2014

Service Organization Control Audit Series: The Need for a Uniform Process of Verification of Service Organizations' Internal Controls and the Implementation of This Process

Kati Nance

Follow this and additional works at: http://commons.emich.edu/honors

Recommended Citation
http://commons.emich.edu/honors/420

This Open Access Senior Honors Thesis is brought to you for free and open access by the Honors College at DigitalCommons@EMU. It has been accepted for inclusion in Senior Honors Theses by an authorized administrator of DigitalCommons@EMU. For more information, please contact lib-ir@emich.edu.
Service Organization Control Audit Series: The Need for a Uniform Process of Verification of Service Organizations' Internal Controls and the Implementation of This Process

Abstract
This thesis documents, through research, the vital elements concerning risk management, internal controls, and the external audit process. It focuses on the need for organizations to have a valid check of the internal controls of their service organizations, and how the SOC audit series has provided a unified method.

Degree Type
Open Access Senior Honors Thesis

Department
Accounting and Finance

First Advisor
Jens Stephen

Keywords
COSO-integrated framework, external auditor, financial reporting, outsourcing, trust service principles
SERVICE ORGANIZATION CONTROL AUDIT SERIES: THE NEED FOR A UNIFORM PROCESS OF VERIFICATION OF SERVICE ORGANIZATIONS' INTERNAL CONTROLS AND THE IMPLEMENTATION OF THIS PROCESS

By

Kati Nance

A Senior Thesis Submitted to the

Eastern Michigan University

Honors College

in Partial Fulfillment of the Requirements for Graduation

with Honors in Accounting.

Approved at Ypsilanti, Michigan, on this date \(12/16/14\)
# Table of Contents

**INTRODUCTION**  
1

**RISK MANAGEMENT & INTERNAL CONTROL**  
3

The purpose of this section is to teach the reader the nature of risks involved in conducting business with the external environment and the importance of understanding the various risks that may affect each business. Internal controls are needed in order to manage these risks efficiently. In an effort to assist businesses with this process, COSO has established an integrated framework.

**ENTERPRISE RISK MANAGEMENT**  
**INTERNAL CONTROL: A BRIEF HISTORY**  
**INTERNAL CONTROL-INTEGRATED FRAMEWORK-COSO**

**EXTERNAL AUDITING**  
10

The purpose of this section is to inform the reader of the role of the external auditor, how that purpose has become increasingly important as the business environment has become more intricate over time, and how different agencies have impacted this role.

**A BRIEF HISTORY**  
**BUSINESS ENVIRONMENT TRENDS**

**SSAE 16 & THE SOC AUDIT SERIES**  
17

The purpose of this section is to enhance the reader's understanding of the newly implemented audits and how these audits have impacted various different professionals involved in the process.

**DESCRIPTION AND EXPLANATION-SSAE 16 & SOC I, II, III**  
**INTERVIEW-EXTERNAL AUDITOR**  
**INTERVIEW-COMPLIANCE OFFICER**  
**INTERVIEW-CHIEF FINANCIAL OFFICER**

**CONCLUSION**  
37

**WORKS CITED**  
39
Introduction

In today's fast-paced, cost-cutting, information-technology dependent business environment, it has become increasingly important for businesses to safeguard against external risks. One vital method of reducing the threat of these risks is to form and implement a set of internal controls. These internal controls not only need to ensure accurate financial reporting, they also need to reduce the loss and misuse of sensitive information. As businesses attempt to cut costs and reduce internal support service expenses, the tendency to employ external service organizations is increasing. Businesses are outsourcing services that have a direct effect over financial reports as well services in which confidential customer information is provided. It is the responsibility of the user organization to verify the internal controls of its service organizations. In 1992, the American Institute of Certified Public Accountants (AICPA) created the Statement of Accounting Standards number 70 (SAS 70.) SAS 70 served as the accepted authority over verification of service organizations' internal controls over financial reporting. SAS 70 was the standard until 2011 when the AICPA issued the Statement on Standards for Attestation Engagements (SSAE) No. 16 and the new Service Organizational Control
(SOC) audits. SSAE No. 16 would be SOC I and provide guidance over internal controls over financial reporting. A completely new type of audit, SOC II, would provide a means of verifying internal controls over other factors, as defined by the Trust Service Principles. These would be controls over the security, availability, privacy, confidentiality, and processing integrity employed by the service organization when handling sensitive information. SOC III would be revised version of an entity’s SOC II audit in which any confidential information is removed and made available for use by the public.

This thesis is not only a study of the evolution of the external audit, it is also a series of first-hand account experiences with conducting and implementing these audits. One interview is from the perspective of an external auditor, Mr. Kirk Balcom, CIA, CISA, CFE and Principal at Rehmann Consulting. Mr. Balcom has conducted SAS 70 audits and each of the SOC audits. A second interview was conducted with Ms. Pfeiffer, the compliance officer at Highland Solutions. Highland Solutions recently completed a successful SOC II type one audit, and is currently undergoing a SOC II type two audit. The last interview was conducted with Mr. Mark Laser, the Chief Financial Officer of yB Management, LLC, a company that recently underwent a successful SOC I type I audit, and is in the process of implementing a type two audit.

The research component of this study is intended to provide a clear explanation of the trends that led to the implementation of the SOC audit. The interviews are intended to provide first-hand accounts of experiences professionals have had implementing these audits.
**Risk Management and Internal Control**

**Enterprise Risk Management**

This section outlines the continuous process of risk management. It explains the importance of risk management and its effect on the business' successful fulfillment of established objectives. While risk management has been practiced for decades, the idea of Enterprise Risk Management was recently created in an attempt to provide transparency to the risk management process.

Today’s business environment rapidly changes, and new risks that may alter a business’ position appear daily. Businesses need to perform a continuous effort to manage risks. In order to manage risks, businesses must create and implement appropriate objectives. There are four types of objectives: strategic, operating, reporting, and compliance. Operating objectives are needed to ensure that the company is operating efficiently and in accordance with the business’ strategic objectives. Reporting objectives are needed to establish ethical guidelines for financial reporting, and compliance objectives are needed to provide guidance in remaining within the boundaries of the law. Once objectives are created, proper internal controls need to be formed, implemented, and monitored. The task of forecasting and forming objectives for success in tomorrow’s market place can be a daunting task. However, resources are available to assist businesses in this process. For example, Enterprise Risk Management has been created in order to provide businesses with guidelines in managing risks that may affect their objectives. First, the organization must understand its unique risk circle.
According to Sobel and Reding (2012), the risk circle is characterized by a continuous cycle, beginning with a company’s objectives, followed by uncertain and unforeseen events, outcomes, and effects and looping back to objectives. As a business travels through this unpredictable cycle, it becomes necessary to revise objectives or create new ones entirely. (p. 10-12). Risks can be either positive or negative. Risk management for any business can be used to either reduce the threat of negative events or take advantage of positive ones. Risk management must be a collective effort by all decision makers in the organization. Risk management tactics must be done continuously and must be flexible as new events are always occurring in both the internal and external environment. Risk management practices for any business must consider that business’ risk profile and risk appetite. The former being the set of unique risks that each company faces, and the latter being the level of risk that each company is willing to accept.

Risks can affect any of these four categories of business objectives: compliance, reporting, strategic, and operations objectives. Proficient managers consider potential risks that are relevant to all aspects of their business, including policies and procedures, valued assets, employees, information systems, and technological resources. In order to successfully manage risks, a business must establish processes for governing an enterprise risk management system, a proper set of internal controls, and daily progress of objectives. An enterprise risk management system is essential in ensuring that daily activities are aligned with objectives, and an enterprise risk management system needs a proper set of internal controls in order to be effective. According to Enterprise Risk Management: Achieving and Sustaining Success, “Enterprise Risk Management (ERM) is an integrated, entity-wide system that addresses the organization’s portfolio of risks in
a manner that creates and protects value, and provides assurance that objectives will be achieved,” (Sobel & Reding, 2012, p. 21). Internal controls that businesses implement in order to take advantage of positive events are considered value creation, while internal controls that minimize the threat of negative events are considered protection from value destruction.

ERM practices in an organization must include the board, who makes ultimate decisions over objectives, risk management, and internal controls; employees who must operate within the determined boundaries; and the internal auditor who provides an independent, objective assessment of the company’s ERM and communicates ways in which to improve. It is key that the auditor does not interfere with the actual processes involved in creating and carrying out ERM, as the primary responsibility of the internal auditor is to maintain an objective position for effective analysis.

Management is responsible for informing each employee of decisions that affect daily operations in order to ensure achievement of objectives and commitment to company strategies. Management is also responsible for determining the company’s risk appetite, making and implementing any decisions based on risk management, and monitoring risk management. The likelihood and potential impact of each risk should be determined, in order to effectively prioritize risk management. Management should form clear, measurable, performance objectives that guide daily operations and encourage continuous compliance for each functional area. During the early stages of management procedures, management should create a complete set of internal controls.

This section has documented in broad terms the vital components and characteristics of maintaining an effective risk management system. It has explained the
important role that management plays in this process, and the importance of organization-wide acceptance and participation.

Internal Control: A Brief History

This section outlines the purpose of internal control in the risk management process. It acknowledges that, while complete elimination of risk is not practical, proper internal controls minimize risk to an acceptable level.

Internal controls are essential tools for fulfilling company objectives. According to The Business Dictionary, internal controls are:

“Systematic measures (such as reviews, checks and balances, methods and procedures) instituted by an organization to (1) conduct its business in an orderly and efficient manner, (2) safeguard its assets and resources, (3) deter and detect errors, fraud, and theft, (4) ensure accuracy and completeness of its accounting data, (5) produce reliable and timely financial and management information, and (6) ensure adherence to its policies and plans.”

Internal controls ensure efficiency, decrease the chances of misuse or misallocation of limited resources, reduce material misstatements in financial reporting, and increase company-wide compliance to all policies and plans. Internal control is not an end-result, but rather, a process that is continuously changing in order to adjust to an ever-changing business environment.

Risk management is intended to provide reasonable assurance; there cannot be absolute protection against all risks. Attempting to eliminate all potential risk would drastically limit potential opportunities, and consequently, harm a company’s success as
greatly as not having established internal controls. The likelihood and impact of each control must also be considered in order to prioritize controls. Each company’s risk appetite will help define which risks are acceptable because probable benefits outweigh possible negative consequences, which risks need to be transferred (i.e. through an insurance policy) and which risks can be reduced through appropriate controls. The most significant risks, however, are ones that are likely to have a devastating impact on the company’s position. Creating controls to avoid these risks will be of top priority.

For any organization to ensure effective implementation of its control activities, it must create a control environment conducive to ethical behavior and commitment to company objectives. A vital key in creating an effective control environment to increase company-wide compliance with ethical standards is for management to demonstrate behaviors in alignment with expectations for employees. The control environment is the first of five components of internal controlled as determined by COSO, Internal Control-Integrated Framework.

This section has highlighted the vital components and activities involved in establishing and implementing internal control. The most important control being an ethical control environment.
Internal Control-Integrated Framework-COSO

This section outlines the guidance provided by Internal Control-Integrated Framework. The Framework can be visualized as being a three-dimensional cube representing the interaction between an organization's objectives, control components, and divisions.

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued the first Internal Control-Integrated Framework in order to establish a unified framework for all organizations. Before this issuance, companies used individual tactics for internal control, such as segregation of duties, however, the framework was needed to create a standard for which to hold companies accountable for creating and maintaining internal control. Many changes have been made to the framework since 1992 in order to adjust to a quickly evolving business environment. The committee recently announced another revision to be released shortly, but it is not yet available to the public. Therefore, businesses are still referring to the 2013 framework.

Proper internal control needs to consider many different aspects of the business and its environment. Larry Rittenberg, PhD, CIA, CPA, Chair Emeritus, COSO, author of COSO Internal Control-Integrated Framework, explained the 2013 COSO Cube. This cube is a three dimensional image used to demonstrate the interaction between a company's objectives (shown across the top), the five components of internal control shown across front, and its divisional areas (shown on the side). Only operational, reporting, and compliance objectives are in the framework, as the committee found that strategic objectives should be a precondition to forming internal controls. The five components of internal control are the control environment, risk assessment, control
activities, information and communication, and monitoring activities (pp. 9-11). The divisional areas along the side are to illustrate the importance of each level within an organization adhering to internal control processes.

The five components that compose the framework include the control environment, risk assessment, information and communication, control activities, and monitoring. The first and most vital of these components is the control environment. The structure and discipline as related to both technical competence and accepted ethical practices determines the environment. In the process of determining relevant internal controls, the agency must assess all potential risks. External and internal risks are identified; objectives are set as to the acceptable level of risk protection, and controls are created to ensure the achievement of those objectives. Lastly, the company determines whether its control activities will be either preventative or detective. The agency then balances information and communication controls between the amount of information the organization must share internally and the needed extent of monitoring procedures to minimize external threats.

The internal auditor is responsible for providing objective opinions concerning control activities and advising management on ways in which to improve upon internal control activities. However, given the impact of internal controls upon a company's success, there is frequently a need for an external auditor to provide testing of defined internal controls. An external auditor may be hired in ordered for the company to verify its internal auditor’s judgments or to provide proof to external parties concerning the company’s compliance with legal and ethical standards.

This section documented the various components of the Framework.
External Auditing

A Brief History

This section introduces the role of the external auditor, highlights the interaction between the organization and the external auditor, and explains how the responsibilities of the role have changed along with the business environment.

In 1933, upon the issuance of the Free Securities Act, corporations that offered shares on the public stock market were required to undergo audits from independent auditors. Thus creating the position of the external auditor. In October 1958, the Committee on Auditing Procedure of the American Institute of Certified Public Accountants issued the Statement on Auditing Procedures number 29 titled the "Scope of the Independent Auditor's Review of Internal Control." The purpose of this statement was to determine the range of authority an independent auditor had during such procedures as studying, evaluating, and offering an opinion on the reliance of the internal controls of an organization. Many events have occurred in the business environment that have increased the need to verify an entity’s internal controls, and thus, increased the importance of the independent, or external, auditor.

Each agency determines its set of business objectives relating to each level of management and functional level of the business. Until fairly recently, all relevant controls in accounting standards related to an entity's controls over its financial reporting and related topics. These topics included: operating efficiently; safeguarding assets; complying with laws and regulations; and reporting complete, accurate, and unbiased financial statements. Internal control is a continuous process in order to limit a business' vulnerability to constantly emerging risks. Even when a company continuously monitors
its risk management activities, controls may fail to achieve the intended objectives. Therefore, frequent tests are needed to verify the integrity of internal controls. For various reasons, such as compliance with laws and regulations, internal reassurance, and to establish credibility with potential stakeholders, companies undergo external audits. CPAs conduct these audits that are independent of the business. These audits may be a snapshot evaluation of the firm’s position at a certain point in time or a continuous testing process over a certain period, normally an annual or semi-annual period.

In addition to the time frame variance, there are also two different strategies for completing external audits. One method is the substantive audit. During a substantive audit, the external auditor, gathers, interprets, and analyzes vast amounts of evidence. Items examined include ledgers, journals, and other documents, to determine if all financial reports, transactions, and accounts are in agreement and if any material misstatements have occurred. This method is very extensive and can place a substantial financial burden on the firm. The second method is the reliance strategy. In a reliant audit, the auditor relies upon the firm’s internal controls and determines if those controls are relevant for and capable of achieving their defined objectives. Previously, this method only required that the external auditor was made fully knowledgeable of the firm’s controls and objectives and was able to provide an accurate opinion of the accuracy and efficiency of those controls. If the external auditor was able to attest to the integrity of the internal controls, then it was assumed that financial statements were being reported accurately. However, new types of audits have been implemented that require that the external auditor test and verify the accuracy and appropriateness of the controls.
This section outlined the creation and evolution of the external auditor’s role in the business environment, the different responsibilities of the external auditor, and the different methods that are used during an external audit.

**Business Environment Trends**

This section outlines different trends in the business environment and how those trends have affected organization’s risk management efforts. The modern business world is one that is constantly changing as technical innovations, security concerns, and cost-cutting efforts have resulted in ever-increasing risks.

In a reaction to upsetting corporate scandals, such as Enron and WorldCom, Congress created the Public Company Accounting Oversight Board (PCAOB) and enacted the Sarbanes-Oxley act (SOX) of 2002. SOX placed significantly more responsibility on top management of all firms to attest to and guarantee the accuracy and completeness of their financial reports. Top management were required to be knowledgeable of relevant financial information and to provide reasonable reassurance that their financial reports were free from material misstatements. There were significantly higher costs involved in maintaining compliance, such as external auditor fees and board compensation. While SOX placed a heavy burden on many corporations, there were also benefits for companies that complied with SOX. Companies gained protection during litigation and heightened attraction from potential investors. One trend that has affected the ability of a company to guarantee sufficient controls over financial reporting is the increasing popularity of outsourcing.
During the great recession from 2007 to 2009, the demand for many companies’ goods and service decreased and numerous organizations were faced with the need to cut internal costs in order to maintain profit margins. Additionally, the business environment became one of a global economy, and companies faced increased competition from countries that operated with significantly lower internal costs. This increased the need to reduce internal costs in order to sustain desired profit levels. Many firms began downsizing their internal workforce. This increased the need for firms to outsource many functions that were once performed within the organization. Organizations that provide services for outside entities are referred to as service organizations. The user entity now had the added responsibility to verify their service companies’ internal controls. The outsourced services were often either directly related to the user companies’ financial reporting activities or required the sharing of confidential information concerning the company, its clients, or both. User organizations needed to ensure that their service providers were capable of meeting their objectives. Service providers were required to undergo external audits carried out by each client’s internal auditors.

The user company’s internal auditor(s) would work with the service organization’s internal auditor(s). Due to the cost and time constraints of a substantive audit, the external auditors normally used the reliance strategy. Each user company has its own distinctive set of objectives and the service organization needed to create and implement internal controls that were capable of meeting each client’s unique objectives. Consequently, service organizations faced the burden of undergoing numerous external audits in order to verify the internal controls that were relevant for each client’s objectives.
In order to simplify this process and reduce the costs involved, in 1992, the American Institute of Certified Public Accounts (AICPA) issued the Statement of Accounting Standards number 70 (SAS 70). This standard became widely accepted as verification that a service organization had undergone an in-depth external audit conducted by a SAS 70 approved external auditor. The auditor would test the relevance and accuracy of the company’s internal controls, and provide an opinion related to that company’s user organizations’ control objectives. SAS 70 provided service organizations the ability to offer reassurance concerning the validity of their internal controls to each user organization and their internal auditors in a uniform format.

SAS 70 was not legally required. Service organizations either implemented SAS 70 compliant external audits to give them a competitive edge over similar service organizations or were required by their clients to provide proof of a successful SAS 70 approved audit. There were two types of SAS 70 audits. During a type one SAS 70, the auditor was required to attest to the presence and suitability of the service organization’s internal controls. This type of audit did not require an assessment on the reliability of these controls, it was simply an affirmation that they were in place. A type two SAS 70, however, was a test of the reliability and accuracy of these internal controls. During the first step of this process, a CPA, external auditor, conducted a test on one item from each control. Then, the auditor determined if the controls were functioning as claimed and were achieving their intended purposes with minimal variance. The external auditor then wrote an opinion either attesting that the controls were operating as intended or that they were found to be inoperative.
SAS 70 unfortunately had a few shortcomings. For example, SAS 70 guidelines had not developed a standard set of controls for organizations, even for those within the same industry. A service organization's senior management decided which internal controls they wanted to define and test. There were no official guidelines or restrictions on these controls. Service organizations' SAS 70 audits varied greatly from one another. Consequently, these audits failed to provide any type of comparability between service organizations. Additionally, user organizations began relying too heavily on the assurance that a service organization had undergone an audit in compliance with SAS 70. Despite the fact that these audits were only to verify an entity's internal controls as related to financial reporting, reliance over other factors of control, such as security and privacy, were placed on these audits.

There was a need to implement internal controls that could ensure the achievement of other important objectives. As a result of various technological innovations, there had been a rise of internal-control breakdowns, which had led to various types of fraud and privacy breaches. Private, sensitive information was being accessed from what were believed to be secure databases. The ever-increasing global economy and the availability of vast amounts of sensitive information on the internet made the task of maintaining proper controls even more difficult. Congress had established acts such as Gramm-Leach-Bliley Act (GLBA), the Health Information Technology for economic and Clinical Health (HITECH), and the Health Insurance Portability & Accountability Act (HIPAA). These new acts required organizations to implement, test, maintain, and verify proper internal controls that were needed to ensure accessibility, security, and processing integrity of processes that guaranteed the privacy
of their clients. Companies that outsource functions to service organizations are also responsible for verifying the service organization's internal controls as they relate to their client's privacy. At this time guidelines and requirements had not been determined.

While there were many limitations on the auditing process at this time, many improvements had been made since Congress passed the Free Trade Act in 1933 and introduced the need for each company to establish a set of internal controls. The auditing process has become an interaction between management, staff, internal auditors, and various external auditors. Effective internal auditors are mainly concerned with preventive control activities but are responsible for detective activities as well. External auditors are responsible for detective activities and examining areas in which organizations established controls may be ineffective and therefore responsible for material misstatements on financial reports. Although there seemed to be an adequate system, as explained, many issues had not yet been addressed.

This section introduced the concept of the service organization, explained the new risks associated with these business relationships, and documented the first attempt to create a uniform external auditing process for service organizations.
Statement on Standard for Attestation Engagements

Number 16 and the Service Organization Control Audit Series

Description and Explanation of the New External Audits

This section outlines the creation of SSAE 16 which would become the first audit type in a new type of service organization audit, the Service Organization Control Audit series. This series would include SOC I, an audit or financial reporting controls, SOC II, and audit based on Trust Service Principles, and SOC III, a publically-available SOC II audit.

As the previous section indicated, there were many problems with implementing and relying on the Statement on Auditing Standards (SAS) 70. One important resource for addressing these issues would become the set of Statement(s) on Standard for Attestation Engagements that AICPA originally created in 1985. These statements defined standards to be used during attestation engagements. According to an article in the Journal of Accountancy:

"An attest engagements is one in which a CPA either is engaged to issue or does issue a written communication that (1) expresses a conclusion with respect to the reliability of an assertion that is the responsibility of one party and (2) is or reasonably might be expected to be used by another (third) party" (Anonymous, 1985).

Initially, these standards did not have the power to supersede Statement on Auditing Standards. However, in 2011, AT Section 801 defined the new Statement on Standards for Attestation Engagements (SSAE) No. 16 that was to supersede SAS No. 70.
SSAE No. 16 would also be known as the Service Organization Control (SOC) I audit, and would be a part of the new SOC series. While SOC I would replace the previously used SAS 70 audit process, the other two audits in the series were based on relatively new standards. The series would include SOC I type one and two, SOC II type one and two, and SOC III. It is not a legal requirement for service organizations to undergo these audits. However, organizations may be required by clients to show proof of successful SOC audits. Service organizations may also elect to implement these audits to give them a competitive edge over similar service organizations or they may do so to attract potential investors. A couple examples of companies that may need SOC I audits include companies that perform payroll processing and loan servicing. While companies that provide cloud computing, network monitoring, or medical claim processing services may benefit from a SOC II audit. Database companies and other similar companies that not only have access to sensitive information but may also have an impact on another entity’s financial reports may need to undergo both types of audits. SOC III audits are only available to companies that have undergone a SOC II audit.

It is important to understand the difference between the SOC audit and a more common external financial audit. A typical external financial audit is conducted by examining the financial transactions, journals, and reports of the organization. While a SOC audit is conducted by examining procedures and internal controls implemented during financial accounting processes. Internal controls are used in this context to ensure that proper measures are being made to avoid any material misstatements of financial information. The traditional type of external audit mainly looked at the firm's operations in a historical view. SOC audits either look at the current effectiveness of the business'
procedures and controls on the day of the audit or examined how those procedures and controls operated over a given period.

Another important variation is that SOC audits require management's written assertion and description of the entire system. Whereas SAS 70 only required a description of internal controls. SOC audits require a more thorough description and hold management to a higher level of accountability in regards to that description. Another major improvement was that SOC audits are more aligned with standards created by the International Accounting Standards Board.

An international approach to determining service organization audit requirements is increasingly important as we move toward a global economy. American companies frequently outsource functions to international companies as these companies provide services at lower costs than can be found domestically. Bringing domestic standards into alignment with international standards ensures that American businesses are competitive for both the consumer market and business to business transactions.

While, there are differences, there are also similarities between the SAS 70 and SOC 1 audit. For instance, both types of audits focus on the service organization's internal controls that have a direct effect on the services that relate to the user organization's financial reports. Both of these audits also have a type 1 and a type 2 report with type 2 being a more extensive test on the effectiveness of the highlighted internal controls.

Another important similarity between these two types of audits is the readiness assessment. The readiness assessment provides a firm with insight into its current weaknesses and gaps that need to be amended before the audit is performed. If the firm does not fix the shortcomings in its system, then there is a higher risk of failing the audit,
being required to amend the issues, and sacrificing more of its resources in order to undergo the process a second time. A firm could choose to hire a CPA to assist in the readiness assessment or conduct it themselves if they have extensive knowledge of the new requirements. The CPA would provide questionnaires that help the firm assess their control objectives, relevant controls, the number of physical locations, and what the appropriate time frame should be. If a SOC I audit is needed, a firm may discover that portions of a previously undergone SAS 70 audit may have readied the firm sufficiently for the SOC I audit, saving the firm time and money during the new audit.

An effective readiness assessment will provide a firm with a complete description of its system, internal controls, and needed improvement. It is important to note that the firm would also conduct internal audits both before and after the assessment in order to detect any weaknesses and highlight areas of exceptional efficiency. In order to prepare for the external audit, the firm would need to provide a plan for improving weak areas and show that these plans are being implemented. Areas that may need improvement include technical competency and policies and procedures in order to ensure accounting and security integrity. After these measures have been taken, the firm would contact a CPA external auditor that is preferably a member of a qualified PCAOB CPA firm.

Type I includes a description of the service organization's system, including a list of internal controls, a description of how those controls work together, and the types of risks the controls are designed to prevent. There is also an explanation of how the controls are relevant to user organizations. Along with the description, there needs to be management's written assessment as to the accuracy and fair representation of the information in the description. This feature was added to the process when SOC audits
were adopted. This aspect helps ensure management’s accountability over the company’s systems. The last step in the process is the external auditor's part in the process. The external auditor reads management's description, examines all control objectives and activities, and verifies that all aspects are fairly and accurately presented in the manager's assessment. The auditor then provides an opinion of the suitability of the firm's systems and the accuracy of the assessment. Type one audits are merely used to verify that, at the time of the audit, the controls that were claimed to be in place are present and that they are suitable for achieving the specified controls. The auditor does not test the controls to ensure that each is operating to efficiently. Therefore, many user companies require service organizations to undergo type two audits in order to prove the operating efficiency of their internal controls.

Type two audits provide an attestation to the efficiency and consistency of each control. The auditor tests 1 item of each control and determine if, based on the effectiveness of the chosen item, the control was achieving its intended objectives accurately and efficiently. Tests are conducted over a period. The most common periods are six months and one year. At the end of the time period, the external auditor provides an opinion concerning how efficiently your controls were working over that period. While absolute assurance would be ideal, it is only required to provide reasonable reassurance. The controls need to be assessed as operating as intended and that the service company’s system is capable of minimizing errors that could lead to financial misrepresentations, privacy breaches, or misplacement or misuse of sensitive information.
The amount of preparation, time, and financial resources need to complete type I and II audits can be quite taxing on an organization. Type two audits are more expensive because they are more detailed, cover a wider scope, and are conducted over a longer period of time. These audits are not cost effective for all firms. However, there are many benefits to obtain through this investment. For example, service companies that wish to provide services to public companies. Failure to do so can result in a substantial loss of revenue. Furthermore, providing proof of successfully implemented SOC audits create a competitive advantage when competing with other service organizations to provide services for all businesses, private or public. Lastly, these audits can be implemented to show an organization’s compliance with laws and regulations. In the event that a service organization is confronted with legal accusations from clients or customers of clients, proof of the completed SOC audit can provide the service organization with protection.

This section explained a new type of service organization audit series. It provided an explanation of each audit in the series, its intended purpose, and implications for service organizations.

**Interview-External Auditor**

This section provides a first-hand account of external audits over time. Kirk Balcom, external auditor, explains the evolution of the external audit over time ending with implementation of the SOC audit series. It is vital that companies understand the
complex process involved in completing a SOC audit. One must know which SOC audit is needed, how to prepare for that audit, and how heavy of financial burden it can be.

In a recent interview with Kirk S. Balcom, CIA, CISA, CFE, Principal of Rehman Consulting, I was able to gain valuable real world insight into the SOC audit process as experienced by an external audit. Mr. Balcom has extensive experience with SAS 70, SAES 16, and the SOC series audits. He shared valuable knowledge pertaining to the transition from SAS 70 to the SOC audits. Mr. Balcom has conducted SOC I type one and two audits, SOC II type one and two audits, and SOC III audits. Through this interview, I was able to understand the importance of implementing these audits in an economy that is relying more and more on information technology and outsourcing services. He explained the importance of company’s implementing the SOC audit that is relevant to the services they perform. I was also able to understand the benefits that both the service organization and user entities gain from the implementation of the SOC series audits.

Mr. Balcom began by explaining the need for a user company to verify the internal controls of its service organizations. Assurance of the service organization’s proper internal controls are essential to the user entity, especially when the services provided have a direct effect on the user organization’s financial reports. For a payroll service company, such as ADP, in essence provides its clients with a journal entry that is directly applied to that client’s financial statements. ADP’s services determine the payroll expense that is reported on its clients’ income statements. This expense, then, affects that business’ reported net income. A misstatement of that expense, creates a misrepresentation of that business’s financial position. Any material misstatement on
financial statements is a violation of the reliability qualitative characteristic of financial reporting.

The enactment of the SAS 70 improved the service organization’s external auditing experience. Before the SAS 70, each of the service company’s clients would send in their auditors. Those auditors would perform an audit of the service company’s internal controls. Throughout this auditing process, the service organization was faced with the responsibility of accommodating each of their clients’ auditors with conference rooms. The audit could last anywhere from two days to a week. During this time, the service company was required to provide requested documentation illustrating relevant internal controls and staff members to assist the external auditors in their investigation. This obligation reduced productivity levels and consumed substantial resources of time and money for service organizations, especially companies that serviced hundreds of clients. It not only required vast amounts of the service organization’s resources, it was also a major investment for the user company as well. Therefore, when SAS 70 was enacted, some user organizations began requiring service organizations to provide proof of a successful SAS 70 audit.

Unfortunately, Mr. Balcom witnessed over-reliance on the SAS 70 audit. His clients often reported that one of its user organizations was requiring them to undergo an SAS 70 audit. The problem was that his client’s services were not in the least related to the user’s financial reports. His client provided summaries of quality measures for a health care provider. The health care provider was requiring his client to undergo a SAS 70 audit in order to gain reassurance that the sensitive information that his client was responsible for was kept confidential. Mr. Balcom refused to do the SAS 70 audit for his
client because he felt it was misuse of the audit. He knew that the health care provider needed reassurance of the accuracy and reliability of the service provider’s internal controls, but there were no audits that could test these types of controls at this time. His client eventually went to another external auditor that was willing to perform the unneeded SAS 70. This situation took place more times than one would think before the SAES 16 was implemented, and he complained about the unreliability of this system for years. Finally, the AICPA noticed the problem, and created the SOC series.

Mr. Balcom overcame certain obstacles he faced and gained valuable benefits from the introduction of the SOC audits. The first thing he did was contact all of his clients to inform them that the SAS 70 had been replaced. His clients had all grown accustomed to using the SAS 70, as it was the guidance for service organization audits for nearly 19 years. As with any new system, there was opposition. Both user and service organizations opposed the changes at first. To complicate matters further, he had the responsibility of informing select clients that they would need the new more extensive SOC II audit. As external auditor, he was faced with the responsibility to educate all of his clients on the new audits, the differences between them, and the importance of complying. The main benefit he received from this new audit process was the addition of many clients that needed to implement the SOC II audit. Service organizations would contact him when they had been required by one or more of their clients to provide proof of a successful SOC II audit. Another benefit that Mr. Balcom received from the new audit process was that there was no longer confusion among user and service organizations as to the requirements of the audit process. User entities knew which SOC
audit pertained to the services they were provided with, and they were able to gain the assurance they needed from their service organizations.

User organizations, frequently require a type two audit. Type one audits are often used to assess whether the service company is ready for type two audit. Given the limited ability of the type one audit to provide reassurance, four out of five user organizations require their service organizations to undergo type two audits. The process normally begins with Mr. Balcom completing a type one audit for his client, then completing a type two audit a year later. While one year is the average time frame for type two audits, the period may be compressed in certain situations. Guidelines require type two SOC I audits to cover a minimum of six months and type two SOC II audits to cover a minimum of two months. An instance in which a SOC II type two audit would cover a two month period would be if a user organization is requiring immediate proof of the service organization’s successful SOC audit. In these circumstances, a follow up type two audit would be planned for a year after the first completion date.

Mr. Balcom provided me with and walked me through a mock SOC I and SOC II audit. These audits provided further understanding over common objectives, controls, and assertions. While the primary purpose of the SOC I and II audits are distinctively different, there are quite a few similarities in their processes. This process is a combined effort of the service organization, the user organization, the service and user companies’ internal auditors, and the independent, SOC certified, CPA, or SOC auditor. While it is an interaction between these parties, the service organization holds the majority of the responsibility in the process. The readiness stage for the initial SOC audit is the most intricate, complex portion of the entire process. Front-end resource and time
consumption can be quite taxing for the service organization. The process must be cost efficient; the revenue that is received due to the completion of this audit, must outweigh the costs incurred.

The user organization determines the objectives. The SOC auditor tests reports on the suitability and, or the accuracy and reliability of the controls. The SOC auditor also may, upon the request of the service organization, educate the service organization, conduct a readiness assessment, and assist in determining needed controls. These additional services are available for an additional fee. Given the costly nature of these services, organizations may not have the means to acquire them. In this case, they all must be conducted internally. The service company is responsible for conducting a risk assessment in order to determine any threats that could deter their fulfillment of the user organization’s objectives. Once those threats are identified, management must create controls to minimize those threats. Management is also responsible for providing a description of the internal framework and an assertion of the accuracy of the report. The service internal auditor is required to provide a report verifying the date the controls were established, the frequency of which tests are conducted, and the accuracy of the description. The user organization’s auditor is responsible for meeting with the SOC auditor, understanding the report, and communicating the results to the user organization’s management.

The process begins with the SOC auditor completing a type one audit, which may or may not be included in the cost of the type two audit. If, during the type one audit, the SOC auditor determines that the controls are not suitable for the intended objectives, they must report to the user organization that the audit failed. In this circumstance, the service
organization incurs the cost of the failed audit and the possible loss of revenue from certain user organizations. Therefore, despite the additional cost of the ready assessment, it may, in fact, be cost beneficial for the service organization to incur that cost before the actual audit. A SOC auditor has the obligation to report any and all failed SOC audits. If during the audit, it is determined that one or more of the controls are not working as reported, the audit must continue as planned. The only other option for the service organization is to terminate the current audit and hire a new SOC auditor. However, the new auditor will be obligated to contact the previous auditor, gain an understanding of the failed audit attempt, and report the information in the new audit. There is not a way to hide a failed SOC audit. The service organization must be thoroughly prepared and, through frequent tests, ensure that all controls are accurate and reliable.

One vital component of any SOC audit is to ensure proper security over the physical environment in which sensitive information is stored. Whether this information is financial in nature or confidential in another manner, it must be secure while in the hands of the Service Organization. Not only is it necessary for the physical location to have security features, such as security cameras, access codes, and proper security staff, there must also be verification of the integrity of the software, network, and employees given access to this information.

A primary concern of the user organization may be to ensure that physical access to computer equipment and storage media in which their financial information is stored is restricted to authorized personnel. One important control over this objective is the locking of all idle workstations left unattended. The service company then establishes tests over this control such as inspected network timeout setting. For this test, appropriate
staff members record and analyze the average of time for each computer left idle to lock. If the average does not consistently fall within the acceptable parameters, then the service organization must determine the source of the problem and correct it.

For a SOC I and SOC II audit, the service company must provide a company overview including the types of services provided, the current management, and the service market. Next, management must provide a description of the control environment and relevant internal controls. They must report their relevant clients' objectives and the relevant control activities. An example of a SOC I audit may include general computer controls that ensure financial data is preserved and protected. A description of this control may include secured access to the computer system including procedures to remove terminated employees. It may include controls over physical access to the server room include passage codes as well as controls to ensure a stable physical environment. Data recovery controls are essential in order to ensure that vital information is maintained in the event of a disruption to the information system.

For a SOC II audit, the first step that must be taken is the system description. The system description includes a definition of the service organization's procedures, personnel (including their functional areas and lines of authority), data (including the type of data they collect and how they use it), software, and infrastructure (including their data centers and their networking devices. There must be an explanation of the method for communicating control procedures to all employees and ensuring compliance among all staff members. The service organization also explains the services they provide, quality measures, and cost reduction processes. There is a description of the governance
board that is responsible for overseeing all operations and who are held accountable for the overall integrity of the service organization’s processes.

A final type of SOC audit is a SOC III audit. This type of audit is an abbreviated SOC II audit. While use and dependence on SOC I and II audits is restricted to the service organization, the external auditor, and the user entity, SOC III is available to the public. Any sensitive information that is included in the SOC II audit is removed to create the SOC III audit. A SOC III seal is placed on the company website and the report can be accessed by clicking on the seal. These seals are especially beneficially to service organizations that service publicly traded corporations.

Many user organizations wish to be certain that the servicer has taken measures to eliminate access of system resources from inappropriate internal or external sources. Only internal users whose position requires access to these information sources will be granted access. There should be an IT manager that is responsible for verifying any user’s access. Each approved user may need to provide the IT manager with proof of top management’s authorization. In order to test these objectives, tests would be conducted to discover if unauthorized personnel were able to enter the system. Controls over criteria for password content and length and the process of locking an account upon too many failed attempts to enter the system.

Controls not only need to be established to ensure the security over information, there also need to be controls in order to protect data safeguarding and accuracy. In order to confirm that all important data is retained, it needs to be maintained on backup software that is monitored and stored at a safe, off-site location. There needs to one specific person responsible for this task and the backup process needs to be tested.
periodically. Tests are conducted by examination of the backup schedule, backup documents, and backup log.

It is not uncommon for a service organization to contact Mr. Balcom before readiness steps have been taken. There have been some occasions in which the service organization has not completed their preparation and needed to be educated on the entire process. Since the majority of the work involved on a SOC audit is the responsibility of the service organization’s management team, there are several different management requirements depending on the type of audit. Mr. Balcom has experienced numerous instances in which the service organization did not initially have proper controls in place. He was faced with responsibility of educating his client, conducting a readiness assessment, and help them establish appropriate controls. It is his hope that as these audits grow in popularity, more clients will be educated thoroughly enough to be proactive in this process. There are major repercussions to beginning a SOC audit before one is ready.

One major change that occurred through this new process and has affected both SOC I and SOC II is a much heavier reliance upon information technology. Sixty percent of SOC I relevant internal controls and about 98% of SOC II relevant internal controls are related to information technology. The main difference between a SOC I and SOC II audit is management’s discretion over the included controls. While management chooses which controls to include for SOC I, a SOC II audit is more of a checklist approach to the audit process. The user entity chooses controls over which of the five trust principles: availability, security, privacy, processing integrity, and confidentiality, they wish to be included in the audit.
In the instance that organizations need both types of audits but are financially restricted, they should opt for a SOC II audit. User organizations report relying much heavier on SOC II audits. Despite the variation between companies and the type of audit that is necessary, many companies insist on completing a SOC I audit when they need a SOC II audit. Mr. Balcom can only assume that this is due to lower financial burden of the SOC I audit. He will not conduct an incorrect audit despite the added revenue. Unfortunately, there are SOC auditors that will conduct these unethical, faulty audits. There still need to be improvements made to the system, but it has progressed substantially in last 22 years.

These audits are presently not legally required, and while Mr. Balcom has many clients that benefit from this process, he does not believe these audits are beneficial for all firms. They should only be conducted if they are cost efficient for the service organization. Mr. Balcom has one client that provides services for approximately 500 user companies. Of these 500 clients, only three require proof of a successful SOC audit. This company would most likely be better off allowing those service organization’s auditors to come into their business and perform their own audits. They do not seem to be receiving enough revenue from these few businesses to cover the cost of the SOC audit process. Despite that, this client continues to undergo these audits every year.

The prices for the different SOC audits vary. The ready assessment, which may be needed for both the SOC I and I audits can range from $3,000 to $5,000 depending on the degree to which Mr. Balcom needs to be involved in the process. A SOC I audit can range from $5,000 to $10,000. A SOC II audit is normally much costlier as it entails many more steps and requires the checking of controls over various different principles.
A SOC II audit can range from $5,000 (if it only needs to cover one principle) up to $20,000. A SOC III audit, the least common of the three types is $3,000 because the bulk of the work for this audit was completed in the SOC II process. While these audits may seem rather costly, the revenue earned by service organizations as a result of these audits can also be substantial. These audits are not intended for every business, but as the business environment becomes more complex, the requirement to provide proof of successful completion will increase.

This interview provided clarity that was only attainable from the perspective of the external auditor. As previously explained, many service organizations are not adequately educated on the audit series prior to requesting Mr. Balcom's services, and may not have necessary controls in place. It is vital to spread awareness of not only the SOC audit process, but also the consequences one may face due to a lack of proficient internal controls.

**Interview—Compliance Officer**

This section outlines the SOC II audit process as experienced by a compliance officer at Highland Solutions. Highland Solutions was required by a major client to provide proof of the SOC II audit. Along with retaining a major client, Pfeiffer and her colleagues also gained self-awareness.

In an interview I conducted with Tracy Pfeiffer, the compliance officer with Highland Solutions, I gained insight into the SOC II audit process from the perspective of
the service organization. Ms. Pfeiffer had a legal background before becoming the compliance officer for Highland Solutions. Ms. Pfeiffer explained that her company has successfully completed a SOC II type one audit and is in the process of undergoing a SOC 2, type two audit. Along with a team of managers from various departments including Human Resources, IT, and Operations, she has worked with the external auditors in ensuring that all internal controls are in place and reliably and accurately operating. Highland Solutions is a service organization that provides outsourced services including cloud computing, social business platforms, and customer relationship management. The company began the SOC II audit process upon the request of a client.

The process has not been easy, but the company and its management has received many benefits other than compliance with a major client. Previous to this process, they were lacking many vital internal controls that needed to be in place. In the end, it was more of a self-discovery tool than a requirement. Management of each department has gained valuable experience through the process. The nature of the control being examined at a certain time determines which manager will head the team during each process. Therefore, each manager has the opportunity to lead the audit process while controls that affect his or her area of expertise are being examined.

One example of a department that has benefitted from this process is the Human Resource department. They have implemented stronger controls over background checks and hiring activities. It is very important to their company’s success to hire the best people for their company. Their clients also need to know that the employees they are hiring that will have access to their information have been checked and cleared before they begin working with their clients.
Highland Solutions is working towards establishing and using a common criteria for controls that affect multiple trust principles. One thing they have noticed is that they have a lot of redundancy in controls for each trust principle. This results in very high overhead costs for the company. The common criteria allows the company to rewrite certain controls that may apply to multiple objectives. While rewriting multiple controls presents higher front-end costs, the goal is to lower internal costs in later years. Not all controls are able to be applied to all principles, there are still some controls that only apply to one principle.

This section introduced the concept of common criteria for trust service principles as they are relied upon for SOC II audits. The new common criteria will not only simplify the SOC II process, it will also result in reduced financial burdens on the service organization.

**Interview- Chief Financial Officer**

This section provides a brief depiction of the SOC I audit as experienced by the Chief Financial Officer of yB Management. yB Management offers consultation services to health care organizations. Given the range of services provided, SOC I and II audits are relevant to this firm.

Mark Laser, CPA, is the Chief Financial Officer of yB Management. His business offers consulting services to businesses in the healthcare industry. Provided services range from assistance maintaining compliance with laws and regulations of the industry,
decision support, product development and placement, financial management, and human resource management. Given the vast range of services, the company has decided to implement SOC I, II, and III. Mr. Laser, CPA explained that yB was not required by a client to undergo the SOC audits. They chose to implement the audits when they began efforts to expand the company and the number of clients served.

The company first began with a readiness assessment, which did not render the desired results. The readiness assessment revealed that yB Management lacked many proper controls, the controls that were in place were not being adequately monitored, and the company failed to provide any sort of organization-wide available resource detailing the internal controls and ways in which employees were to uphold them. Although the amount of work that was needed to only prepare for the SOC I audit, but also to complete may have been taxing on the company and its resources, Mr. Laser believes that it will be a wise investment. The healthcare industry is especially concerned with proper financial management, instant accessibility to valid patient information, and protection of patient confidential information. In order to attract the business of healthcare firms, yB needs to confirm that internal controls over both financial and non-financial information are adequate and properly managed.

The process began in January of 2014 with the readiness assessment. In April 2014, SOC I type one was successfully completed. At that point, the company began to prepare for the SOC I type two audit. Upon successful completion of the audit, they will begin the process of preparing for a SOC II type one audit. The company is aware that completion of SOC II audits will be a more complex, lengthy process. Mr. Laser believes it will be ideal to go right from SOC I into SOC II because while the internal controls
needed for a SOC II audit are different, the company will be used to the process and will be more efficient in completing the second audit. It has been a learning process for the entire company, and it will not only make the company more marketable, but it also enhances the understanding and participation of employees in the internal control processes.

Mr. Laser explains that his company will complete the process with a SOC III audit. He is aware that many companies have not opted to go the extra mile in order to complete the SOC III audit. Although, choosing not to implement the SOC III audit may initially reserve financial resources, it will limit the use of the successful SOC audit and the marketability that can be gained through the process. Having a SOC audit seal on the yB Management website will be a source of pride and a tool to provide assurance to all healthcare professionals that may then become clients.

This section is a brief description of the ways in which the SOC audit process can strengthen a company, provide insight into areas that need improvement, and allow a company to gain a competitive advantage from the process. A service organization that operates in the healthcare industry is subject to heightened restrictions and regulations.

**Conclusion**

Businesses in today's professional world are continuously confronted with various different risks. Organizations need to assure various different stakeholders that proper precautions are being taken in order to minimize the threat of these risks and maintaining integrity in all aspects of business. Only through an objective, unbiased individual can outsiders truly have reassurance that businesses are operating ethically and
efficiently. Not only is it necessary for businesses to maintain their own continuous risk management activities, they also need to verify that any of their service providers are also actively managing risks that will inevitably affect their own risk management efforts. It is not conceivable that each organization be responsible to oversee the efforts used by each service provider, as this would come at an unrealistic cost to the service organization. Upon recognition of this dilemma, the American Institute of Certified Public Accountants have created a uniform format for service organizations to provide verification of successful external audits.

First, the SAS 70 was implemented, but then found to be inadequate for fulfilling its purpose, and the SOC audit series was created. Not only was a more efficient audit over financial reporting needed, there was also the need to verify service organizations’ controls over the trust principles: availability, security, privacy, processing integrity, and confidentiality. As organizations rely heavier on information technology, governance over these principles becomes increasingly difficult. Proof of each service provider’s controls over these principles provides much needed assurance to the user organization. As the business environment continues to evolve, the SOC audits will need to be revised or replaced with a type of audit that is more relevant to the businesses of the time.
Works Cited


