our organization uses IT to report security weaknesses in systems or services.
A.6.3.3	Reporting software malfunctions	Our organization uses IT to report software malfunctions.
A.6.3.4	Learning from incidents	Our organization uses IT to periodically analyze security incident logs for trends.
A.7.1.1	Physical security perimeter	Our organization uses IT to secure the physical perimeter of our buildings.
A.7.1.2	Physical entry controls	Our organization uses IT to manage visitor access to secure areas within our buildings.
A.7.1.2	Physical entry controls	Our organization uses IT to provide an auditable trail of access to physical facilities.
A.7.1.2	Physical entry controls	Our organization uses IT to review and update access rights to secure physical areas.
A.7.1.3	Securing offices, rooms, and facilities	Our organization uses IT to secure offices and rooms.
A.7.1.3	Securing offices, rooms, and facilities	Our organization uses IT to detect unauthorized access to physical facilities.
A.7.1.3	Securing offices, rooms, and facilities	Our organization uses IT to enforce the use of access codes for server and communication rooms.
A.7.1.3	Securing offices, rooms, and facilities	Our organization uses IT to control access to internal phone directories.
A.7.1.4	Working in secure areas	Our organization uses IT to implement additional controls for areas with higher security needs.
A.7.1.5	Isolated delivery and loading areas	Our organization uses IT to restrict access to the facility from the delivery or loading area.
A.7.2.1	Equipment setting and protection	Our organization uses IT to protect equipment from unauthorized access.
A.7.2.1	Equipment setting and protection	Our organization uses IT to protect equipment from unauthorized removal from the premises.
A.7.2.1	Equipment setting and protection	Our organization uses IT to monitor equipment for adverse environmental conditions.
Other question		Our organization uses IT to restrict access to organizational system audit tools.
Other question		Our organization has IT employees who are involved with SOX compliance activities.
Other question		Our organization has achieved SOX compliance.

(continued on next page)

Likert Scale Questions

ISO 17799 Component[a]	Survey Item
Other question	Our organization has had IT security issues unrelated to SOX compliance during the past two years.
Other question	Our IT personnel have received SOX compliance training.
Other question	Our auditors have received IT training.
Other question	I consider myself an expert on Sarbanes-Oxley.
Other question	In general, I consider myself an expert on IT controls.
Other question	Our organization has implemented new IT controls in response to SOX.

[a] The information in the left columns of the table did not appear on the final survey. It is included here only so that the reader can see how the items were mapped to ISO 17799. This is also not a complete list of items contained on the survey. We asked the respondents to respond to questions regarding 108 IT-related controls.

REFERENCES

Anand, S. 2008. Information security implications of Sarbanes-Oxley. *Information Security Journal: A Global Perspective* 17 (2): 75–70.

Armstrong, J. S., and T. S. Overton. 1977. Estimating nonresponse bias in mail surveys. *JMR, Journal of Marketing Research* 14 (3): 396–403.

Baker, W., and L. Wallace. 2007. Is information security under control? Investigating quality in information security management. *IEEE Security and Privacy* 5 (1): 36–44.

Bowen, P. L., M.-Y. D. Cheung, and F. H. Rohde. 2007. Enhancing IT governance practices: A model and case study of an organization's efforts. *International Journal of Accounting Information Systems* 8 (3): 191–221.

Brown, W., and F. Nasuti. 2002. Sarbanes-Oxley and enterprise security: IT governance—What it takes to get the job done. *Security Management Practices* 14 (5): 15–28.

Calder, A., and S. Watkins. 2002. *IT Governance Data Security & BS 7799/ISO 17799: A Manager's Guide to Effective Information Security*. London, U.K.: Kogan Page.

Carlson, T. 2008. *Understanding ISO 27002*. Bay Area, CA: Orange Parachute. Available at: http://www.orangeparachute.com/documents/Understanding_ISO_27001.pdf.

CIOInsight. 2004. *EXP Research: Sarbanes-Oxley 2004: Are You Ready to Comply?* New York, NY: CIO-Insight. Available at: http://www.cioinsight.com/c/a/Research/Research-SarbanesOxley-Are-You-Ready-to-Comply/.

Curtis, M. B., J. G. Jenkins, J. C. Bedard, and D. R. Deis. 2009. Auditors' training and proficiency in information systems: A research synthesis. *Journal of Information Systems* 23 (1): 79–96.

Damianides, M. 2004. How does SOX change IT? *Journal of Corporate Accounting & Finance* 15 (6): 35–41.

———. 2005. Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management* 22 (1): 77–85.

Da Veiga, A., and J. Eloff. 2007. An information security governance framework. *Information Systems Management* 24 (4): 361–372.

Engel, E., R. Hayes, and X. Wang. 2007. The Sarbanes-Oxley Act and firms' going-private decisions. *Journal of Accounting and Economics* 44: 116–145.

Ford, M. 2009. Size, structure and change implementation: An empirical comparison of small and large organizations. *Management Research News* 32 (4): 303–320.

Garcia, V. 2004. Seven points financial institutions should know about IT spending for compliance. *Journal of Financial Regulation and Compliance* 12 (4): 330–339.

Greenfield, D. 2007. IT by the book. *InformationWeek* 35–38.

Harris, S. 2006. Alphabet soup: Understanding standards for risk management and compliance. *Information Security Magazine* (June 2).

Haworth, D. A., and L. R. Pietron. 2006. Sarbanes-Oxley: Achieving compliance by starting with ISO 17799. *Information Systems Management* 23 (1): 73–87.

Information Systems Audit and Control Association (ISACA). 2005. *COBIT Mapping: Mapping ISO/IEC 17799: 2000 with COBIT*. Rolling Meadows, IL: ISACA. Available at: http://www.isaca-oregon.org/docs/Mapping%20Cobit%20to%20ISO%2017799.pdf.

International Organization for Standardization (ISO). 2005. *Information Technology—Security Techniques—Code of Practice for Information Security Management*. Geneva, Switzerland: ISO. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612.

IT Governance Institute (ITGI). 2006. *IT Control Objectives for Sarbanes-Oxley*. Available at: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables?Pages/IT-Control-Objectives-for-Sarbanes-Oxley-2nd-Edition.aspx.

Kaarst-Brown, M., and S. Kelly. 2005. *IT Governance and Sarbanes-Oxley: The Latest Sales Pitch or Real Challenges for the IT Function?* Paper read at Proceedings of the 38th Hawaii International Conference on Systems Sciences, at IEEE.

Klamm, B., and M. Weidenmier-Watson. 2009. SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. *Journal of Information Systems* (Fall): 1–23.

Lazarides, T. 2007. Comply! Resistance is futile. *Information Management & Computer Security* 15 (5): 339–349.

Leskela, L., and D. Logan. 2003. *Sarbanes-Oxley Compliance Demands IS Involvement*. Stamford, CT: Gartner. Available at: http://www.gartner.com/resources/117800/117873/117873.pdf.

Linkous, J. 2008. Puzzle pieces: The relationship between SOX, COSO, and COBIT. Available at: http://eiqviews.wordpress.com/2008/11/20/puzzle-pieces-the-relationship-between-sox-coso-and-cobit/.

Ma, Q., A. Johnston, and M. Pearson. 2008. Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security* 16 (3): 251–270.

McCuaig, B. 2006. The ABCs of reporting on controls. *Internal Auditor* (October): 35–39.

Mock, T. J., L. Sun, R. Srivastava, and M. Vasarhelyl. 2009. An evidential reasoning approach to Sarbanes-Oxley mandated internal control risk assessment. *International Journal of Accounting Information Systems* 10 (2): 65–78.

National Institute of Standards and Technology. 2007. *Criteria for Performance Excellence*. Gaithersburg, MD: National Institute of Standards and Technology.

Praxiom Research Group Limited. 2008. *ISO IEC 27002 2005 Introduction*. Edmonton, Canada: Praxiom Research Group Limited. Available at: http://www.praxiom.com/iso-17799-intro.htm.

Richardson, R. 2008. *2008 CSI Computer Crime & Security Survey*. New York, NY: Computer Security Institute. http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

Tang, J. 2008. The implementation of Deming's System Model to improve security management: A case study. *International Journal of Management* 25 (1): 54–68.

United States Code. 2008. *Public Printing and Documents: Definitions*. Title 44, Section 3552. Washington, D.C.: United States Code.

U.S. House of Representatives, Committee on Financial Services. 2002. Sarbanes-Oxley Act of 2002. Public Law No. 107-204. Washington, D.C.: Government Printing Office.

U.S. Small Business Administration. 2006. *Table of Small Business Size Standards*. Washington, D.C.: U.S. Small Business Administration.

von Solms, B. 2005. Information security governance: COBIT or ISO 17799 or both? *Computers & Security* 24: 99–104.

Weidenmier, M., and S. Ramamoorti. 2006. Research opportunities in information technology and internal auditing. *Journal of Information Systems* 20 (1): 205–219.