Integrating IT Auditing (SAS 70 Reporting) to Benefit both the User and Service Organizations: An Organizational Change Perspective

Thomas J. Bell III, CISA, Ph.D.

Texas Wesleyan University, 1201 Wesleyan Street, Fort Worth, Texas 76105
Phone: (817) 531- 4845 Fax: (817) 531- 6585
tbell@txwes.edu

ABSTRACT

This research explores ways SAS 70 reporting can become more beneficial to both the service and user organizations. SAS 70 reports are attestations render by CPAs usually with the assistance of a Certified Information System Auditor (CISA). SAS (Statement on Auditing Standards) 70 is an international auditing standard created by the American Institute of Certified Public Accounting (AICPA) for service or outsourced organizations. SAS 70 principally serve as a communication vehicle for the service organization to communicate its control activities that pertain to IT and related processes.

This is a topic of significant importance because many of the functions performed by third party service providers affect user organizations' financial statements. And if the user organization is publicly owned a SAS 70 attestation report based on inadequate testing may yield a misstatement on the adequacy of controls which may breach compliance with Sarbanes Oxley regulations. Yet third party service providers must concurrently offer information to their customers, and user organizations while protecting its data from unauthorized access, use, or disclosure in a seemingly growing regulatory business climate. Sharing information through the Internet is now a prevailing practice (Panda, 1999) with security breaches affecting 90% of all businesses each year and costing some $17 billion (Austin & Darby, 2003). To investigate how service organizations are changing in response to their clients and user organizations ever increasing demand for more information access over the Internet and the inherent security risk associated with these demands, this paper examines a theoretical framework by analyzing the tradeoffs a SAS 70 IT audit yields and concludes with a suggested methodology.

Keywords*: IT Security, EDP Audit, Security, Information Security Audit, SAS 70, Organizational Change, Managerial Cognition, Sarbanes Oxley.*

INFORMATION TECHNOLOGY ROLE IN TODAY'S INCREASINGLY REGULATED BUSINESS ENVIRONMENT

The role of IT in business can be viewed as a process of supporting the business operations, supporting managerial decision-making and supporting strategic competitive advantage. This can be done on many levels but cost reduction is the most significant. The role of IT is useful when automation of processes can reduce labor and other overhead costs allowing

competition on price.

As Carr (2003) posit, “The operational risk associated with IT are many- technical glitches, obsolescence, services outage, unreliable vendors or partners, security breaches, even terrorism-and some have become magnified as companies have moved from tightly controlled, proprietary systems to open, shared ones. Today, an IT disruption can paralyze a company’s ability to make products, deliver its service, and connect with its customers, not to mention foul its reputation. Yet few companies have done a thorough job of identifying and tempering their vulnerabilities. Worrying about what might go wrong may not be as glamorous a job as speculating about the future, but it is a more essential job right now.”

The operational risk associated with financial reporting processes for most organizations are intricately linked with IT systems. Few companies manage their data manually and nearly all companies rely on electronic management of data, documents, and key operational processes. In order to keep cost of the operations down and ultimately increase the shareholders wealth, many companies have decided to outsource some of their IT operations. Thus increasing IT’s role in the cost cutting process as well as in the internal control oversight.

Chief information officers (CIO) are administratively accountable for the privacy, security, access, accuracy and the reliability of the systems that manage and report the financial data. Systems are deeply integrated in the initiating, authorizing, processing, and reporting of financial data. As such, they are in fact linked to the overall financial reporting process and need to be assessed, along with other important process for compliance with Sarbanes-Oxley Act. Although the Sarbanes-Oxley Act signals a fundamental change in business operations and financial reporting, and places responsibility in corporate financial reporting on the CEO and CFO, the CIO role is noteworthy in management's assessment of internal control under Section 404 and in supporting the financial statement certification process. That, of course, does not diminish CEO’s and CFO’s responsibilities. Under Section 302 of the Sarbanes-Oxley Act, the CEO and CFO are personally and legally responsible for the effectiveness of internal control over business processes and the related information systems that record, store, and process the results of such processes into financial statements (Cannon, 2005).

THE NEED FOR REGULATING AND OVERSEEING BUSINESSES AND THEIR VENDORS

With regards to several major business scandals which resulted in a precipitous decline of public trust in accounting and reporting practices, on July 30, 2002, President George W. Bush signed into law The Sarbanes-Oxley Act of 2002. A major provision in the Act is that it establishes a new quasi-public agency, the Public Company Accounting Oversight Board, which is charged with overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies. The Act also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure (AICPA.org, 2002).

Perhaps, the most contentious aspect of Sarbanes-Oxley Act is Section 404, which requires management and the external auditor to report on the adequacy of the company's internal control

over financial reporting. This stipulation is quite costly, since it mandates companies to implement, document and test important financial manual and automated controls all of which requires sometime enormous billable hours by an auditor.

IT department managers at publicly traded companies are well aware of control and compliance issues surrounding the Sarbanes-Oxley Act. Compliance with Sarbanes-Oxley Act refers to all aspect of businesses, domestic and outsourced ones. Public companies that outsource data center responsibilities have to manage their operations and are ultimately responsible for adherence to the same standards as if the operations were conducted in-house. In recent years it has become increasingly popular for companies to outsource many of their business support processes with growing concerns for the potential loss of control and therefore compliance violations. Companies wanting to address this concern while taking advantage of the benefits of outsourcing including cost efficiencies and increased internal focus might consider evaluating outsourced provider in the three critical areas of people, processes and technology; businesses can position itself to not only take advantage of the cost savings of outsourcing, but also ensure that regulatory compliance mandates are met.

STATEMENT ON AUDITING STANDARDS 70 (SAS 70) DEFINED

The Statement on Auditing Standards (SAS 70) is an auditing standard created by the American Institute of Certified Public Accountants (AICPA) that is utilized among publicly traded organizations to certify that they have put internal security controls in place to protect sensitive information. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent auditing firm which should provide reasonable assurance that the controls are functioning in a manner consistent with stated policies, and are in complies with applicable laws and regulations. It is a guide that allows service organizations a means of disclosing their controls to user organizations which represent reasonable assurance of compliance with regulations and provide a degree of confidence in the service provider's ability to conduct business securely.

A SAS 70 audit is intended to assist service/user organizations and their auditors by describing illustrative control objectives and controls that service organizations may have in place. When such controls are present and operating effectively, they may enable auditors of user organizations to assess their control risk which is affected by the service organization(s). This and other ancillary audits are gaining recognition in the corporate world largely due to the Sarbanes-Oxley (SOX) Act passed in 2002. This legislation was designed to restore investor confidence following several highly publicized corporate financial scandals ranging from bankruptcies to internal control breakdowns. "Overall, the SAS 70 is a demonstration of both the legal and business commitment to greater levels of reliability, availability and security" (Cronin, 2007).

In today's quick paced economy, it is necessary to assure a business of the security and integrity of their data particularly when outsourced to a third party organization. The SAS 70 audit is an internationally recognized auditing standard that provides reasonable assurance by examining, documenting, and preferably testing internal controls within service organizations.

Companies that execute and maintain accountability of transactions that impacts the user organization financial reporting are candidates for the SAS 70. Outsourcing of services is a viable alternative to many organizations because of its cost savings and gained expertise in the particular area of interest. The SAS 70 service auditor reports are used by user organizations, customers, prospective customers, and financers to gain an understanding of the control environment of outsourcing companies.

A user organization is a company that seeks outsourcing services by a third party that directly impacts financial reporting controls. They have responsibility and accountability by the Sarbanes-Oxley Act, for designing and evaluating internal security controls between the two organizations to ensure they meet the desired objectives. A key factor in determining if a user organization is effected by the new legislation is if they are required under the General Accepted Accounting Principles (GAAP) to include transactions processed by the service provider in their own financial statements (Deloitte, 2007). The SAS 70 is the accepted format under the Securities Exchange Committee (SEC) regulations for a user organization to analyze controls put in place by the service organization to ensure that there are controls in place, and they are working appropriately. The SAS 70 "has long provided the financial auditors of user organizations a standard by which they can understand the design and effectiveness of service organization controls and design tests of user organization control" (Deloitte, 2007).

STATEMENT ON AUDITING STANDARDS 70 (SAS 70) REPORTS

SAS 70 is a guide that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A formal report including the auditor's opinion, called a service auditor's report, is issued to the service organization at the conclusion of a SAS 70 examination. This report is an auditor to auditor communication between the service and user organization.

There are two different types of reports that are a result of a SAS 70 audit, a Type I and a Type II report. A Type I service auditor's report includes the service auditor's attestation of the fairness of the presentation of the service organization's description of controls that had been placed in operation and the suitability of the design of the controls to achieve the specified objectives (SAS70.com, 2007).

A Type I audit concentrates on the controls that are in place at a specific date in time and does not include testing the effectiveness of the controls in place. The depth of this audit is very limited, as it states the presentation and design of controls in place in terms of their ability to meet defined control objectives, but does not test its effectiveness. These reports occur over a one day period so they have limited value to a user organization. A Type II service auditor's report is the most thorough report of a SAS 70 audit because it contains a description of the controls in place, and also includes a description of the auditor's tests of control effectiveness for a minimum of a six month period. The Type II examination of the SAS 70 begins the same as Type I, but goes a step further into testing and observing. Type II analyzes the controls and also observes them in action rather than the Type I that just describes the controls in place. The Type II service auditor's report will state "whether the controls that were tested were operating with

sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified" (SAS70.com, 2007). A Type II service auditor's report is more common and also the preferred choice of SAS 70 because it is a more in depth analysis of not only what controls are in place, but how effective those controls are to meet the desired objectives.

TYPES OF SAS 70 REPORTS FOR SERVICE ORGANIZATIONS

SAS 70 reports represent an increasingly popular way for service providers and outsourcing service firms to calm their client or user organization's financial responsibility and compliance concerns. There are two types of SAS audits, both of which offer a report as the most essential product. Type I audit also referred to as a "Report on Controls Placed in Operation" and Type II audit also referred to as a "Report on Controls Placed in Operation and Tests of Operating Effectiveness" (AICPA.org, 2007). Type I audit includes: a description of detailed controls, whether the specified controls are suitably designed to achieve broader control objectives, whether the specified controls had been placed in operation as of a specific date and an auditor's opinion attesting to the information in the report, but containing a specific disclaimer of opinion on the operating effectiveness of the controls.

The Type II audit goes a step beyond the Type I report. In a Type II audit, the service provider's controls are tested over a six-month period of time to determine if they are in fact operating effectively. A Type II report includes the same assessment as a Type I report, while also including a thorough description of the tests applied and their results.

Service provider can, by their own choice, request either one of the reports. However it is important to understand that if service providers elect to obtain only Type I audit, which lacks the level of due diligence offered by a Type II audit as well as does not state whether the controls described by the service provider are operating effectively, the user organization's auditors cannot be reasonably assured that the service provider's control mechanisms actually work.

SAS 70 has grown in significance in recent years as companies strive to comply with heightened regulatory requirements. Federal legislation enacted in the wake of corporate accounting scandals and by public concern over the security and privacy of personal information has delineated new rules for the handling and reporting of data. The Health Insurance Portability and Accountability Act of 1996, the Gramm-Leach-Bliley Act of 1999, and particularly the Sarbanes-Oxley Act are examples of legislation that have had a strong impact on companies' auditing in addition, the popularity of outsourcing among today's businesses further drives the need for SAS 70 auditing (SAS 70.com). According to an article written by Christopher L. Schellman, co-founder of SAS 70 Solutions,

> "Many public companies, as part of their respective efforts to achieve compliance under Section 404, discovered that certain financial reporting controls that they relied upon were actually maintained by outsourced third-party service providers." (Schellman 2005)

That is to say, to be considered compliant a company must verify that its service provider's

controls, in addition to its own, are effective.

Compliance with Sarbanes-Oxley Act can become quite expensive. A survey conducted by Financial Executive International in 2004 found that the average cost of compliance in the first year with Section 404 was over $3 million. Although SAS 70 auditing can potentially help reduce costs by eliminating the need to send or use internal company auditors to assess rather service providers can provide auditors with a copy of their service providers' SAS 70 audit reports (FEI 2004). By successfully completing a SAS 70 audit, service providers can offer customers a valuable tool for planning and streamlining the audit of their financial statements. From the business perspective, having a SAS 70 audit completed signifies a commitment to quality by providing information about the internal controls and security practices of the service organization.

THE SARBANES-OXLEY ACT

The Sarbanes-Oxley Act of 2002 is responsible for the increased presence of a SAS 70 in the business climate. Its purpose is to protect the public and investors by improving the reliability and accuracy of corporate disclosures. This legislation was enacted as a direct result over public concern about the security and privacy of personal information and the misrepresentation of financial information by large corporations.

The SAS 70 audit is now becoming an industry standard on what is expected from organizations as it relates to internal controls in compliance with Sarbanes-Oxley. The Act regulated several areas in the business setting for publicly traded companies; an independent auditor must review the companies' financial information, it requires that public companies must evaluate and openly disclose their financial statements, management must report annually on the effectiveness of internal controls, CEO's and CFO's must certify and be held personally responsible for the integrity of financial reports, and added criminal and civil penalties for violations of the law dealing with securities fraud (tech-faq.com, 2007). In addition to these new mandates for publicly traded companies, the Public Company Accounting Oversight Board (PCAOB) was established, whose role is to oversee auditors of public companies and pressure them to become and remain compliant with regulations to ultimately help protect investors by ensuring a fair and independent audit process.

One of the most important and widely recognized sections of the Act is Section 404, as it relates to the SAS 70. It compels publicly traded companies to expand the use of SAS 70 to ensure the accuracy and effectiveness of the internal controls over financial reporting. Section 404 is responsible for holding CEO's and CFO's personally liable for the effectiveness of internal controls. The responsibility extends to controls in place at service organizations, forcing the CEO's and CFO's to analyze that the controls are functioning adequately as originally intended. The SEC has interpreted Section 404 as follows "In situations where management has outsourced certain functions to third party service providers, management maintains a responsibility to assess the controls over the outsourced operations" (Deloitte, 2007). The SAS 70 audit is designated by the SEC as an acceptable method for management to review the security controls in place for service organizations. As a result, SAS 70 is a preferred method to

provide user organizations with the necessary information on internal security among service organizations. Section 404 encourages publicly traded companies and service organizations to expand the use of SAS 70 audits to remain compliant with new regulations and holds management responsible for financial reporting misrepresentation. The Sarbanes-Oxley Act has required organizations to comprehensively analyze important security controls in place to ensure accurate reporting, or face civil and criminal penalties as a consequence.

SARBANES-OXLEY BUSINESS IMPLICATIONS AND REQUIREMENTS: AN ORGANIZATIONAL COMMUNICATION AGENT

While there is a clear need to have legislation present, the downside is that there has to be changes implemented and new systems created to comply with the new reporting and financial control requirements which are very costly. Publicly traded companies must in some cases undergo extensive changes in how earnings are reported, audit their business and improve process transparency. Public companies are required to change their financial reporting structure in numerous instances, which presumably benefits the investors. Depending on the nature of the business, an audit of this scope could take hundreds, possibly thousands of hours to complete, which is an enormous yet arguably necessary commitment from an organization to ensure thorough audit controls are in place and operational to ensure reasonable effectiveness.

SAS 70 AUDIT SCOPE

This audit tends toward being more comprehensive to any other audit simply because of the scope of the audit and the amount of abundant information available in the service auditor's report. The key components of assessing internal control for the SAS 70 audit consists of risk assessment, control environment and activities, information and communication, and monitoring of controls put into place (Nickel, 2007). The analysis of these areas should theoretically allow the auditor to gain a better understanding of the environment and culture of the organization.

The scope of the SAS 70 should be carefully planned and coordinated between the service organization and the user organization to ensure that all areas necessary are covered by the audit. It is essential that the two organizations communicate and coordinate the scope of the audit to be effective. Because of the unique nature of what information is generally covered in a SAS 70 audit there should be procedures, policies, and controls in place to monitor what the scope and outcome of the audit. This audit is specialized and can be a time consuming process, consequently, the entire organization normally does not go through the audit. Auditing the entire organization is not feasible given the amount of detail required and the scope of the audit. Instead, the identified areas that are being used to outsource activities related to the user organization are usually candidates for auditing. By mandate only a Certified Public Accountant (CPA) or an accounting firm is authorized to conduct a SAS 70 and issue a service auditor's report which is largely an IT audit report.

ADVANTAGES TO SERVICE ORGANIZATIONS

Although SAS 70 will increase a service organizations costs and responsibilities, it is an indicator of assurance that the company has reasonably effective controls over its operations.

> "A SAS 70 demonstrates that the infrastructure, applications and processes have passed rigorous, independent third party testing and have an environment that incorporates the processes and controls that are necessary for effectively hosting and/or exchanging corporate data and financial information" (Cronin, 2007).

This audit can build trust with existing customers, as well as attract new customers, because it portrays a company committed to quality improvement. Another positive attribute to the audit is that it will help the organization identify internal controls weaknesses and/or breaches. The SAS 70 process will allow the organization time (usually 6 months) to evaluate what security controls they have put in place and if they are in fact effective. When a service organization has committed the resources necessary to obtain a SAS 70 audit it is typically not necessary to repeat that process for other user organizations or clients, resulting in cost savings. Service organizations and service providers required by law to demonstrate that they have adequate controls when they obtain and process data belonging to their customers are using SAS 70 audits to satisfy such requirements. The SAS 70 is a useful tool to help communicate to customers that the necessary steps have been taken to implement and test security controls which are requisites to protecting and reporting accurate information.

ADVANTAGES TO THE USER ORGANIZATION

While there are many advantages to the service organization, a SAS 70 ultimately will benefit the user organization because they will gain a greater understanding of the service organizations internal controls. The service auditor's report is chock-full of information describing the service organizations specific controls, and in the case of a Type II audit, whether these controls are effective. SAS 70 reports are a useful tool for the user organizations' auditors when planning financial statements (www.tech-faq.com, 2007). Given this benefit, it is no longer necessary for the user organization to send their own auditors into the service organization since the service provider has already undergone a SAS 70 audit by an independent auditor. The service organization has taken the first steps in helping the user organization make a decision to use their services because they have taken proactive steps in implementing and testing their internal controls. Most importantly, user organizations are able to gain valuable understanding and assurance of the internal controls in place to protect its information and data.

SAS 70 AS A MARKETING TOOL FOR SERVICE ORGANIZATIONS

Although there are some widely criticized shortcomings in the SAS 70 audit process, it still holds some measure of credibility in the business culture. The audit can put one company at an advantage over another, as evidence of that, some organizations incorporate the overview section of their SAS 70 directly into their marketing material. The ability to provide a SAS 70 report has become a marketing tool to some organizations because it signals an organization

committed to quality by implementing and maintaining internal security controls. A SAS 70 represents to some extent a measure of assurance that a service organization is committed to illustrate their services is consistent, safe, and reliable and that they are compliant with the emerging regulatory mandates (Cronin, 2007).

SAS 70 symbolizes that the organization has taken the time and resources necessary to analyze the security controls to reduce the likelihood of financial loss or corruption of secure information, which user organizations expect from a service provider. In fact, with the growth from the Sarbanes-Oxley Act, user organizations are now expecting service organizations to provide them with a service auditor's report that attest to the reasonable assurance of their IT security controls. Some companies have effectively used their SAS 70 report as marketing tool to suggest the organization has implemented security controls and have tested the reliability and effectiveness of which those controls were designed to operate. Often such marketing tactics may suggest a good-housekeeping-seal-of approval, although a user organization should not assume that an unqualified opinion is synonymous with effective controls; it is the responsibility of the user organization to determine whether the controls were suitably designed to achieve specified control objectives.

SAS 70 CRITICISMS

A SAS 70 audit arguably holds various advantages both for the service organization as well as the user organization, but there are some flaws to the audit that is gaining attention and criticism for being an outdated audit. There are some fundamental problems that many believe need to be addressed to encourage consistency among a SAS 70 audit. One potential problem that the audit has is that there is no predetermined set of standards that the audit must have which result in inconsistencies or allow an auditor to omit information that might be of importance. SAS 70 audits is not a standardized checklist of items that must audited, therefore one service auditor's report of an organization could be completely different if another auditor conducted the same audit. This leaves room for human judgment and error(s) which could potentially give a service and user organizations a false sense of security that the internal controls is effective. A Type II audit goes into tremendous detail, but it does not guarantee absolute compliance with Sarbanes-Oxley only reasonable assurance.

Moreover the timing of the audit could lead to potential problems if the service organization and the user organizations' reporting period differ. If the audit is conducted in June and the user organizations' fiscal year ends in December, there is potentially a period of 6 months that is not accounted for. If the controls are lax in that time frame, it could compromise the accuracy and reliability of the financial statements of the user organization (Schneider, 2004). Yet another potential problem of the audit is only a CPA or an accounting firm is permitted to conduct the audit, which arguably, accountants educational training usually lacks the use of technology involved in security controls. Understanding how outsourcing services use of technology may affect user organizations' financial statements is an integral part of security controls audit.

Another concern centers on how much of the audit is required to be revealed. The service organization is only required to report the failures of the SAS 70 test and does not have to

include the scope that the audit covered, which could lead to potential problems for the user organization (Schneider, 2004). All of which brings into question how to ensure the SAS 70 audit will serve the needs to both the user and service organizations.

SAS 70 IT AUDITING AND ORGANIZATIONAL CHANGE

A conceptual model provides a theoretical foundation for a study and guides research toward critical questions (Van De Ven, 1989). The Conceptual Model (Figure One) synthesizes recent organizational change literature to include ideas from the rational, learning, and cognitive theories on organizational change (Rajagopalan & Spreitzer, 1997). The model illustrates the dynamic interplay of endogenous, exogenous, managerial, and learning factors inherent in the organizational change process. The model acknowledges the direct effects of the environment and organization on changes in strategy; recognizes that changes in the content of strategy must match the requirements of a firm's environmental and organizational contexts in order to be successful; acknowledges the crucial role played by managerial actions in creating an environmental and organizational context conducive to a firm's strategies; depicts managerial learning as a continuous reshaping of managerial cognition that develops as outcomes from changes in strategy begin to emerge; and, acknowledges that changes in the content of strategy result from both variations in contextual conditions and from variations in managerial cognition and actions (ibid.)

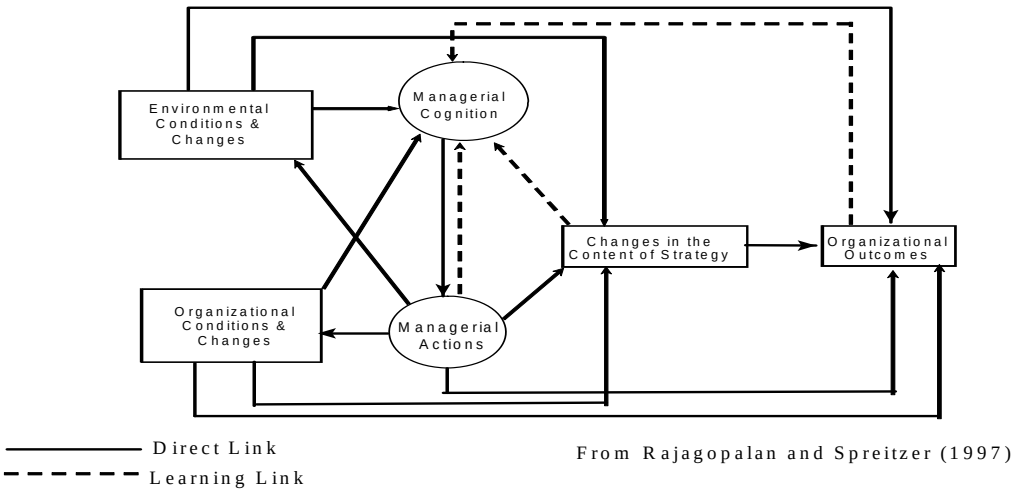

Figure 1: Conceptual Model

Employing an organizational change model to study the audit process from an information security perspective is appropriate because while corporate IS security models have historically emphasized the role of management in setting, maintaining, and implementing security policies, procedures, and standards, businesses are also developing organizational structures and operational procedures surrounding technologies (Segev et al., 1998). This has included setting up basic safeguards such as insurance, audits, system application controls, physical protection

systems and surveillance devices as well as developing contingency and disaster recovery procedures. In a recent case study of Bank of America an employee noted, "the key to security … lies not with the technology, but with the organization itself" (ibid. p. 85).

The first step in this research was to integrate information security and privacy issues found during the SAS 70 engagement into the conceptual model. These constructs capture an organization's external and internal information security environments, manager's perceptions about information security, changes to organizational processes resulting from increased security concerns, and organizational outcomes resulting from IT security initiatives. The research began by performing a qualitative content analysis of the existing literature. The literature review took the form of first noting the ideas of consideration in each research paper or article then organizing these topics into the related constructs (Detert et al., 2000).

To validate the classification of issues discussed in extant literature and to ensure no important information security issues was omitted; interviews will be conducted with several information security senior executives directly responsible for the information security strategies of their organization. The initial organization of topics will be presented to each interviewee in separate one-hour meetings and their feedback will be used to further refine the research. Table 1 constructs will summarize the results findings. Particular emphasis will be given to isolated those issues specifically applicable to third party services.

CONSTRUCT	IDEAS ABOUT INFORMATION SECURITY
Environmental Conditions & Changes	Current and pending legislation • Sarbanes-Oxley Act • Gramm-Leach-Bliley Act of 1999 • Health Insurance Portability and Accountability Act (HIPAA) • U.S. Patriot Act of 2001 • Corporate Information Security Act of 2003 • Children's Online Privacy Protection Act • Identity Theft Prevention Act • Privacy Act of 2003 • Federal Information Security Act of 2002 • Other International, Federal, State, and Local laws/regulations Technology vulnerabilities • Generally inadequate technology standards for secure computing • Wi-Fi protocol security flaws (Housley & Arbaugh, 2003; Schmigt & Townsend, 2003) & Wireless Equivalent Privacy (WEP) vulnerabilities (Cam-Winget et al., 2003) • Information systems threats (Hulme, 2004) • Viruses, trojans, worms, denial-of-service attacks • Unauthorized data access/disclosure

CONSTRUCT	IDEAS ABOUT INFORMATION SECURITY
	• Electronic criminal acts (Sullivan, 2004) • Identify theft/internet fraud/Phishing • Other fraudulent schemes • Other employee criminal acts
Organizational Conditions & Changes	Secure distributed corporate data • Across supplier/outsourced networks • Across N-Tier & remote networks such as mobile computing Data assurance • Internal security controls/audit requirements • Enforcement of Human Resource and other company policies • Organizational Culture • Internal Software Vulnerabilities • Software bugs/errors/omissions/back doors
Managerial Cognition	Current Managerial Concerns (Melymuka, 2003) • Economic growth, profit margins, and competitive threats • Supplier/customer relations • Legal penalties • Shareholder concerns Perceived Security Priorities for the Future (InformationWeek, 2003) • Raise user awareness of policy and procedures • Train/retrain/attract qualified staff • Security review and assessment • Data ownership and classification standards • Incident response teams
Managerial Actions	Managerial oversight (Segev et al, 1998) • Setting, maintaining, and implementing security policies, procedures, and standards • Increased hiring of certified security professionals • Increased training Installation of security hardware & software (CSO, 2004) • Biometrics/smart cards/other access controls • Firewall applications/VPNs/ intrusion detection and prevention systems • Certificate authorities/encryption • Secure e-mail/web filtering/enterprise security management

CONSTRUCT	IDEAS ABOUT INFORMATION SECURITY
	Acquisition of security services (CSO, 2004) • Consulting/managed security services • Digital forensics/disaster recovery/business continuity • Penetration testing and other outside audit services Installation of physical security devices (CSO, 2004) • Integrated systems/monitoring equipment • Alarms, burglar/fire electronic, CCTV & surveillance systems • Perimeter security/Access Controls Other managerial actions • Wireless/mobile security
Changes in the Content of Strategy	Risk Management (Segev et al., 1998) • Contingency/disaster recovery plans • Continuity plans • Insurance/Audits Development of new business units • Centralized IT Security Council (Fisher, 2004) New business groups (Segev et al., 1998)
Organizational Outcomes	Customer Retention (Culnan & Armstrong, 1999) Loss Prevention • Reduce unauthorized access/service attacks • Reduce loss of data/unauthorized disclosure • Improve data accuracy • Litigation avoidance Improved Business Processes (Fonseca & McCarthy, 2003) Public Perception

Table 1: Information Security/Privacy Concerns

PROPOSED QUESTIONS FOR FUTURE RESEARCH

A number of interesting research questions emerge from this conceptual analysis. Sarbanes-Oxley legislation is an excellent example of current legislation mandating organizational change. The author believes that a proactive information security strategy would provide substantial positive benefits. The first proposed research question explores this idea: What are the advantages and disadvantages of having a proactive (internally driven) versus reactive (externally driven) strategic approach to the information security issues related to SAS 70 audits?

Second, based on audit interviews management is concerned with the negative consequences of security breaches, but that security issues are considered secondarily, which exposes the organization to considerable risk. The second research question is: How can executive awareness of security issues and best practices related to SAS 70 audits be raised and how can security personnel better communicate the level of threats?

Third, while discussing security implementations, the management indicated that they encounter substantial resistance among organizational members. Executives often demand to be excluded from even simple security measures like having to regularly change their passwords and others within the organization find ways to circumvent controls. For those trying to successfully protect information assets this is very frustrating because even though they are held responsible for systems security, they usually have little direct authority to enforce security policies. The third research question addresses this issue by asking: What are the characteristics of an organization's culture that must be adhered to in order to establish and maintain successful governance of its information security strategies related to requisite organizational change needed to address SAS70 audit results?

CONCLUSION AND SUGGESTED METHODOLOGY

To investigate the research questions posed, the author suggest using a case study approach of a service provider in the throes of a SAS 70 audit; culled information observed, recorded and analyzed for stages of patterns in relation to internal and external influences. This case study will involve unstructured interviews and ethnographic methodology (meaning the subject is allowed to express themselves in their own words).

Examining the implications of a SAS 70 audit from this perspective accommodates people's situated use of technologies making no assumptions about the stability, predictability, or suggested changes needed to address audit findings. This study of information security controls employed by services providers and evaluated via the SAS 70 audit process is important because "…As corporations continue to cede control over their IT applications and networks to vendors and other third parties, the threats they face will proliferate. They need to prepare themselves for technical glitches, outages, and security breaches, shifting their attention from opportunities to vulnerabilities" (Carr, 2003). Perhaps the requisite benefit of a SAS 70 audit is not fully realized without adequate commensurate organizational change. Further the SAS 70 process is a tool which focuses attention on risks and vulnerabilities encountered by end-users when using technologies as they were designed, they also can and do circumvent inscribed ways of using the technologies – either ignoring certain properties of the technology, working around them, or inventing new ones that may go beyond or even contradict designers' expectations and inscriptions (Orlikowski, 2000).

REFERENCES

"About SAS 70." < http://www.sas70.com/about.htm>

Austin, R. D. and C. Darby (2003), "The Myth of Secure Computing," *Harvard Business Review*, 81(6), pp.120 –126.

Cannon, David M., and Glenn A. Growe. "How Does Sarbanes-Oxley Affect Outsourcing?" Journal of Corporate Accounting & Finance 16 (2005): 13-20.

Carr Nicholas G. (2003), "IT Doesn't Matter," Harvard Business Review, Vol. 81, No. 5, May 2003.

Cam-Winget, N., R. Housley, D. Wagner, and J. Walker (2003), "Security Flaws in 802.11 Data Link Protocols," *Communications of the ACM*, 46 (5), pp. 35 – 39.

CSO, "CSO Survey," *CSO Online*, January 16.

Cronin, Phillip. "Understanding the Many Benefits of a SAS 70." Polar Cove White Papers: Professionals Dedicated to Enterprise Security and Client Satisfaction. 26 June 2007. <www.polarcove.com/whitepapers/benefitsofsas70.htm>

Culnan, M. and P. Armstrong (1999), "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," Organization Science, 10(1), pp. 104 – 115.

Detert, J., R. Schroeder, and J. Mauriel (2000), "A Framework for Linking Culture and Improvement Initiatives in Organizations," *Academy of Management Review*, 25(4), pp. 850 - 863.

Fisher, D. (2004), "Agencies Beef Up IT Security," *eWeek*, January 5, pp. 9 – 10.

Fonseca, B. and J. McCarthy (2003), "Identity Management: Technology of Trust," *Infoworld*, June 23, pp. 55 – 61.

Housley, R. and W. Arbaugh (2003), "Security Problems in 812.11 – Based Networks," *Communications of the ACM*, 46 (5), pp. 31 – 34.

Hulme, G. (2004), "Security Threats Won't Let Up," *Informationweek*, January 5, pp. 59 – 62.

InformationWeek (2003), "What's to Come," November 10, pp. 116.

Melymuka, K. (2003), "Too Much To Do!," *Computerworld.com*, January 2.

Nickel, Christopher, and Charles Denyer. "An Introduction to SAS 70 Audits." Benefits Law Journal. Vol.20 No.1: Pg 58-68.

Orlikowski, W. (2000), "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations," *Organization Science*, 11(4), pp. 404 – 428.

Panda, B. and J. Giordano (1999). "Defensive Information Warfare," *Communications of the ACM*, July, 42(7), 30 - 32.

Rajagopalan, N. and G. Spreitzer (1997), "Toward a Theory of Strategic Change: A Multi-lens Perspective and Integrative Framework," *The Academy of Management Review*, 22(1), 48-79.

Schmidt, T. and A. Townsend (2003), "Why WiFi Wants to be Free," *Communications of the ACM*, 46 (5), pp. 47 – 52.

Schneider, Chris. "A World of Trouble: Even with an extended deadline for Sarbox compliance, questions about offshoring on edge." CFO Magazine. Spring 2004

Segev, A., J. Porra, and M. Roldan (1998), "Internet Security and the Case of Bank of America," *Communications of the ACM*, 41(10), pp.81 – 87.

Sullivan, A. (2004), "Identity Theft, Internet Fraud Reports Up in U.S.," *Reuters*, January 22, 2004.

"The New Landscape." SAS 70 in the Sarbanes-Oxley Era. Deloitte. Pg 1-7. 2007

<http://www.cfo.com/article.cfm/3012421/c_3046608> Tech FAQ. 24 June 2007. http://www.tech-faq.com

Van De Ven, A. (1989), "Nothing is Quite So Practical as a Good Theory," *Academy of Management Review*, 14(4), 486 - 489.

Lanz, Joel. "Incorporating SAS No. 70 and Other Reports Into a Vendor Management Program." RMA Journal 86 (2004): 40-45.

Cannon, David M., and Glenn A. Growe. "How Does Sarbanes-Oxley Affect Outsourcing?" Journal of Corporate Accounting & Finance 16 (2005): 13-20.

Schellman, Christopher L. "SAS No. 70: Evaluating Service Organizations' Internal Controls Is Key To Section 404 Compliance," Florida CPA Today, November 4, 2005

Schellman, Christopher L. "A SAS 70 Auditor's Response to the Critics." SAS70Solutions.Com. 2001 SAS 70 Solutions, Inc. 18 June 2007 <http://sas70solutions.com/SAS70-AudtorsReponsetotheCritics.html>.

FEI, “FEI Special Suvey on Sarbanes-Oxley Section 404 Implementation Executive Summary,” FEI.org July 2004 <http://www.fei.org/files/spacer.cfm?file_id=1133> June 26, 2006

Gossels, Jonathan G. "SAS 70: the Emperor Has No Clothes." SystemExperts.com 2001. June 27, 2007 <http://www.systemexperts.com/tutors/sas70.pdf>.

"Statement on Auditing Standards (SAS) No. 70." SAS70.Com. 10 June 2007. June 23, 2007 < http://sas70.com/index2.htm>

“Summary of the Provisions of the Sarbanes-Oxley Act of 2002." AICPA.Org. 2002. June 23, 2007
<http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/Summary+of+the+Provisions+of+the+Sarbanes-Oxley+Act+of+2002.htm>.