Exploring Perceptions of Corporate Managers Regarding the Use of Continuous Control Monitoring

Dissertation Manuscript

Submitted to Northcentral University

School of Business and Technology Management

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

CYNTHIA ANN DAVIDSON

San Diego, California

August 2018

Approval Page

Exploring Perceptions of Corporate Managers Regarding the Use of Continuous Control Monitoring

By

Cynthia Ann Davidson

Approved by:

Abigail G. Scheg 9/24/18

School Representative: Abigail G. Scheg, Ph.D. Date

Certified by:

Kelley Walters 9/24/2018

Dean of School: Kelley Walters, Ph.D. Date

Abstract

Organizations were required to make well-informed and timely decisions in regards to financial and regulatory requirements to maintain proper enterprise risk management and prevent fraud. Performing traditional control monitoring for enterprise risk management efforts, compliance, and fraud prevention efforts can be time-consuming yet crucial for making business decisions; therefore, business executives must evaluate and establish a control monitoring methodology. Inaccurate financial information could result in false business reports, fraud, loss in shareholder value, and lead to corroding trust in capital markets. The escalation of fraud and financial inaccuracies is of major concern to business leaders. Business processes, controls, and best practices for continuous control monitoring may not be consistent, resulting in diminished quality of enterprise risk management for corporate financial reporting. This qualitative, multiple-case study was designed to explore the practice of continuous control monitoring in support of enterprise risk management and fraud prevention. The purpose of the study was to explore the perceptions and experiences regarding the use of technical tools and processes for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts.

Table of Contents

Chapter 1: Introduction

For a corporation to maintain a competitive advantage, managers needed to make decisions based upon timely and accurate financial information (AICPA, 2012). Continuous control monitoring was a technology monitoring process through which to improve the detection, compliance, and risk issues associated with financial and operational activities within an organization, and thus had an important role within business as a means to achieve increased enterprise risk management, also providing potential for increasing productivity and competitive advantages within the control monitoring functions (AICPA 2012; Ajah & Inyiama, 2011; Singh, Best, Bojilov, & Blunt, 2014). Due to the daily changes in business operations and regulatory requirements, traditional controls monitoring paradigm was outdated and unsuitable to provide real-time assurance for making proper corporate business decisions (AICPA, 2012; Lombardi, Vasarhelyi, & Verver, 2014; Ramamoorti & Dupree, 2010). Additionally, organizations were subject to increasing penalties and fines for non-compliance with financial reporting standards.

Fraud remained a largely unmitigated risk due to perpetrators attempts to conceal the fraud tracks, resulting in a lack of audit trail. Ramamoorti and Dupree (2010) indicated that manual detection of fraud perpetrated within information-intensive transactions or financial processing operations as being increasingly impractical due to the sheer volume and complexity of the data. Further, manual detection occurred too late to prevent both the expenses and devastating consequences to company reputation (Ramamoorti & Dupree, 2010). Thus, automated controls provided indispensable value in detecting fraud within system operations and proactive fraud risk management including mitigation efforts must involve automated anti-fraud programs and controls (Steinhoff, Price, Comello, & Cocozza, 2016). Specifically, continuous monitoring service opportunities include converting from manual to automated controls,

designing controls around processes, formulating tests and monitoring routines, and dispensing operational risk management services including data extraction tools, data analytics, that were used to automate business operations, and add value (AICPA, 2012; Singh et al., 2014).

Fraud was more effectively detected in data analytics, as speed was critical when dealing with instances of fraud to mitigate both risk and loss (Singh et al., 2014). Within publicly traded corporations, the ongoing rapid cadence of the technological change required a timely understanding of both the risks and opportunities associated with IT phenomena (Singh, et al., 2014). As continuous control monitoring had the potential for radically changing the manner in which corporations operate, there was real promise in contributions to organizational effectiveness, efficiencies in enterprise risk management, and long-term profitability.

A case study approach that explored continuous control monitoring provided valuable knowledge that minimized existing literature gaps, identifying situations and trends of corporate managers (Yin, 2014). Executives within organizations had a need to gain understanding relative to how this technology transforms control monitoring, and risk management, including whether the transformation leads ultimately to productivity gains, or produced a chaotic state among impacted stakeholders.

Statement of the Problem

The problem was there were impediments to adoption, implementation, and use of continuous control monitoring procedures for fraud prevention controls to manage organizational risk in maintaining corporate requirements (Hardy & Laslett, 2015; Salvioni, & Astori, 2014; Singh et al., 2014). Corporate managers encountered problems with continuous controls implementation that affect their collective ability to deal with enterprise risk management and fraud prevention (Hardy & Laslett, 2015; Salvioni, & Astori, 2014; Singh, et

al., 2014). As regulations become more stringent, there existed a demand for increasing the efficiency of control monitoring, and compliance efforts including fraud detection (ACFE, 2017). Continuous control monitoring had an important role in corporate management as a method through which to achieve increased operational efficiencies and provided an opportunity for increases in productivity and competitive advantages within compliance and fraud prevention functions (Lombardi et al., 2014).

Despite advancements in information technology and fraud detection, fraud still ran rampant, as the 2014 fraud report indicates that a typical company continued to lose approximately five percent of revenue to fraud each year (Verschoor, 2014). While there were studies on individual topics relating to information technology and fraud, limited research existed considering fraud prevention needs and challenges of corporate managers relative to current technology advancements. Available studies regarding continuous control monitoring method existed yet had not fully examined perspectives of corporate managers regarding efficiency improvements, including a lack of information related to financial fraud detection and prevention efforts, and regulatory compliance (Deloitte, 2010; KPMG, 2008). Corporate managers within organizations had a need to understand how the technology provided methods for transformation in work environments, and if such transformation leads to an ultimate overall gain, or instead produced more chaotic states of operation between managers and the key stakeholders.

Purpose of the Study

The purpose of this qualitative multi-case study was to identify and explore the perceptions and experiences of corporate managers' regarding the impediments to adoption for the implementation and use of continuous control monitoring procedures for maintaining

corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts. Up to 20 corporate managers were interviewed from Fortune 500 companies located within the Eastern United States.

This study provided a new approach for understanding the perceptions and challenges relative to continuous control monitoring implementation efforts for corporate managers. The unit of analysis to represent each case was the organization, consisting of a purposive sample of leading Fortune 500 institutions, having regulatory and legal mandates (Creswell, 2014; Yin, 2014). The sampling for the research included up to 20 participants, consisting of individual managers chosen from up to 6 organizations who have experience with various corporate leadership roles and responsibilities that could include chief executive officers (CEO), chief financial officers (CFO), or accounting and finance directors who were experts in financial and control monitoring processes, and had experience in financial risk or fraud risk management. This study was conducted utilizing purposeful sampling, with a focus on organizations within the Eastern United States that were confronted with legal and regulatory mandates (Creswell, 2014; Yin, 2014). To triangulate the interview data 1 manager from the financial fraud prevention or equivalent office in each of these organizations were interviewed as well.

Theoretical Framework

When adopting new technology, including advanced information fraud prevention tools, a key theoretical model associated with adoption was the diffusion of innovations theory. The diffusion of innovations theory (Huffman & Crump, 2005) was the framework through which the communication of the innovations in fraud prevention techniques travels through the channels, over time, among corporate managers. The four main elements key to the diffusion of

innovations theory, as noted by Huffman and Crump (2005), included innovation, communication channels, time, and social systems.

The basis for rates of adoption of these innovations related to the characteristics of relative advantage, compatibility, complexity, trialability, and the observability for other corporate managers within the given social system (Huffman & Crump, 2005). Applying the diffusion of innovations theory indicated the value in sharing of knowledge from early adopters with late adopters, to communicate the innovation advantages, and impact adoption rates by corporate managers, and improve overall enterprise risk management, resulting in reductions in fraud (Davis, 1989). Sharing of information in this manner improved potential usage of modern information technology tools, which in turn allowed corporate managers to more effectively prevent fraud relative to financial statements. The degree of relative advantages of the fraud prevention technology compared to the existing manual tools currently utilized by corporate managers was a key element to the diffusion of the innovations throughout the given social group of corporate managers (Huffman & Crump, 2005).

Corporate management views relative to the degree of innovations value reported by corporate managers compatible with existing values and norms were important to the adoption of the innovations. These views may have contributed as reasons for the innovations being slow to be implemented widely in practice (Hong, Thong, Wong, & Tam, 2002). Another noted issue related to the complexity of these innovations and the potential perceived thought that new prevention tools were difficult to understand and use, and thus adoption has potentially been slower as a result (Huffman & Crump, 2005). While there has been some value gained in increasing the observability of the positive results, an issue that remained was the need for improving the communication between peers in the social system regarding the new ideas and

potential future innovations available in fraud prevention in this area (Huffman & Crump, 2005; Lombardi et al., 2014; Masli, Peters, Richardson, & Sanchez, 2010).

Research data using this theory built upon and provided greater visibility in the areas of financial fraud prevention and meet regulatory requirements. Prior research had focused on the quantitative technical side of continuous control monitoring, rather than exploring the perceptions and experiences of financial managers regarding the use of technical tools for continuous controls monitoring. As businesses grew globally, technology was rapidly changing, and business requirements have become stricter with financial reporting, thus additional future research provided further information to business executives that enhanced corporate business strategy.

There existed given rates of adoption of these innovations based upon the characteristics of relative advantage, compatibility, complexity, trialability, and the observability to others within the given social system of corporate managers. The diffusion of innovations theory included the sharing of knowledge from early adopters with late adopters, in order to communicate the innovation advantages and increase adoption by more corporate managers. Technology Acceptance Model (TAM) was one specific model that provided a framework for explaining information technology acceptance behaviors, including acceptance of the new fraud prevention techniques. Technology Acceptance Model provided information including the impact of external variables on individual corporate managers' intention toward accepting IT changes. These types of individual differences had significant impacts on IT acceptance decisions (Hong et al., 2002). The theoretical ground for the model was Fishbein and Ajzen's Theory of Reasoned Action (TRA) (Hu, Chau, Sheng, & Tam, 1999). The basis of this theory was upon beliefs influencing individual attitudes, which in turn shaped the behavioral intention guiding, which resulted in the

individuals' behavior. This theory allowed for an identification of the individual influences of corporate managers, and their perceptions of ease of use, and complexity involved with the innovations in fraud techniques.

There have been few qualitative studies that explored the information technology adaptation process, and automation in accounting to identify factors in implementation that determined the actual success of business and operation augmentation (Bergeron & Raymond, 1997; Lombardi et al., 2014). Indicated by Bergeron and Raymond (1997) was that organizational support, implementation process, and control procedures impacted the initial realization of benefits from any information technology adoption, however; that historical study focused on any new technology, rather than specifically towards the implementation of continuous control monitoring resources. Further, while other existing studies have examined factors that may affect business values, the study results did not estimate improvements in compliance (Ajah & Inyiama, 2015; Hardy, & Laslett, 2015; Lombardi, et al., 2014).

Gaps existed in research relating to continuous control monitoring and information technology governance that have potential to contribute to chaotic states for organizations (Hardy, & Laslett, 2015; Lombardi et al., 2014). The various continuous control monitoring methods associated with the control monitoring methodology may have been a confusing factor for corporate managers when considering adoption (Singh et al., 2014). The results of this research shifted the focus of continuous control monitoring from financial controls and regulations to improved efficiency in fraud prevention and enterprise risk management for financial reporting.

Nature of the Study

This qualitative, multiple-case study design consisted of exploring the perceptions and experiences of corporate managers regarding the use of technical tools for continuous control monitoring through interviews. Lee (2006) observed that conducting case studies and applying various data-generating techniques, complex and ambiguous issues could be penetrated. The power of the case study was its attention to an illumination of the local situation (Creswell, 2014). In this research, there were individual case studies conducted to explore the perceptions and experiences of executives who were confronted with complex financial reporting and regulatory compliance issues. With the understanding that one of the most important sources of case study information was the interview, this research approach consisted of interviews to gain knowledge regarding the perceptions of continuous control monitoring techniques for financial reporting (Trochim & Donnelly, 2008; Yin, 2014).

The purpose of the interviews was probing the ideas of the interviewees about auditing processes, financial reporting, and regulatory standards (Yin, 2014). Further, there was an exploration of control monitoring processes and methodologies by interviewing corporate accounting professionals that have hands-on experience within their organizations. The data generated from the study provided a deeper understanding of the auditing and governance situation in organizations in an effort to share the findings of this study and develop a better understanding or strategy for continuous control monitoring to use in their organizations.

For this study, used during data collection was a semi-structured interview guide. After obtaining IRB approval and prior to use, testing of the guide was completed by the researcher's manager and three colleagues as a pilot study to ensure that the questions address the purpose and goal of

this research. Further, data gathered from the pilot study allowed for adjustment of the interview guide to ensure the research purpose and goal was met. The interview data from the pilot study served as validation of the research instrument and excluded from the final set of study results. The script contained questions to gather information needed to answer the main research questions. The interview questions included: (a) demographic inquiries such as job title, employee count, business, or governmental functions, (b) psychographic inquiries such as purchase motives and usages, (c) particular regulatory or legal compliance requirements, and (d) barriers (ACIPA, 2012). These questions were designed to stimulate open dialogue with the managers concerning the methodology of continuous control monitoring. The open-ended questions were sub-questions which provided elucidation of the main research questions (see Appendix A).

The data collected in the field and accounting experience of the researcher assisted in closing the gap of the human elements that were missing from the prior research. The research data built upon and provided greater visibility to prior work in the areas of financial compliance, reporting, and meeting regulatory requirements. Prior research had focused on the technical side of continuous control monitoring where this research focused on the perceptions and experiences of financial executives regarding the use of technical tools for continuous control monitoring. Further, the research had a focus of closing the gaps and provided benefits to the financial accounting industry and financial decision makers of corporations and businesses.

Research Questions

A strength that supports the use of the qualitative research method, with the case study method of design was that the stated questions related to the phenomenon, aligned with the purpose statement, of open-ended type, which reflected the nature of the research (Yin, 2014).

For the given research, a qualitative, multiple-case study which explored the perceptions and experiences of corporate managers regarding the use of technical tools and processes for continuous control monitoring, some identified research questions for the study were:

> **Research question 1.** What were the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts?
>
> **Research question 2.** What were the perceptions of managers regarding theintroduction of new technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods?

Significance of the Study

This research provided a new approach for understanding the perceptions and challenges relative to continuous control monitoring implementation efforts for corporate managers regarding their knowledge and willingness to adopt fraud prevention software tools. The research data built upon and provides greater visibility in the areas of financial fraud prevention, and the meeting of regulatory requirements. Prior research had focused on the quantitative technical side of continuous control monitoring, where the current research focused on the perceptions and experiences of financial managers regarding the use of technical tools for continuous controls monitoring. As businesses grew globally, technology has rapidly changed, and business requirements become stricter with financial reporting, thus additional future research provided further information to business executives enhancing corporate business strategy. Furthermore, the introduction of new legal and regulatory mandates has increased the need for dependable controls, as these regulations can invoke sanctions upon those corporate

managers failing to comply (ACFE, 2017). Understanding the business impact of continuous control monitoring on financial reporting and regulatory compliance was important to the success and future growth of the industry.

Executives had a need to communicate information about organizational performance to the outside world through financial reports, which provided summarized information about the organization's financials for external decision makers. The Sarbanes-Oxley Act added the dimension of internal financial reporting assurance expected of internal auditors and audit committees (ACFE, 2017). Chief Executive Officers, Chief Financial Officers, and auditors must report on, and attest to, the effectiveness of internal controls over financial reporting (ACFE, 2017). Therefore, there was importance in understanding the capabilities of new technologies or methodologies that could assist an organization to be regulatory compliant and efficiently report financial data, and the benefits and challenges of implementing these technologies.

As organizations and technology evolved, there existed challenges for decision makers, as well as opportunities for enhancing business practices and financial reporting, and meeting stakeholder expectations. Each organization constantly evolved as it innovated to meet the changing auditing and financial needs, including changing processes, people, skills, and technologies (ACFE, 2017). Thus, it was important for senior management to evaluate long-term strategies in order to consider definitive steps to translate that vision into a program of activities (ACFE, 2017). These visions comprised future focused goals for growth in business processes and competitive position, including considerations for evolving technological innovations. Corporate managers evaluated the level of preparedness regarding meeting increased regulatory and governance requirements when implementing new compliance and

reporting processes. Thus, it was important to gain understanding regarding the perceptions of corporate managers relative to implementation of continuous control monitoring tools and to understand the benefits of challenges in implementing these resources to provide increased effectiveness in compliance, enterprise risk management, and fraud prevention.

Definitions of Key Terms

Some key terms to include related to the given research were continuous assurance, continuous control monitoring, and information technology governance.

Continuous assurance. The continuous assurance was the combination of activities performed by internal audit to evaluate internal controls and risk management and to assess management's controls on monitoring activities (AICPA, 2012). The continuous aspect of continuous assurance refers to the uninterrupted control and risk assessments and evaluates the adequacy of management's continuous monitoring activities.

Continuous control monitoring. Continuous control monitoring was the method that allows corporate managers, and other business leaders to observe the performance of one or many processes, systems, or types of data (AICPA, 2012). This process and technology assists in the detection of compliance and risk issues associated with financial and operational activities within an organization (AICPA, 2012). Continuous monitoring included an aspect of a continuous, consistent, and timely identification of problems or weaknesses, followed by quick corrective action responses that reduce the cost of any periodic required regulatory, financial, or operational reviews to a more reasonable level (AICPA, 2012).

Information technology governance. Information technology governance provided the framework for the leadership, organizational structure and business processes, including standards and compliance with these standards. This governance ensured that the information

technology of an organization supports and enables the achievement of strategies and objectives (AICPA, 2012). The primary goal of information technology governance was assurance of business value and mitigation of the associated risks.

Summary

Although continuous control monitoring methodology had been part of the information technology industry for several years, there were corporate managers who have not adopted this methodology in their organization to assist in compliance efforts, and enterprise risk management (AICPA, 2012; KPMG, 2008). Gaps remained in research relating to continuous control monitoring and information technology governance that have potential to contribute to chaotic states for organizations (Hardy, & Laslett, 2015; Lombardi et al., 2014). The various continuous control monitoring methods associated with the control monitoring methodology were a confusing factor for corporate managers when considering adoption (Singh et al., 2014). The results of this research shifted the focus of continuous control monitoring from financial controls and regulations to improved efficiency in fraud prevention and enterprise risk management for financial reporting.

The adoption of continuous control monitoring was a prudent management decision due to the cost recovery, efficiency, and fraud-prevention benefits that the capability provided (Hardy, & Laslett, 2015). With the evolution of continuous control monitoring methods, recent advances made the technologies more widely available and affordable, yet firm leaders had not made significant steps with these methodologies (Hardy, & Laslett, 2015; Whiting et. al., 2012). The purpose of this qualitative, multiple-case study was to explore the experiences and perceptions of audit processes used with compliance efforts including control monitoring, and the impacts on enterprise risk management, including fraud risk. Using a theoretical framework

and prior research development provided the rationale for performing the planned investigation into regulatory compliance, enterprise risk management, and control monitoring processes.

Chapter 2: Literature Review

Introduction

Evolving regulatory environments, increased globalization, market pressures to improve operations, and rapidly changing business conditions create an ongoing need for timeliness and ongoing assurance that controls were working effectively and risk was being properly mitigated (Steinhoff, et al., 2016). Continuous control monitoring could provide corporate managers a holistic view of operations and the ability to explore company-wide detailed transactions as a means to assess control frameworks electronically. Through the use of these methods, corporate managers have the opportunity to improve enterprise risk management programs, including fraud risk mitigation efforts. A challenge with continuous control monitoring remained an inability for employees to adapt to a change within large technical, even as the technology has continued to advance significantly, making these approaches a more practical solution for managers in the area of potential improvements in enterprise risk management (Steinhoff et al., 2016). This literature review included narratives related to (a) continuous control monitoring; (b) globalization; (c) governance; (d) information technology; (e) implementation; and (f) risk and fraud detection.

Documentation

The literature reviewed included publications newer than 5 years old and seminal studies. Discussions included in this section also focused on the analysis of websites of business organizations like the American Institute of Certified Accountants (AICPA), the Association of Certified Fraud Examiners (ACFE), Deloitte, KPMG, and the Information Systems Audit and Control Association (ISACA). The Northcentral University online library and Google Scholar provided the required links to the databases and online libraries. Key databases accessed for

peer-reviewed articles, books, and journals included Ebrary, EBSCOhost, Pro Quest, Academic Search Complete, and Business Source Complete. Search terms included *continuous control monitoring* combined with advanced search terms including *financial reporting*, *business*, *accounting*, *information technology*, and *fraud*. Using these keywords, 153 relevant articles were obtained, from which the researcher selected 60 abstracts. After reading through these abstracts, 37 useful documents formed the basis for this literature review.

Some advances in the study of the introduction of technologies for continuous control monitoring and methodologies had not been made (Lombardi et al., 2014; Singh et al., 2014). A consistent set of recommendations or guidelines for continuous control monitoring had not been developed, nor has there been an exploration of the perceptions and experiences of financial executives regarding the incorporation of technical tools for continuous control monitoring and potential improvements for enterprise risk management, including fraud risk. Existing work had focused on the putative benefits and business process improvements yet had not advanced any guidelines and recommendations on regulatory compliance, and advantages for enterprise risk management efforts (Lombardi, et al., 2014; Singh et al., 2014).

Theoretical Framework

Diffusion of innovations theory. A key theoretical model associated with adoption was the diffusion of innovations. The diffusion of innovations theory (Huffman & Crump, 2005) was a noted framework through which the communication of the innovations in fraud prevention techniques travels through the channels, over time, among corporate managers. Four main elements key to the diffusion of innovations theory, as noted by Huffman and Crump (2005) included innovation, communication channels, time, and social systems.

The basis for rates of adoption of these innovations related to the characteristics of relative advantage, compatibility, complexity, trialability, and the observability for other corporate managers within the given social system (Huffman & Crump, 2005). Applying the diffusion of innovations theory through the given research, allowed information to be gathered from the corporate managers in a way that indicated the value in sharing of knowledge from early adopters with late adopters, to communicate the innovation advantages, and impact adoption rates by corporate managers, and improve overall enterprise risk management, resulting in reductions in fraud (Davis, 1989). Thus, sharing of information in this manner contributed to the improved potential usage of modern information technology tools, which in turn allowed corporate managers to more effectively prevent fraud relative to financial statements. Furthermore, the degree of relative advantages of the fraud prevention technology compared to the existing manual tools currently utilized by corporate managers was a key to the application of the diffusion of the innovations theory throughout the given social group of corporate managers (Huffman & Crump, 2005).

Corporate management views were relative to the degree of innovations. The value corporate managers found compatible with existing values and norms was important to understanding relative to the adoption of the innovations (Hong et al., 2002). Further, due to the complexity of these innovations, and any potential perceived thought that new prevention tools were difficult to understand and use, could have contributed to slower adoption (Huffman & Crump, 2005). Research data using this theory built upon and provided greater visibility in the areas of financial fraud prevention and meeting regulatory requirements. As businesses grew globally, technology is rapidly changing, and business requirements became stricter with financial reporting, additional future research provided further information to business

executives that could enhance corporate business strategy. There existed given rates of adoption of these innovations based upon the characteristics of relative advantage, compatibility, complexity, trialability, and the observability to others within the given social system of corporate managers. The diffusion of innovations theory indicated a need for sharing of knowledge from early adopters with late adopters, in order to communicate the innovation advantages and increase adoption by more corporate managers.

Technology acceptance model. Technology acceptance model (TAM) was one specific model that provided a framework for explaining information technology acceptance behaviors, including acceptance of the new fraud prevention techniques. Technology Acceptance Model provided information regarding the impact of external variables on individual corporate managers' intention toward accepting IT changes. These types of individual differences have significant impacts on IT acceptance decisions (Hong et al., 2002). The theoretical ground for the model was Fishbein and Ajzen's Theory of Reasoned Action (Hu et al., 1999). This theory was based upon beliefs influencing individual attitudes, which in turn shape the behavioral intention guiding, which result in the individuals' behavior. This theory provided a method for identification and examination of the individual influences of corporate managers, and their perceptions of ease of use, and complexity involved with the innovations in fraud techniques.

Continuous Control Monitoring

Continuous auditing tools, techniques, and technology had been widely discussed by academics, the business community, and audit professionals over the years regarding the impact continuous auditing has on the audit industry (Majdalawieh, Sahraoui, & Barkhi, 2012; Vasarhelyi, Romero, & Kuenkaikaew, 2012). However, there was not as much research into continuous control monitoring tools (Lombardi et al., 2014). The introduction of new

methodologies provided both advantages and disadvantages to organizational goals due to their current processes, technology platforms, and resources (Lombardi et al., 2014). A new methodology provided opportunities for encouragement for corporate managers within the organizations to invest in a large amount of time and resources and ensuring that they received a positive return on investment in the implementation.

Through the different studies performed on continuous control monitoring, some lessons and insights have been obtained regarding continuous monitoring (Lombardi et al., 2014; Singh, et al., 2014). These studies allowed for an examination of the provided insightful information regarding the unique issues inherent with continuous control monitoring, which were fundamentally different from issues encountered in standard control monitoring (Lombardi, et al., 2014; Singh, et al., 2014). Lombardi, Vasarhelyi, and Verver (2014) identified several key steps in continuous control monitoring including:

A. Identification of potential processes or controls based on industry frameworks of COSO, COBIT 5, and ITIL and defining a clear scope of control assurance based on business and IT risk assessment to establish a priority of controls for continuous monitoring.

B. Development and formalization of control goals and key assertions within the concept of information technology risk.

C. Definition of the automated metrics that highlight either success or failure of a given assertion.

D. The determination was made of the process frequencies necessary to conduct tests at a given point of time that was close to when key transactions and processes occur.

> E. Creation of processes for managing the alarms generated, including proper communication, and necessary investigation of failed assertions, ultimately correcting any control weakness, or potential for enterprise risk, including fraud.
>
> (Lombardi et al. 2014)

Although this information provided managers some important learning towards gaining an understanding in the area of continuous control monitoring, there remained a need for further understanding regarding the overall scope of enterprise risk management benefits provided from a structure based on critical business and IT processes. Additionally, there was a need for examination of the prioritization based on risk and prior experience in reviewing the controls through audits, self-assessments, and control breakdowns. The priority or suitability of controls for continuous monitoring required further consideration of the relationships among controls, for example, configuration and vulnerability management could have reliance upon asset management and may be deficient and not suitable for inclusion in the scope of assurance. In such a case, the controls that depended on it may not have been suitable for continuous monitoring. In order to understand these areas, the study provided information regarding the managers' perceptions of the introduction of new technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods.

Key historical background. In a landmark study for the field, Masli, et al., (2010) indicated that due to both business and regulatory demands there were increased pressures and needs for sophisticated internal control monitoring. Yet external audit partners continued to have doubts regarding the benefits of these audit-related information technology resources, both continuous audit and continuous control monitoring tools. To provide some insight in the area of research, Masli et al. (2010) tested a hypothesis regarding three explicit benefits for assurance

outcomes: "more effective internal control systems, enhanced audit efficiency, and timely audit reporting" (p. 1002). The research examined both types of assurance, internal and external, associated with an implementation of continuous technology. The study identified 139 announcements of internal control monitoring program purchases from 2003 through 2006, with an additional assigned control group. Overall, results showed there was support for and an identification of three key benefits related to hypothesis assertions that implementations of technology control monitoring programs increased effectiveness. Further, there were indications for a need for further identification of objective-oriented metrics to assess benefits of technology implementations. However, the existing research included a large utilization of archival data and the related potential for omitted correlated variables. A further constraint of the research related to the sample limitation to disclosures of Sarbanes-Oxley related internal control software implementations by organizations. Consequently, there was an indication that there remained a need for understanding the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts.

Additionally, while some historical surveys conducted by Deloitte (2010), which included multiple case studies, had shown increased interests in continuous control monitoring to ensure proper oversight and compliance and recent corporate failures and corporate transparency have led to the concept of continuous control monitoring, the practice of implementing continuous control monitoring tools and the demand for these services remained low. Further, noted by the results of these case studies, Deloitte (2010) indicated that relatively few corporations have implemented programs of continuous control monitoring or continuous

auditing, due to lacking strong business case support, or a clear picture of the potential benefits for implementation. Finally, there were indications of widespread levels of confusion regarding the definitions of the two different types of resources. This provided support for a need of additional research into the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts. The implementation rate remained low despite the need for improvements to enterprise risk management in order to improve corporate transparency and decrease corporate failures.

In relation to ERP systems, Kuhn and Sutton (2010), in another key historical study noted a focus of continuous control monitoring towards the identification of strengths and weaknesses of continuous auditing. Kuhn et al. further examined continuous auditing tools including EAM and MCL as two key continuous audit tools for overall corporate governance, designed specifically for business processes and enterprise resource planning, which provided corporate managers abilities relative to governance and risk management (Kuhn, & Sutton, 2010). Due to the evolving state of governance and focus of the research on methods that provided benefits for corporate managers to manage risk strategically, information indicated there were ongoing issues that managers face, and a weakness of the research was that there remained debate regarding how to manage those issues. There was thus support of a need for examining the experiences of corporate managers with regards to impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts. Further supported was a need for the perceptions of managers regarding the introduction of new

technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods.

Current environment. Some organizations had been evaluating the introduction of continuous control monitoring to support regulatory control assessment requirements (Singh et al., 2014; Steinhoff, et al., 2016). When beginning a continuous control-monitoring program focused towards enterprise risk management including fraud risk, corporate managers needed to understand the objectives and requirements that involved in continuous control monitoring (Steinhoff et al., 2016). These studies indicated that in designing an approach to continuous control monitoring, managers should consider all the businesses' objectives to ensure management enterprise risk management and fraud prevention goals were met adequately (Singh et al., 2014; Steinhoff et al., 2016). Further, there was support of a need for examining the experiences of corporate managers with regards to impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts.

Singh et al, (2014), investigated three continuous monitoring systems, SAP Secure, CAMAP, and Bagheera-SE through completion of real-world organizational activities review, in order to highlight the application of data analytics ability to process transaction data and monitor for controls and audit purposes on a near real-time basis. The study involved completion of a review of the design and implementation of these three separate systems in real-world organizations in order to highlight the application of data analytics ability to process transaction data and monitor for controls and audit purposes on a near real-time basis. The findings indicated benefits for identifying errors in transactional data, particularly related to the noted support that CAMAP provided the most relevant level of information for the given research as an

identified continuous control-monitoring tool, which allowed corporate managers to analyze financial data to identify control exceptions including violations of segregation of duties and anomalous vendor transactions in accounts payable activities. Additionally, support was provided through the identification of key issues for corporate managers to consider related to continuous control monitoring resource implementations, including areas of red flags and potential vulnerability to vendor fraud due to inadequate segregation of duties, resulting implemented changes in controls for the organization involved in the study. Through the identification of these red flags, corporate managers improved the identification of risk, and there was potential for improvements in enterprise risk management and fraud preventions. These results supported a need for implementing continuous control monitoring and the need for examining further the value of executive management regarding potential benefits for improving enterprise risk management, including prevention of fraud. There was the limitation that the information reviewed included information technology resources with a focus on continuous auditing. Information was needed regarding companies of varying sizes and views towards continuous auditing and monitoring functionality that supports enterprise risk management goals need to further evolve, as it was noted they have yet to do (Singh et al., 2014). This supported a need for examining the experiences of corporate managers with regards to impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts.

In a study of small and medium organizations, Dull (2014) further focused on continuous control monitoring use of tracking access to information for risk management, and detection of fraud, indicating that through the use of security settings unauthorized access used to commit

fraud can be monitored. This focus included monitoring debit and credit card payments, payroll data, and sales returns. The results were focused upon increased monitoring through Benford analysis and indicated that continuous monitoring of these control areas improves the governance and risk management of the organization, for organizations beyond large corporations. Further, Benford analysis was a resource for managers to identify potential fraud risk, and manage the risks.

Nigrini (2017) further indicated, in a case study of HealthSouth financial statement fraud, that Benford analysis was a continuous control monitoring resource based on statistical probabilities, utilized to analyze the first digits of monetary amounts within accounting transactions, and identify any anomalies and raise red flags related to avoiding the controls built into the system including approval levels, such as cash disbursements of the organization (Nigrini, 2017). Benford's Law was reviewed and divided into five categories of accounting classifications. Further, the study included the proposal of a Benford-based audit sampling method that selected as the audit sample the set of transactions or balances needing removal from the audit population to allow for a population that conforms to Benford, which was then reviewed and reexamined. The typical software programs identified best for this type of continuous control monitoring included ACL and IDEA, which allowed managers to perform analysis easily for a wide range of datasets, and transactions could be imported into either software (Nigrini, 2017). Through the case study method, as was advocated, large audit samples could be easily generated, however, there existed a noted accuracy rate that was questionable even when known errors were seeded into the data. Finally, Nigrini (2017) reviewed new perspectives on using Benford's Law in auditing by reviewing four key areas that included mathematical bases, type of auditee data, options to limit sample size, and sampling approach

limitations. These perspectives had a basis on some facts related to the execution of the HealthSouth financial statement fraud. Support was provided for the goal of the research for improved enterprise management and fraud prevention, as through identifying these anomalies, corporate managers can then inquire about potential issues, and manages fraud risk. Identified was a continued focus of various completed research on the technical side of continuous control monitoring, rather than focusing on understanding the perceptions and challenges relative to continuous control monitoring implementation efforts for corporate managers. There remained a gap in the literature related to the experiences of corporate managers concerning impediments to adoption, implementation, and use of continuous control monitoring procedures for fraud prevention controls to manage organizational risk in maintaining corporate requirements including enterprise risk management and fraud prevention efforts. These were currently unknown, and therefore these fraud prevention tools continued to be underutilized.

In other research, Mandru (2016) completed a qualitative and quantitative analysis of enterprise risk management utilizing two identified methods; risk score matrix Risk score matrix Â decision tree and Monte Carlo simulation, with results that showed the risk management process, involves five basic stages including setting goals, risk identification, risk evaluation, risk response planning, and risk monitoring and control. Additionally, there was information provided regarding another key preventive measure for corporate managers to apply when facing risks and these methods allowed corporate managers to improve preservation of the competitive market advantage. Mandru (2016) indicated these improvements included the use of systems parallel scanning and risk scoring methods.

While the existing studies completed to date included some information about continuous monitoring technology, some research focus continued to be in the area of continuous auditing,

rather than continuous control monitoring (Kuhn & Sutton, 2010; Majdalawieh, et al., 2012; Singh et al., 2014; Vasarhelyi, et al., 2012). Further, while there were studies on individual topics relating to information technology, limited research existed considering fraud prevention needs and the challenges of corporate managers relative to current technological advancements and enterprise risk management initiatives. Thus, a gap remained relative to examining the area of need for increasing efficiency of control monitoring, and compliance efforts including fraud detection (ACFE, 2017). Continuous control monitoring has an important role in corporate management as a method through which to achieve increased operational efficiencies and provided an opportunity for increases in productivity and competitive advantages within compliance and fraud prevention functions, including the growing need of organizations expanding into global markets (Lombardi et al., 2014).

The key to making effective use of continuous control monitoring was to develop a good understanding of the main business processes, the associated information systems, and infrastructure. When an organization adopted continuous control monitoring, corporate managers were required to have knowledge of information systems and data analysis skills. Corporate managers had a need to support the continuous control monitoring efforts to ensure a successful implementation (ACFE, 2017; Mandru, 2016; Singh, et al., 2014; Steinhoff, et al., 2016).

Globalization

As an organization expanded the business to locations including international operations, concerns relative to the security of business data ranked high with corporate managers (Steinhoff, et al., 2016). Information technology governance was essential in ensuring organizational leaders follow regulations and laws to protect business information. In a survey response to the AICPA, the Institute of Internal Auditors (IIA) attributed increased interest in

continuous control monitoring to the evolving regulatory environment, including the increased globalization of businesses (AICPA, 2012). Further, noted was that previous qualitative research performed on control monitoring and business process auditing showed that continuous control monitoring has expanded to international companies and indicates that concerns with security controls and governance remained (AICPA, 2012). Supported was a need to understand the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts. Additionally, indicated was the need for examining the perceptions of managers regarding the introduction of new technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods (AICPA, 2012).

Researching information technology governance within global organizations involves different areas, including regulations, policies, and procedures (Salvioni & Astori, 2013). Each given country has varied laws and regulations for export and import controls, and the governance of those controls (Salvioni & Astori, 2013). Salvioni and Astori (2013) indicated that information technology governance plays an important part in the success of the organization. Most organizations have controls and guidelines in place to ensure the assessment of the effectiveness of information technology governance (Salvioni & Astori, 2013). Domestic or international organizations were required to have controls to achieve information technology as levied, and these regulations could differ according to the government laws in place (Salvioni, & Astori, 2013). Globalization had the potential to impact corporate manager decisions related to the implementation of continuous control monitoring for enterprise risk management, and fraud risk management. There continued a lack of research with the focus towards examining the need

to understand the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts.

While available resources provided some information regarding globalization and indicate there was a potential impact for managers in decision-making, they did not examine the impacts of globalization to the adoption of continuous control monitoring procedures (AICPA, 2012; Salvioni & Astori, 2013; Steinhoff, et al., 2016). Continuous control monitoring was a resource for improving enterprise risk management, and fraud prevention, not covered by these resources. Further, these resources did not examine the use of continuous control monitoring in fraud prevention efforts for information technology governance, including the perceptions of managers regarding the use of tools such as system parallel scanning, and risk scoring methods (AICPA, 2012; Salvioni & Astori, 2013; Steinhoff, et.al., 2016). As corporate managers were faced with business environments that become more complex and international, the complexity and scope of compliance efforts also increase significantly. Companies were faced with conflicting regulations when international boundaries were crossed (Salvioni & Astori, 2013). Businesses that pursued globalization could leverage information technology to ensure enterprise risk management in these new complex environments of operation.

Governance

Key historical background. Olach (2008) noted the regulation of auditors and oversight activities by the audit enforcement agency Public Company Accounting Oversight Board (PCAOB) including audit inspections. As noted in the qualitative research by Olach (2008), the resource provided information regarding potential disciplinary actions for violations of the

Sarbanes-Oxley Act, PCAOB and U.S. Securities and Exchange Commission (SEC) rules. The study by Olach (2008) provided seminal information important to executives in organizations in providing those rules related to proper internal controls, and the responsibilities of management and the company board of directors for ensuring effective internal control over financial reporting. Consequently, while the rules were provided, it was not indicated how to implement methods to improve effective internal control, enterprise risk management, or fraud prevention. This research was relevant as it related to the potential experiences of corporate managers and potential impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management.

In an additional landmark study, Gheorghe (2010) indicated the importance of audit methodology and the need to minimize information technology risks through an updated audit methodology in information technology governance. This qualitative historical research by Gheroghe (2010) indicated the importance of classifying relevant information technology risks associated with governance, to identify critical system risks, due to the evolving nature of information technology systems. Gheorghe (2010) further indicated the need to control these risks in order to meet strategic business goals and maintain legal and regulatory compliance. Further information indicated was regarding the need for updates to methods for identifying and controlling risks associated with evolving information technology. However, missing from the research was an identification of specific methods including implementation of continuous technology to evolve the actual identification and control of risks, including how to achieve improvement of enterprise risk management, and fraud prevention (Gheorghe, 2010). This supports a need for additional research relative to the need to understand the use of continuous

control monitoring value in fraud prevention efforts for information technology governance efforts. The information provided by these two studies indicated the need to understand the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts. Additionally, there was support for a need to examine the use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including the perceptions of managers regarding the use of these resources.

Current regulatory environment. Vasarhelyi (2012), in a qualitative historical review in the area of cloud computing, risk analysis, and implementation of continuous control monitoring, studied continuous assurance including advances in financial accounting due to cloud computing relative to risk analysis, and methods for continuous assurance, including factors that affect implementation of continuous control monitoring. A key area of focus by Vasarhelyi (2012) was towards providing accounting information systems data including an identification of required legal standards, which companies and managers must comply with, and their relevance to the evolving information systems resources. Vasarhelyi provided key seminal information including details related to risk analysis, standards, and continuous control monitoring, important for the current research effort (2012). However, there was a lack of detail to a historical review, and thus perceptions and experiences of corporate managers' regarding the impediments to adoption for the implementation and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts. This limited the relevance associated with the identification of factors that affect an actual implementation.

Richardson (2012) indicated the Dodd-Frank Act included requirements for corporate managers to measure systemic risk in order to provide the requirements to meet the enhanced regulations was indicated. As noted by Richardson (2012), the Dodd-Frank Act now required executive management to utilize tools for measuring systemic risks, designate sectors that pose a specific systemic risk, and provided for further enhanced regulation of those identified sectors. Further, there was importance to executives in organizations associated with providing those rules for the identification of systemic risks, including fraud risk, and the responsibilities of management for proper financial reporting of the results of operation of the company (Richardson, 2012). However, there was a limited focus on proper financial reporting of results of operation, including a lack of information regarding the potential for corporate managers to further improve efficiency in fraud prevention, and enterprise risk management, and increase perceived value of the continuous control monitoring resources. In other research completed by Gupta, Weirich, & Turner (2013) it was noted that audit quality and integrity of the accounting profession have remained integral parts of financial reporting. The Sarbanes-Oxley Act had direct ramifications on the nature of fraud discovery and compliance efforts for all publicly traded companies. Further, the Sarbanes-Oxley (SOx) Act had fundamentally influenced financial reporting, internal control, and corporate governance (Gupta, Weirich, & Turner, 2013). The unstated goal of SOx was to ensure corporate fraud would not have the opportunity to occur. Ordinarily, however, most corporate managers agreed that the current day impact that has the most momentous provision was Section 404, requiring substantiation of financial reporting controls. Increasing corporate accountability and regulatory pressures pushed corporate managers to enhance effectiveness and efficiency in their work, in meeting corporate stewardship responsibilities, including enterprise risk management efforts and fraud prevention

and detection (Gupta, et al., 2013). Accordingly, was the requirement for corporate managers to not only put controls in place but to evaluate controls on an ongoing basis to provide shareholders reliable financial statements which reflect the true state of the company (Gupta, et al., 2013). These regulations potentially affected managers' decisions regarding implementation of continuous control monitoring resources. There was a continued overall focus mainly on financial reporting impacts, rather than on enterprise risk management, and fraud prevention. There remained a gap in understanding that corporate compliance offers advantages for potential improvements in risk management beyond financial reporting.

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Guidance on Monitoring Internal Control Systems supported using continuous monitoring technology and reports tailored to an organization (ISACA, 2014). According to COSO, when an organization monitors, this improves identification of and correction of internal control problems on a more timely basis; producing more accurate and reliable information for use in decision-making. Further, COSO (2013) indicated that continuous monitoring improves the accuracy and timeliness of financial statements, allowing organizations to be in better position to provide required certifications and assertions on the effectiveness of internal controls, and improves risk management. According to COSO's Internal Control—Integrated Framework (2013), using technology-based continuous monitoring techniques provide an efficient and low-cost way to review large volumes of data. When these techniques were embedded within a system, all business-event transactions may be examined in real time, rather than the traditional review of a subset of transactions after business events occur. An ongoing evaluation program of controls was implemented efficiently and effectively when using the embedded continuous monitoring techniques along with thorough reviews of the results of monitoring. COSO

objectives were related to the enterprise goals, information technology related goals, and some enabler goals in control objectives for information and related technologies, with financial statement assertions loosely translated in the technology context to areas of completeness, accuracy, validity, and restricted access (ISACA, 2014). The majority of the literature on continuous control monitoring related to business processes, and, as such, there was no specifically documented alignment or mapping among information technology control objectives or goals and the formal assertions necessary for formalized objective testing (ISACA, 2014). Further included was the provision of information that relates to the existing gap in the literature, related to the need for corporate managers within organizations to understand how the technology provided methods also for transformation in work environments (ISACA, 2014). Due to this gap in the literature, there remained an unknown relative to whether transformation leads to an ultimate overall gain, or instead produces a more chaotic state of operation between managers and the key stakeholders. This provided support for the research study purpose to further identify and explore the perceptions and experiences of corporate managers' regarding the impediments to adoption for the implementation and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts.

According to the ISACA (2014), processes for management assurance of controls were more informal than an audit, because they were based often upon professional judgment, rather than detailed testing. An audit was a systematic process in which a qualified team or person objectively obtains and evaluates the evidence regarding assertions about a process and forms an opinion on the degree to which the assertion was implemented. Further, the ISACA (2014) noted that in order to automate an assurance process, control descriptions must be reviewed to

separate those components of the control that can be formally tested, and those components that will rely on professional judgment. There was information provided by the ISACA (2014) regarding that internal control objectives in a business context, which were categorized against five assertions used in the COSO model: existence/occurrence/validity, completeness, rights and obligations, valuation, and presentation and disclosure. These assertions had been expanded in the SAS 106, "Audit Evidence," (AICPA, 2012) and, for the purposes of a technology context, can be restated in generic terms.

In additional research efforts by Malaescu and Sutton (2015) a quantitative study included 100 auditor participants and examined the reliance of external auditors on the internal auditor's use of continuous audit. As noted, there were increased demands upon corporate managers to produce timely and fluid assurance in the area of risk management. Consequently, the results indicated a need for movement towards automated control environments, and increased reliance levels by external auditors of internal audit work in a continuous audit environment, as opposed to the traditional environment of control monitoring (Malaescu & Sutton, 2015). Further, the results showed that audit fees were higher for traditional control testing by management, compared with the use of continuous control testing tools. Regarding key findings, information was provided relative to the benefits of implementing continuous control monitoring. However, there was a limitation related to the use of continuous audit, and not continuous control monitoring information technology resources by internal audit. Continuous information technology resources allowed corporate managers to have opportunities to reduce the burden of regulatory compliance, and enterprise risk management costs, by automating internal controls testing (Malescu & Sutton, 2015). This related to the ongoing gap that existed in the literature, related to information technology, and control monitoring resources.

While there were studies on individual topics relating to information technology and fraud, limited research existed considering fraud prevention needs and challenges of corporate managers relative to current technological advancements, particularly continuous control monitoring. Available studies regarding continuous control monitoring method existed yet researchers had not fully examined perspectives of corporate managers regarding efficiency improvements, including a lack of information related to financial fraud detection and prevention efforts, and regulatory compliance to include the use of information technology resources (ISACA, 2014; Malescu & Sutton, 2015).

Based on the Sarbanes-Oxley and SEC regulations, corporate managers had the responsibility of assessing risk and for the design and implementation of controls within an organization. Internal audit had the responsibility of evaluating the controls implemented by management and providing assurance to the audit committee as to the state of management's controls and maintaining proper enterprise risk management, and fraud control. The managers of companies were required not to only put controls in place, but to evaluate the controls on an ongoing basis so shareholders have reliable financial statements that reflect the true state of the company. While it was initially met with some resistance initially, most companies agreed Sarbanes-Oxley has led to heightening awareness of control inefficiencies and ultimately helps to protect the integrity of the company, including improved enterprise risk management.

Information Technology

Key historical data. In the area of information technology, Kuhn and Sutton (2010) completed a landmark qualitative historical study related to the current state of and the future directions for use of continuous auditing in ERP system environments. Results indicated that there were identified strengths and weaknesses of continuous auditing for ERP systems. Further,

noted was that continuous auditing tools including EAM and MCL were two key continuous audit tools for overall corporate governance, designed specifically for business processes and enterprise resource planning, which provide corporate managers abilities relative to governance and risk management (Kuhn Jr. & Sutton, 2010). Due to the evolving state of governance, and a focus of the research on methods that provided benefits for corporate managers to manage risk strategically, information provided regarded issues managers might face overall when implementing new technology, and the ongoing debate regarding how to manage those issues. Notwithstanding, the focus was limited to the current and future state of continuous auditing resources rather than continuous control monitoring information technology resources, thus the application of the information was more general overall in nature. This supported there were gaps in the research relative to continuous control monitoring information technology tools, due to the focus towards continuous auditing. Further, there remained a need in the area of gaining an understanding regarding the perceptions of corporate managers relative to implementation of continuous control monitoring tools, in order to understand the benefits and challenges in implementing these resources to provide increased effectiveness in compliance, enterprise risk management, and fraud prevention.

A separate landmark information technology study completed by Masli et al (2010) tested the hypothesis regarding three explicit benefits for assurance outcomes: "more effective internal control systems, enhanced audit efficiency, and timely audit reporting" (p. 1002). The research questions included both types of assurance, internal and external, associated with an implementation of continuous technology. The study included identification of 139 announcements of internal control monitoring program purchases from 2003 through 2006, with an additional assigned control group. Overall, these results indicated support for benefits related

to the hypothesis assertions that the implementations of technology control monitoring programs increase the operating effectiveness of the operations of controls. Furthermore, there was additional support provided that indicated the importance of identification of objective-oriented metrics to assess benefits of technology implementations. Consequently, as with other resources, the focus was limited to continuous auditing monitoring resources, rather than on management focused continuous control monitoring resources.

Based on the results of these landmark studies, there was an identified gap in the literature, and need for examination of corporate management resources that provide improvement opportunity and increases in enterprise risk management including fraud detection and prevention. A key responsibility overall indicated for managers in financial services was providing assurance to the chief executive officer (CEO) and executives of management of high-rated risk factors and that appropriate controls were in place and operating effectively.

Current technology environment. Due to increases in the regulatory regime, increasing technology complexity, and pressures on cost, organizations must identify productivity improvements in the evaluation of the performance of internal controls. One method of productivity improvement is applying technology to allow near continuous, monitoring of control operating effectiveness, known as continuous controls monitoring (Lombardi et al., 2014). This is particularly true for high-frequency transactions. It was important to understand that continuous control monitoring is a subset of continuous assurance, alongside continuous data assurance, which involved verifying the integrity of data flowing through systems, as well as continuous risk monitoring and assessment, measuring risk dynamically (AICPA, 2012). Improved management and monitoring of controls through continuous control monitoring, and associated risk management activities provide opportunities to reduce the extent to which audit

and assurance staff need to undertake annual detailed testing of controls and improve overall enterprise risk management efforts including fraud prevention and detection (Lombardi et al., 2014; Majdalawieh, et al., 2012). Existing studies by researchers had noted that there were potential cost reductions through improved efficiency and effectiveness as well as other potential benefits including reduced risk velocity and potentially reduced remediation cost, greater visibility and the ability to identify trends, which potentially provided improved overall risk management (Lombardi et al., 2014; Majdalawieh, et al., 2012). A limitation identified throughout studies was that the focus has been on improvements to financial reporting, rather than actually improved enterprise risk management (Lombardi et al., 2014; Majdalawieh, et al., 2012). Moreover, another gap that remained related to the diffusion of innovation was a need for improving the communication between peers in the corporate manager social system regarding these new ideas including what potential future innovations were available in fraud prevention (Lombardi et al., 2014; Majdalawieh et al., 2012). This existing gap related to the need to examine the experiences of corporate managers regarding impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts.

Further knowledge was gained from a study completed by Singh et al., (2014), which provided information on continuous auditing and continuous control monitoring, with specific areas related to the investigation of three continuous auditing and continuous monitoring systems, in particular, SAP Secure, CAMAP, and Bagheera-SE. The methodology was a qualitative case study. Singh, et al. (2014) noted that the review of the design and implementation of these three separate systems in real-world organizations in order to highlight

the application of data analytics ability to process transaction data and monitor for controls and audit purposes on a near real-time basis. CAMAP provided the most relevant information for the given research as the identified continuous control-monitoring tool, which analyzed financial data to identify control exceptions including violations of segregation of duties, and anomalous vendor transactions in accounts payable activities. The findings revealed issues including red flags and potential vulnerability to vendor fraud due to inadequate segregation of duties, resulting in implemented changes in controls for the organization involved in the study. The results included information on how implementing continuous control monitoring adds value for executive management regarding potential benefits for improving enterprise risk management, including prevention of fraud. One noted strength was information provided regarding key issues and potential benefits of both continuous auditing and continuous control monitoring in ERP environments. Consequently, one noted weakness of the study was the limitation of focus to that of examining the quantitative technical side of continuous control monitoring, a gap remained regarding understanding the perceptions and experiences of financial managers regarding the use of technical tools for continuous controls monitoring. According to Lombardi, Vasarhelyi, and Verver (2014), and Majdalawih, Sahraoui, and Barkhi (2012) there were indications that in order to continuously assess controls, rules need to be developed to test in real-time compliance. Further, indicated was that the required tests should be classified into seven broad categories based on traditional audit processes or evidence types (Lombardi et al., 2014; Majdalawieh, Sahraoui, & Barkhi, 2012). These categories included asset management queries, electronic confirmations and statement queries, re-performance of selected controls, observations, analytical procedures, and automating collation of responses. Asset management queries and transaction confirmation were considered type 1 or 2 tests that use the company's

existing or improved key risk indicators to provide a risk indicator continuous assurance (RICA) framework (Nigrini, & Johnson, 2008). Additionally, past audit report evidence may assist in the identification of sources of data and applicable analytics (Lombardi et al., 2014). Strengths of these studies included details related to a need to develop control monitoring and testing in real time, and management data for high volume transactions in specific cases. An overall weakness was that the focus of these studies was on the technical side of continuous control monitoring, with a gap remaining regarding what potential improvement there is relative to enterprise risk management, and fraud prevention. This supports a need for understanding the experiences of corporate managers regarding the use of technical tools and processes for continuous control monitoring. Managers may identify benefits by monitoring processes through mechanisms including key risk indicators, to alert the business to potential control issues, as part of a continuous improvement cycle, and improve overall enterprise risk management, including the management of fraud risk. Continuous control monitoring takes selected key risk indicators combined with the results of other tests and analytics on processes, and forms part of an overall risk assurance program in which the concerns over the monitored controls were validated before being prioritized and acted upon alongside issues identified by another periodic manual testing (AICPA, 2012).

In further research completed by Schermann, Wiesche, and Krcmar (2012), it was indicated that additional risk and key control deficiencies were identified through management risk and control self-assessments that form part of the program based on management knowledge gained through operating the plan-build-run-monitor cycle. The goal of this research was an investigation of information systems (IS) role in addressing the challenge of achieving a trade-off between exploitative and exploratory management control activities for corporate

management. Because the relationship between IS and management control activities is complex, Schermann, et al. (2012) utilized the grounded theory approach and provided an integrative view relative to the issue. Further developed was a grounded model that explored the relationship between IS and management control activities, to highlight the ways in which GRC IS served as a catalyzer for establishing balanced management control systems that enable corporate managers to simultaneously exploit and explore richer management control information. Integrated issue management utilized a GRC platform facilitates digitization, automation of alerts and management of remediation activities once these were agreed upon by management. As noted by existing studies, technology was an essential element in continuous control monitoring, which serves as a key strategic enabler, enhancing all aspects of the control compliance process (Steinhoff, et al., 2016; Ajah & Inyiama, 2011; Masli, et al., 2010). These studies included information that technology-enabled control monitoring can make the control testing process faster, cheaper, more efficient, and more effective (Ajah, & Inyiama, 2011; Masli, et al., 2010). Furthermore, with a technology-enabled approach to continuous control monitoring, organizations have theoretically eliminated the need to rely upon a linear model, and these advances in information technology provided for greater efficiencies to meet the increasing demands on corporate managers to improve enterprise risk management efforts (Steinhoff, et al., 2016). However, while these studies have examined factors that may affect business values, study results did not estimate improvements in compliance (Ajah & Inyiama, 2011; Masli et al., 2010; Steinhoff et.al., 2016). There remained a gap in the literature in this area of potential improvement to enterprise risk management, and fraud prevention and detection.

Issues. In further research completed by Dickins and Reisch (2012), examined were information technology, fraud risk, and an ongoing inability to identify fraud with existing audit

resources. As indicated by Dickens and Reisch (2012), an inability to identify fraud was often due to lack of experience with identifying information technology risks. The main research focus was related to the identification of the importance of detection of fraud through red-flag indicators, which must include IT-related issues and the use of evolving systems internal controls detected. This research was important due to the inclusion of automated continuous audit tests performed on the processes. Additionally, information provided related to a key area of the research, the issue of having the necessary experience of staff in the given organization, and a lack of knowledge base, resulting in a need for training in information technology. Notwithstanding, the focus was again limited to continuous audit, and does not include continuous control monitoring information technology. There remained a gap in the research regarding existing continuous control monitoring resources utilized by corporate managers for enterprise risk management. Thus, this provided additional support for the need to identify the perceptions of managers regarding the introduction of new technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods.

Firms today had become far more complex and technologically dependent than they were even in the recent past. The complexity and dependency on technology suggested that organizational controls needed to be re-engineered to provide cost-effective processes or return on investments. Making use of new technologies such as continuous assurance or continuous monitoring allowed organizations to incorporate new processes that were cost-effective and with greater capability. The passage of the Sarbanes-Oxley Act of 2002, in particular, the requirements of Section 404 greatly expanded the internal control work performed, has resulted in a strong increase in demand for qualified personnel, leading to personnel shortages and management cost increases. Additionally, the progressive sophistication of information

technology underlying modem business processes has made the traditional approach of control monitoring ineffective. Corporate enterprise resource planning systems, designed for high-volume online transaction processing, incorporate thousands of automated controls that can be configured in numerous ways, and the manual verification of the status of these controls is becoming costly. Additional drivers of audit automation adoption include the ever-growing complexity of business transactions and increasing risk exposure of modem enterprises. Several studies have shown that the deployment of information technology and decision support systems to automate certain parts of the control monitoring process usually results in a better-controlled, enterprise risk management system (Lombardi et al., 2014, Majdalawieh, et al., 2012; Steinhoff, et al., 2016). While continuous monitoring of access controls and authorizations is well developed in computer security applications, monitoring enterprise system configuration and business process settings remained an emerging area of development (Ajah & Inyiama, 2011; Lombardi et al., 2014, Majdalawieh, et al., 2012; Steinhoff, et al., 2016).

Information technology advancements affected how companies were organized, conducted business, and communicated with both stakeholders and employees (Ajah, & Inyiama, 2011; Lombardi et al., 2014; Majdalawieh, et al., 2012; Vasarhelyi, & Verver, 2014). Changes in technology and increases in business complexity had attributed to a need to develop new methodologies and processes for control monitoring. Recent technical and regulatory developments had contributed to corporate managers' adoption of technology tools for continuous control monitoring (Ajah & Inyiama, 2011; Lombardi, et al., 2014; Majdalawieh, et al., 2012; Steinhoff, et al., 2016). Prior research had focused on the quantitative technical side of continuous control monitoring, rather than exploring the perceptions and experiences of financial managers regarding the use of technical tools for continuous controls monitoring. As businesses

grew globally, technology had rapidly changed, and business requirements had become stricter with financial reporting, thus additional future research provided further information to business executives that could enhance corporate business strategy. Ordinarily, continuous control monitoring programs had provided benefits for organizations; however, barriers still existed for implementation. Both cultural and technical in nature, these barriers included training and development needs for future corporate managers, accounting staff, and auditors. Further, there were needs for investment justification and information related to the need for improved enterprise risk management to meet increased compliance rules monitoring (Ajah & Inyiama, 2011; Lombardi et al., 2014; Majdalawieh, et al., 2012; Steinhoff, et al., 2016). As continuous control monitoring solutions become more sophisticated, organizations must move rapidly toward implementation of automation resources (Steinhoff, et al., 2016).

Implementation

Multiple advancements in fraud-fighting techniques have been available for corporate management for some time, yet managers have not widely implemented the tools to combat financial statement fraud internally. Data mining and continuous controls monitoring were two tools frequently identified as providing effective benefits in combatting fraud related to information technology advancements occurring in the modern corporate accounting environment. Several research studies have touted the effectiveness, in various environments while using data mining techniques. Hsieh and Lin (2013) evaluated the U.S. Marine's likelihood of using earnings manipulation by using a process of data mining called Benford's law to detect fraud. In Nigeria, researchers Ajah and Inyiama utilized several of the information technology-based techniques, including data mining, credit risk management, and biometrics, to create a safer loan system (Ajah & Inyiama, 2011). To combat management fraud Whiting et al.

conducted research using several types of powerful data analysis techniques (2012). Consequently, some identified strengths were the focus on advancing the current data mining tools, and these research studies identified the areas of predictive learning, stochastic gradient boosting, and random forests, as key tools in advancing fraud prevention efforts. Ordinarily, the identified main objective of data mining was the ability of the program to adapt and learn to recognize patterns of both the users and the machine with predictive learning. Stochastic gradient boosting increases the efficacy of predictive learning techniques by combining statistical regression analysis trees with a goal of decreasing errors, and preventing fraud (Whiting et al., 2012). Building on boosting techniques, a random forest method uses regression tree data that still includes all the original data and has not been pruned (Whiting et al., 2012). Accordingly, as these techniques increased the effectiveness of detecting fraud more than traditional data mining alone, there was a need for corporate management to consider these techniques as tools for internal fraud prevention, as they improved the ability to detect instances of financial statement fraud.

Some studies completed by researchers have shown that continuous control monitoring (CCM) provide managers an information technology-based fraud tool, which advances the corporate manager's ability to monitor fraud within the company by using automated anti-fraud controls. CCM had the potential to provide the corporate management of the company the capacity to monitor items otherwise almost impossible to audit manually due to the complicated nature of the data included (Ramamoorti & Dupree, 2010). Consequently, the CCM programs had the ability to identify exceptions, through a comparison of data against preset parameters, identify key changes, and monitor the consistency and reliability of data received. By constantly monitoring all aspects of the company, the CCM system offered benefits of improvements upon

the existing system of internal controls, keeping them current, and preventing them from breaking down over time (Ramamoorti & Dupree, 2010).

Further, related to the diffusion of innovations was that due to the complexity of the technology fraud prevention tools, and ease of use issues, some managers considered the option of using a third party for their CCM, which might have included external auditors, or fraud examiners, while other managers had yet to begin taking any steps. Alternatively, some corporate managers chose to address the topic in a different way, attempting to train their employees to spot irregularities, believing they knew the company behaviors' best, yet these practices required substantially more time than automated, and advanced technology options (*The nature of fraud is changing*, 2013). Notwithstanding, even with these advances in technology, a corporation could not abandon their traditional fraud, compliance, and internal audit tools. Rather, data mining and continuous controls monitoring would work best operating alongside one another. Thus, examining the use of modern information technology tools for fraud prevention, in conjunction with existing fraud methods of corporate managers, to improve the current fraud detection and prevention relative to financial statement reporting was important.

Recent adoptions. In the case study conducted by Lombardi, Vasarhelyi, and Verver (2014), for Talecris Biotherapeutics Inc., a global Biotherapeutics and Biotechnology Company that organization successfully implemented continuous monitoring of financial transactions to mitigate potential control, error, and fraud issues. The implementation was the responsibility of the business unit owners but was instigated and driven by the internal audit function. Talecris saw enormous benefits because of this continuous monitoring installation (Lombardi et al., 2014). The entire implementation process took one year, and although it took longer than

expected, continuous auditing technology has benefited the company in countless ways. Some of the key outcomes included (a) improved risk management and accountability,(b) monitoring and enforcing policy changes, (c) strengthened fraud detection, (d) tightened relationships with vendors to improve procedures, (e) strengthened processes and more stable controls, and (f) improved cross-functional controls (Lombardi, et al., 2014). The company's overall goal was to monitor controls and have the business process owners oversee the progress, and then implement each of the other five business process areas, focusing on one at a time (Lombardi, et al., 2014). In the Talecris project, managers and business process owners were involved in the creation of control tests, so they could clearly identify what needed to be reviewed (Lombardi et al., 2014).

ACL software. In the Talecris case, ACL was the main continuous control monitoring tool utilized by consultants who created all of the required documents and the company consulted with an outside information technology provider on integrating continuous auditing and monitoring software with the existing SAP installation. A direct link existed between SAP and ACL and an ad hoc basis was utilized to test parameters for filtering (Lombardi et al., 2014). After the ACL continuous auditing technology was customized and implemented for Talecris, management implemented auditing controls for each major section of the Purchase to Payable cycle: accounts payable, purchasing, and the financial controls group (Lombardi et al., 2014). Talecris had business units with separate and different issues that needed to be addressed and the tests were customized to each business' unique needs. Using ACL technology, the financial controls group within Talecris then took over and led each team in setting up additional controls to address any identified issues (Lombardi et al., 2014). The technology allowed management to perform the type of purchasing card tests that provide information valuable in the identification of unauthorized usage, allowing for potential increases in the efficient monitoring and analyzing

of high volume transactions. Additionally, these types of tests can lead to managers enhancing enterprise risk management efforts, including detection and prevention of fraud, while further ensuring the leveraging of available discounts and rebate opportunities. Further investigated were the benefits and challenges of implementing continuous controls monitoring (CCM). A noted remaining issue for all implementations, however, was that although continuous control monitoring has considered by the audit and information systems professions for years, there still remained a primary problem regarding how to integrate this methodology effectively within large technological infrastructures (Lombardi et al., 2014).

During the study, a number of those improvements were introduced to the Enterprise Resource Planning (ERP) system and could be demonstrated through the front-end of the business intelligence model (BIM). These BIM, a part of SAP, were another type of identified reporting tool that collects data from myriad feeder systems. As it was indicated that executives must be quick in making business decisions because they were under pressure from the increased complexity and regulation of business a noted overall strength for implementations of continuous control monitoring for corporate manager consideration was the indication that ability to examine transactions that compromise financial reporting. This could be one potentially effective way to identify a company's underlying risk, possible breaches of controls, and areas for improvement. Lombardi, Vasarhelyi, and Verver (2014) found that due to increasing interest in controls monitoring, professional publications have generated information regarding the potential benefits of CCM, thereby creating awareness, and addressing practical implementation issues along the way. These implications were applicable to auditing, accounting information systems, and other business curricula that examine company controls and their monitoring activities, including being of importance to corporate managers considering implementations of continuous

control monitoring resources for improving enterprise resource efforts, and fraud prevention. This provided support for the given research, and that continuous auditing and monitoring technology provided a vital function for ensuring the business units and cycles comply with controls. These tools offer a path forward for corporate managers in increasing enterprise risk management, and fraud prevention and detection.

Cloud technology. The efficient management of cloud infrastructure and deployments is another topic area related to information technology that attracting significant interest and has relevance to control monitoring advancements. Cloud computing was characterized by the information technology resources provided as general utilities to the organization, that were leased, and released in an on-demand manner. Complex cloud deployments may have led to an intricate layered structure, thus understanding these hierarchical systems, including proper management and control optimally involved both new and challenging tasks facilitated by monitoring pervasively.

Fatema, Emeakaroha, Healy, Morrison, and Lynn (2014) identified evolutionary adaptation of monitoring tools' capabilities from general purpose to cloud monitoring, including the practical cloud operational areas that would help cloud providers and customers in making an informed choice of an appropriate monitoring tool. A range of monitoring tools currently in use was evaluated to gain their technical insights, including the desired capabilities of monitoring tools to serve different cloud operational areas from both providers' and consumers' perspectives. Despite the identification of capabilities and potential for improvements, there remained an indication that these available tools were underutilized (Fatema, Emeakaroha, Healy, Morrison, & Lynn, 2014). Consequently, some key information gained included the practical capabilities that an ideal monitoring tool should possess to serve the objectives in these operational areas.

Moreover, based on these identified capabilities, a taxonomy was further presented and analyzed to determine various cloud monitoring tool strengths and weaknesses.

There remained future research challenges and trends in cloud monitoring and management, particularly as more corporate managers consider the implementation of financial systems which operate within cloud systems. The results of the study conducted by Fatema et al. (2014) discussed the challenges that existed and identified some future research trends in the area of cloud monitoring. Indicated was that although a broad variety of monitoring tools were available, from general-purpose infrastructure monitoring tools that predate cloud computing, to high-level application monitoring services that were themselves hosted in the cloud, few tools were available for general-purpose application monitoring, with the most appropriate application monitoring technique dependent upon the nature of the application (Fatema et al., 2014).

General-purpose infrastructure monitoring tools typically utilized a client-server model by installing an agent in every system monitored, and monitoring agents measure the metric values from monitored components and send them to the monitoring server. The server stored the collected metrics into database analyses of them sent alerts and generated graphs, and various trending reports based on the monitored metrics retrieved from the database. Depending on the system configuration, the existing primitive metric measurements initiated may be either through the monitoring server or by an external program script that resides on the monitored resource, and the latter arrangement has proven useful when performing monitoring behind a firewall (Fatema et al., 2014). When initiating a monitoring agent for collecting metrics, the measured elements were relevant metric values from the monitored components, and then sent these on to the monitoring server, and then depending on the configuration of the system, the server sent

alerts to interested parties on an occurrence of an event. Most of these monitoring systems used e-mail or other SMS as alerting mechanisms (Fatema et al., 2014).

Similar to the general-purpose monitoring tools, independent Cloud monitoring tools had agents installed in the monitored systems, which measured and sent monitored data to the server for processing. The server issued an alert in cases that need attention. Most cloud monitoring tools provided services like Software as a Service (SaaS), utilized to monitor third-party cloud installations (Fatema et al., 2014). A key area of information identified was that there were many desirable monitoring capabilities for managers to consider when implementing the new technology. Some noted areas to monitor included scalability, portability, non-intrusiveness, robustness, multi-tenancy, interoperability, customizability, extensibility, shared-resource monitoring, usability, affordability, and archivability (Fatema et al., 2014). This data provided support for the need for the current research and understanding the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts. Additionally, there was support for a need to examine the use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including the perceptions of managers regarding the use of these cloud resources.

There were indications that the monitoring resources and techniques had an important role to play in the research area that the information required to make informed decisions and that appropriate monitoring was crucial (Fatema et al., 2014). Accordingly, this provided support for the research, as surveying the capabilities of monitoring tools provided benefits, including the identification of certain key objectives including improvements to enterprise risk

management, and fraud detection and prevention efforts for corporate managers. Furthermore, these monitoring tools, including key performance indicators, were essential components to deal with various objectives for corporate managers when implementing various cloud operational areas.

Gaps remained in the research relating to continuous control monitoring and information technology governance that have potential to contribute to chaotic states for organizations (Hardy, & Laslett, 2015; Lombardi et al., 2014). Further, the currently available continuous control monitoring methods associated with the control monitoring methodology remained a confusing factor for corporate managers when considering adoption (Singh et al., 2014). Available literature related to the technical data indicated that planning for the implementation of any automated tests needed to take into account likely difficulties such as obtaining data management approvals; data sourcing and aggregation lead times; the need for control domain expertise; technology acquisition and integration costs; and the need for information sharing and coordination among audit, risk and compliance functions (Vasarhelyi, Romero, & Kuenkaikaew, 2012). These were important considerations, tied to the degrees of innovation of technology, which influenced the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts. While existing studies had examined factors that may affect business values, the study results did not estimate improvements in compliance, or in efforts to prevent or detect fraud (Ajah & Inyiama, 2015; Bergeron & Raymond, 1997; Lombardi et al., 2014).

Risk and Fraud Detection

History. In a landmark study by Coderre (2005), referred to as the CARLAB study, face-to-face semi-structured interviews were completed with auditors of large public companies across varied industries, including twenty-two internal auditors. Key results noted by Coderre (2005) were that adoption of continuous auditing was still in initial stages, access needed to the data required for performing continuous auditing remained limited by companies, audit tasks were performed manually and periodically, current audit resources were inadequate, and the emerging technology remained confusing. Further provided were key findings regarding the implementation of new technology, and the perceptions of perceived ease of use and usefulness of continuous auditing tools, which could be further applicable to continuous control monitoring. One limitation, however, was that the study related to continuous auditing technology, and not continuous control monitoring. The focus of the study was related to auditors, and not corporate managers, or enterprise risk management efforts with an internal focus to prevent and detect fraud, and improve corporate risk management (Coderre, 2005). This indicates a gap in the literature review, with a lack of resources related to continuous control monitoring technology, and enterprise risk management. While some valuable overall knowledge has been gained regarding general implementation efforts, there remained a gap regarding specific knowledge related to the perceptions and experiences of corporate managers regarding the use of technical tools and processes for continuous control monitoring.

Another landmark case study was performed by Gutholc (2008) of the Memorial Healthcare System, which had been a leading healthcare provider for over 50 years, with six hospitals and multiple outpatient facilities including the flagship Memorial Regional Hospital, and the Joe DiMaggio Children's Hospital. Memorial Healthcare System implemented a

continuous auditing and monitoring in their Purchase-to-Payment cycle, in a project directed by the finance department (Gutholc, 2008). Over a period of just three months after installing continuous auditing, the team was on track meeting the projected return on investments and identified key areas for control enhancements, procedural improvements, and cost savings (Gutholc, 2008). Memorial Healthcare System consisted of a comprehensive array of health services and was one of the largest employers in Broward County, with more than 10,000 employees (Gutholc, 2008). The continuous control method implemented in the Memorial Healthcare Systems Purchase-to-Payment cycle was designed according to the Committee of Sponsoring Organizations framework (Gutholc, 2008). COSO framework was recognized as the internal control standards for supporting Sarbanes-Oxley Section 404 compliance (Gutholc, 2008). The Memorial Healthcare System was committed to achieving the highest standards of financial governance and management support (Gutholc, 2008). As such, the CFO and Director of Financial Controls began a search for auditing and monitoring solutions that helped to evaluate and strengthen critical business processes. Through the completion of the continuous control project, the team identified key areas for procedural and operational improvements by pinpointing more than a half-million dollars in potentially recoverable payments that had occurred over the past three years (Gutholc, 2008). Further, through continuous monitoring, there was increased visibility into higher risk areas of the business, early warnings to management, and real-time evaluation of all transactions (Gutholc, 2008). With the implementation of continuous control monitoring, Memorial Healthcare System enhanced procedures that boosted efficiency and eliminated third-party audit commissions while reducing costs (Gutholc, 2008). While this provided some key information for the area of continuous control monitoring, the focus remained on the quantitative technical side of continuous control

monitoring, rather than exploring the perceptions and experiences of financial managers regarding the use of technical tools for continuous controls monitoring (Gutholc, 2008). As business requirements were becoming stricter with financial reporting, additional future research has a need to fill this gap and provide further information to business executives that could enhance corporate business strategy.

A third landmark case study by Ajah and Inyiama (2011) related to information technology fraud detection resources, with the focus on methods for implementing information technology systems for control monitoring in banking systems in Nigeria. The case study examined the bank loan fraud detection and IT-based combat strategies, with a focus on analysis within the loan assessments system. Ajah and Inyiama (2011) identified a need for corporate banking managers to resolve a high occurrence of non-performing loans due to the lack of good decision-making tools for disbursing the loans, leading to bank failures. Two identified benefits of these systems for corporate management were improved profitability and lower default rates. Credit risk management (CRM) was the continuous control-monitoring tool studied. Through the study of the credit risk management tool in the banking system case study, there were performance increase methods for corporate finance managers (Ajah & Inyiama, 2011). However, this automated program was still not currently widely utilized, leaving mortgage companies exposed to potential fraud (Ajah & Inyiama, 2011). There was information on the research topic relative to CRM technology advances, and the potential for improved operational and fraud prevention methods for all organizations and corporate managers that grant credit to customers.

Current State. Gonzalez, Sharma, and Galleta (2012) indicated perceptions of investors' considered non-professionals related to perceived incremental values of assurance that either

continuous monitoring technology tool provided compared to traditional methods were examined. In the quantitative experiment of 120 participants, via a national survey company, the results showed that non-professional investors placed value upon continuous audit, and held beliefs that material errors and asset misappropriation were decreased through the use of the tools, however; they were unlikely to increase investment based upon the implementation of the tools due to the costs to the organization of implementing the resources (Gonzalez, et al., 2012). There were key findings regarding the impact of the costs relative to benefits for an organization in implementing continuous control monitoring resources. Furthermore, information was provided regarding the key differences between continuous auditing and control monitoring. However, the actual focus of perceived benefits related to continuous auditing rather than continuous monitoring and was from a financial controls and regulations point of view. There remained a gap and need for a focus on continuous control monitoring to examine benefits of efficiency in fraud prevention and enterprise risk management for corporate manager decision-making.

In relation to corporate fraud Soltani (2014) examined control issues relating to managerial choices. Case reviews were interpreted with the results of an evaluation of corporate fraud at six corporations. It was noted by Soltani (2014) that, for all the given companies' common issues included poor ethical climate and a lack of commitment to ethical principles. There were limitations that were noted in the study including understanding the inside story of the fraud cases, and a need to also explore the legal and regulatory perspectives, and different viewpoints (Soltani, 2014). In order for management to approach financial fraud and gain buy-in for enterprise risk management, there was a noted need to include a complete theoretical framework. Further, the cases noted in the study by Soltani (2014) included elements necessary

for supporting the research topic theoretical framework. Additionally, as noted by the qualitative interviews conducted by Gillespie, Dietz, and Lockey (2014), fraud violations and methods for financial management to handle enterprise risk management and recovery from financial fraud were identified. Through the main research question was an examination of how best to manage enterprise risk management, particularly after a loss of trust due to a fraud incident. These results indicated managers should implement best practices for preventing further instances of fraud, and these practices must include implementing new technology resources (Gillespie, et al., 2014). These studies support the need to understand impacts new technology resources including continuous control monitoring provide relative to benefits for financial management to consider in enterprise risk management, and fraud prevention efforts (Gillespie et al., 2014; Soltani, 2014). Additionally, Holtfreter and Harrington (2014), indicated the importance of implementing data protection tools in the prevention of cyber-crime perpetrated against corporations. Additionally, included was key seminal information related to the importance of securing the information technology systems to identify, monitor, and classify data breaches. Information also indicated the importance of data security for corporate executives, and the need to consider data security in relation to the implementation of information technology resources. Furthermore, if part of the solution to enterprise risk management includes continuous control monitoring resources that involve outsourcing partners were considered, data security and protection of the data is key (Holtfreter & Harrington, 2014). These resources support the need for a case study approach that explores continuous control monitoring which can provide valuable knowledge that minimizes existing literature gaps, identifying situations, and trends of corporate managers (Yin, 2014). Further, this supports the need for corporate managers to gain

understanding relative to how this technology transforms control monitoring, and risk management.

In relation to continuous control monitoring specifically, Lombardi, Vasarhelyi, and Verver (2014) indicated the important benefits from instances of error and fraud were significantly reduced, operational efficiencies were enhanced, and improvement to the bottom line is achieved through a combination of cost savings and reduction in overpayments and revenue leakage. Thus, continuous control monitoring has the potential to reduce the burden of regulatory compliance by automating internal controls testing. Further, another potential advantage of implementing continuous control monitoring tools is the independence of the control monitoring for enterprise risk management from the underlying operational and financial systems (Lombardi et al., 2014). There was an indication that the design of continuous control monitoring is the goal toward identification of specific transaction anomalies, and identification of breaches in controls, to provide corporate managers a method to protect the integrity of the business. Further, there was support related to continuous control monitoring technology providing corporate managers the detailed transaction information, to enable improved identification of fraud, error, and abuse. Additionally, support was noted by the case study of Elder, Janvrin, and Caster (2014) on corporate financial fraud and fraud prevention, related to Peregrine Financial Group and the embezzlement by the chief executive officer of $215 million in customer balances, hidden by preparing false bank statements and cash balance confirmations. Indicated was an examination of the use of a continuous control-monitoring tool, electronic confirmation of all customer accounts, to uncover fraud, which utilized data analysis that provided a mixed-method approach with cash and liquid assets is an open area to fraud without oversight. These results indicated the way the cash confirmation process flows needs evaluated,

and provided information related to the topic problem area of improved technological advances, verification of records, and need for continuous control monitoring over cash (Elder, et al., 2014). Further provided were key findings of support that continuous control monitoring adds value to financial managers' resources for improving fraud prevention and enterprise risk management. The regulator, in this case, the National Futures Association (NFA), demanded that Peregrine participate in an electronic confirmation process for verification of customer accounts. Additionally, this case supports the importance of auditing cash, and how new electronic confirmation technology improves the ability to authenticate confirmation responses (Elder, Janvrin, & Caster, 2014). As with other studies, there was a noted limitation of focus to the quantitative technical side of continuous control monitoring, rather than exploring the perceptions and experiences of financial managers regarding the implementation and use of technical tools for continuous controls monitoring (Elder et al., 2014). As business requirements were becoming stricter with financial reporting, additional future research had a need to fill this gap and provide further information to business executives that would enhance corporate business strategy.

Relative to occupational fraud Verschoor (2014) included information regarding small business losses in the United States due to corrupt employee actions. As noted by Verschoor (2014), the median loss overall for small business is $154,000 and correlates with how much responsibility the individual has. When executives were involved, it was noted, that the average loss rose to $500,000 per incident (Verschoor, 2014). This was key information regarding fraud losses and provided support for implementing continuous control monitoring as a method for corporate managers for preventing fraud events, and potential benefits for corporate managers in improving enterprise risk management. Additionally, the Association of Certified Fraud

Examiners (2016) conducted a recent study regarding worldwide occupational fraud. The methodology was a qualitative case study and included 2,410 cases. The results showed how prevalent fraud remained throughout the business and accounting world. The annual ACFE (2016) indicated that "more than 6.3 billion dollars are lost to fraud, with the average loss in the United States of $120,000" (p.1). This provided additional details regarding the costs of not identifying fraud and further indicated a need to improve enterprise risk management for corporate management, as financial statement fraud results in the highest fraud loss type.

The intended design of continuous control monitoring is to find transaction anomalies and to identify breaches in controls so corporate managers can protect the integrity of the business, and through these realize gains in the area of enterprise risk management. Continuous control monitoring technology provided granular and individual transaction detail information, which enables identification of fraud, error, and abuse (Hardy & Lazlett, 2015; Steinhoff, et al., 2016). Indicated was that while there were studies on individual topics relating to information technology and fraud, limited research exists considering fraud prevention needs and challenges of corporate managers relative to current technology advancements. The existing available studies regarding continuous control monitoring method have not fully examined perspectives of corporate managers regarding efficiency improvements, including a lack of information related to financial fraud detection and prevention efforts, and regulatory compliance (Deloitte, 2010; KPMG, 2008). Technology may provide a method of transformation beyond just those in work environments, and corporate managers within organizations have a need to understand continuous control monitoring technology implementation, including whether transformation efforts result in an ultimate overall gain, or instead produce more chaotic states of operation between managers and the key stakeholders.

Summary

Organizational leaders need to find novel approaches to continuous control monitoring in order to ensure the success of future implementations (Lombardi et al., 2014). Current identified methods fail to address how the quality of information, whether a continuous control monitoring system is in place or not, rest in the corporate culture and internal control structure of the business organization (ACFE, 2016; Gillespie, Dietz, & Lockey, 2014; Soltani, 2014). Gaps remained in research related to continuous control monitoring and information technology governance, which have potential to contribute to chaotic states for organizations (Hardy & Laslett, 2015; Lombardi et al., 2014). Various continuous control monitoring methods associated with the control monitoring methodology may be a confusing factor for corporate managers when considering adoption (Singh et al., 2014). The results of this research can provide benefits in shifting the focus of continuous control monitoring from financial controls and regulations, to improved efficiency in fraud prevention and enterprise risk management.

The research study began to fill the gap in the current research by performing a qualitative analysis regarding the perceptions and experiences of financial executives on a continuous control monitoring methodology. With the more robust regulatory requirements, business executives were searching for methods to ensure the financial reporting is accurate, and depicts a true financial picture of the organization, while improving overall enterprise risk management, including fraud prevention and detection methods (Steinhoff, Price, Comello, & Cocozza, 2016). The results of the research expanded the current body of information by providing recommendations and guidelines for improved enterprise risk management, and fraud prevention methods.

Chapter 3: Research Method

Management must make decisions based on timely and accurate financial information, in order to maintain competitive advantage and properly manage the risks of fraud (AICPA, 2012; ACFE, 2016; Steinhoff, Price, Comello, & Cocozza, 2016). Continuous control monitoring had an important role for managers to use as a means to achieve increased enterprise risk management, and to increase productivity and competitive advantage within the control monitoring functions (AICPA, 2012; ACFE, 2016; Steinhoff, et.al, 2016). Due to the daily changes in the business surroundings and regulatory requirements, a traditional control monitoring paradigm was outdated and was not suitable to provide real-time assurance for making business decisions, and managing risk related to fraud prevention and detection (AICPA, 2012; ACFE, 2016; Steinhoff, et.al, 2016). The purpose of this qualitative, multiple-case study was exploring the perceptions and experiences of financial executives regarding control monitoring approaches, both automated and continuous, which included system auditing processes, business impacts, and requirements. Thus, the research questions for the study were as follows:

Research question 1. What were the experiences of corporate managers concerning impediments to adoption for the implementation and use of continuous control monitoring procedures for maintaining corporate requirements concerning enterprise risk management and fraud prevention efforts?

Research question 2. What were the perceptions of executives regarding the introduction of new technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods?

Research data was collected using open-ended questions during personal interviews. Based on the data collection design, qualitative software from Qualitative Solutions and Research (QSR), NUD*IST Vivo 10 (NVivo10) was utilized, along with manual coding, for text/transcript coding, analysis, and theme identification from the interview data in this qualitative study. This chapter includes details regarding research methods and design, participants, instruments, data collection, processing, and analysis, methodological assumptions, limitations, and delimitations, and ethical assurances.

Research Methodology and Design

Qualitative research is defined as research that produces descriptive data derived from a given participant's written or spoken words as well as their observed behavior (Taylor, Bogdan, & DeVault, 2015). Qualitative research was most applicable as the study involved individual scenarios in which the thoughts and feelings of the participants were identified (Taylor et al., 2015). The qualitative method allowed participants to present experiences regarding implementation of continuous control monitoring resources and allowed for the discovery of fraud prevention components unique to the organization. Further, this method allowed the researcher to uncover information that might not have been extracted from the preliminary research for the study (Taylor et al., 2015). The qualitative research methodology has a number of designs. Some common qualitative approaches included phenomenology, grounded theory, historical, and case study (Punch, 2013).

Quantitative research is based on numerical data that is transformed into information that is statistical in nature (Goertz & Mahoney, 2012). Statistical and measurable data from quantitative research would have been used to quantify defined variables in an effort to form facts and patterns in research (Punch, 2013). The quantitative approach was not aligned with the

objective of this study because the purpose was to identify the perspectives of corporate managers and challenges to implementation of continuous control monitoring resources in improving enterprise risk management. Further, a quantitative approach would have required the development of a specific hypothesis by the researcher regarding the relevant components of impediments to implementation efforts. This method would have eliminated any opportunity to discover new components that might have arisen from the data collection, the results of which would not have been appropriate for the study because the relevant perspectives and reasons for corporate managers not implementing these resources were not identified for the organization. Furthermore, for the mixed-method approach, there would have been a combination of both the qualitative and quantitative (Goertz & Mahoney, 2012). The mixed method approach was inappropriate because the purpose of the study was to identify impediments to implementing continuous control monitoring resources for fraud prevention and enterprise risk management efforts, rather than quantifying them; therefore, any methodology involving quantitative analysis was not warranted.

Each qualitative design has a specific purpose, with research related to each focused towards the proper identification and appropriate application for each design (Lin, 2013). The phenomenology design focuses on the lived experiences of individuals in an effort to explore the subjective meanings of the data produced (Kafle, 2013). The phenomenology approach would be appropriate for gaining an understanding of the reasons for implementing continuous control monitoring in an organization; however, the design would not have yielded adequate data for identifying issues related to fraud prevention (Lin, 2013). Another common qualitative design was grounded theory (Lin, 2013), that would have utilized the data to produce a theory (Leavy & Bryant, 2014). Through this approach, problems would have been discovered that existed in the

social environment or society while explaining how the phenomenon was handled (Punch, 2013). This design would not be appropriate for this study because the phenomenon of a need for fraud prevention in financial reporting has already been established as the problem; therefore, it did not need to be discovered (Leavy & Bryant, 2014). Furthermore, identifying the reasons for a lack of implementation of continuous control monitoring technology tools to improve enterprise risk management was an existing problem within an organization; therefore, developing theory would not have been warranted due to the practical nature of the study (Leavy & Bryant, 2014). Ethnography was another type of qualitative research, defined as an in-depth study of a culture or group, and was a qualitative approach that has many similarities to the case study (Clerke & Hopwood, 2014). However, while both designs were in-depth studies of an individual or group, the process of gathering data distinguished the two from one another (Clerke & Hopwood, 2014). Case studies utilized direct observation to gather data about the subject, creating an outward perspective, while ethnography involved gaining entrance into the culture as a direct participant (Clerke & Hopwood, 2014). That perspective of an internal approach in ethnography made the approach unsuitable for this research study. Therefore, case study design provided an in-depth study of an individual, group, community, or institution that acquires exploratory and descriptive information to investigate a problem in a true-life context (Yin, 2013). As case studies focused from substantial previous research that allowed the researcher to draw conclusions based on the interactions throughout the study, the exploratory and descriptive nature of the approach made it the most appropriate design for the study. Case study researchers were interested in the reason behind a phenomenon (Yin, 2013).

Gaining an understanding of the details for implementing continuous controls monitoring techniques by corporate managers lent itself to the case study approach to generate specific

information. As the study involved observational methods, extensively utilized in business, law, and policy analysis, the case study method of research provided the methodology to gain an understanding of change processes, as they were unfolding (Yin, 2014). The case study required exploring the perceptions of corporate managers, with the specific focus and a description of the process understood as a specific instance of the studied phenomenon affecting the research, and for the research, as continuous control monitoring methods (Yin, 2014). The research was a qualitative, multiple case study because this approach enabled an in-depth exploration of the views, perspectives, and opinions of experienced managers and executives with respect to continuous control monitoring methods. Compared to a single case study, multiple case study allowed for an exploration of the continuous control monitoring process at multiple embedded levels. Additionally, contrasting and comparing across different organizations, with different business types, management styles, and organizational goals allowed the findings of the study to have wider relevance (Yazan, 2015). This approach provided the inherent ability to gather multiple sources of evidence from qualified participants, offering convergent perspectives for the same phenomenon (Yazan, 2015). Furthermore, the use of multiple case studies provided a broader range of data, that is optional for the study as it allowed for increased accuracy due to a basis upon different sources of data (Yin, 2014).

Thus, a qualitative multiple-case study approach was supported as the appropriate method and will allow for contrasting and comparing across different organizations, with different business types, management styles, and allowed the findings to have wider relevance (Yin, 2014). By conducting multiple-case studies, there was an opportunity for comparisons available both within and between these diverse organizations. Equally important, unlike other methods, the multiple-case study provided information that demonstrated replication, and a common

conclusion from more than one case, which allowed for the possibility for external generalizability of the findings (Yazan, 2015).

Other research designs were considered, yet not chosen as the appropriate design for this study. An ethnography design would have a focus on an entire group with shared common interest and explore the culture over an extended period of several months or several years, a period longer than the research study period, with a focus on culture rather than perceptions of corporate managers (Zenker & Kumoll, 2010). The phenomenological study design would have explored the meaning of the event while requiring the researcher to be immersed in the study settings (Kafle, 2013; Yin, 2014). Further, in phenomenological research, a researcher would have been involved in direct observation of the participants in gathering research data for translation (Kafle,2013). Another theory considered for this qualitative business research was grounded theory (Wu & Beaunae, 2014). Grounded theory was noted as a tool to increase the credibility of the business study and further offers opportunities of producing generalized data results, which drives the creation of innovative theory, however, had noted challenges in the area of coding (Wu & Beaunae, 2014). Additionally, grounded theory was not without controversy as the root of grounded theory contradicts the point of view of Leavy and Bryant (2014), the grounded theory would involve research without a stated problem, and there is added criticism of the long period involved in the completion of grounded theory research. Therefore, a reason for the selection of qualitative case study methodology over other methods was that it allowed for flexibility, greater spontaneity, and an opportunity to probe further during the interview process (Chenail, 2011). With this qualitative design, the researcher was able to seek answers to the research questions and the corporate managers' self-perceptions with respect to continuous

control monitoring. Thus, this approach allowed findings that focused on the themes that emerged from the discussions.

A case study design provided for more effective qualitative design as a method of inquiry used to investigate the phenomenon involving the group of corporate managers, to examine the boundaries of the phenomenon of implementing continuous control monitoring that was not clearly defined. Further, a case study design allowed for examination of an understanding of this complex issue, in order to extend knowledge from existing research. Data to be collected through interviews assisted in understanding business impacts and regulatory compliance across multiple environments. Additionally, a multiple-case design allowed for increases in the probability of implementing a case study over a single-case design because single-case designs were vulnerable if the entire study relies on a single case (Yin, 2014). More importantly, using two or more cases can be substantial because it demonstrated replication and common conclusions from more than one case and expand the external generalizability of the findings (Yin, 2014). To ensure the research covers barriers and issues of implementation, an identified set of questions was used to instrument the interviews with each participant.

A case study must include a specific focus and a description of an event, person or process understood as a specific instance of the studied phenomenon affecting the research, which for the study were continuous auditing methods (Creswell, 2014; Holloway & Wheeler, 2013; Yin, 2014). The case study involved exploring the perceptions and experiences of control monitoring processes and methods (Yin, 2014). One of the most important sources of the case study data was the interview; therefore, interviews were conducted throughout this research to gain knowledge and information on business decisions and financial reporting that have been triumphant or ineffective with implementing a continuous control monitoring methodology (Yin,

2014). Qualitative multiple-case research methods usually rely on fieldwork that often requires researchers to spend time at the particular sites being studied (Yin, 2014). The case study field worker should have a firm grasp on the issues being studied to reduce the information to be sought to manageable proportions (Creswell, 2014; Holloway & Wheeler, 2013; Yin, 2014). Knowledge regarding continuous control monitoring and financial reporting was important to ensure a firm grasp of the control monitoring concepts and discussions. Despite the knowledge, the researcher was vigilant in order to remain unbiased by preconceived personal viewpoints (Yin, 2014).

Population

The population from which participants were drawn was the group of compliance and risk managers at major US corporations, who were part of the Fortune 500 listing. The sample for the study consisted of two participants from each of the ten major organizations for a minimum of 20 participants. Identification of the participants in the research was through the use of a current Fortune 500 listing of large accelerated filers in the United States consisting of a compliance, and enterprise risk management department. Identifying the companies in this manner ensured appropriate selection of participants (Yazan, 2015). Participant interviews provided information regarding the knowledge and experience of continuous control monitoring processes and approaches taken within their organizations for financial reporting and regulatory compliance. Corporate managers were appropriate participants with whom to explore to the research problem because they have insight on the implementation of continuous control monitoring resources from various perspectives (Yazan, 2015). As such, a sample from this population was able to provide detailed and illuminating descriptions regarding the efforts and

initiatives designed to improve the enterprise risk management resources and experiences among corporate managers, and the impact with respect to fraud prevention outcomes (Yazan, 2015).

Sample

The representative unit of analysis for each case for the given research was the organization, consisting of a purposeful sample from a listing of publicly traded companies deemed accelerated filers in the United States, as selected from the Fortune 500 listing (Yazan, 2015). Collection methods included interviews, and methods for coding and analysis were applicable to the design based on the primary qualitative research methods, and design (Yazan, 2015). For the given research, the methodological framework was the multiple-case study, open-ended questions, and interviews were used to explore financial reporting and regulatory compliance (Yin, 2014). Further, explored in depth within this qualitative study, was an event, process, program, related to one or more individuals. The participants for this research were identified using a current Fortune 500 listing of eastern United States companies. These participants were interviewed to gain knowledge and experience of continuous control monitoring processes and approaches within their organizations for financial reporting, regulatory compliance, and enterprise risk management.

Unlike the predetermined instrument-based questions or observations used in quantitative research methods, this qualitative research included emerging methods and open-ended questions. The qualitative research interviews described meanings of central themes in the organization of participants, using open-ended questions to cover both factual and the significance level of understanding, which provided useful information for getting the story behind the participant's experiences (Yazan, 2015). The interviewer through the research

questions pursued in-depth information, which also required follow-up interviews for further investigation of responses (Yazan, 2015).

Materials and Instrumentation

Within the methodological framework of the multiple-case study, open-ended questions and interviews were used to explore regulatory compliance, enterprise risk management, and fraud prevention efforts. The qualitative research interviews described the meanings of central themes in the organization of the participants. These qualitative research interviews utilized open-ended questions with the purpose to seek to cover both a factual and a significance level of understanding, particularly useful for getting the story behind the given participant's experiences (Yin, 2014). The interviewer then pursued in-depth information around the research questions that may have to require follow-up interviews to further investigate their responses. In this study, research interviews took place by telephone, or through the use of the internet, via Skype. Interviews conducted in person via Skype were the primary approach for collecting data, however; telephone interviews were utilized as needed for follow-up questions, or when not possible to conduct an in-person interview. A case study should use multiple sources of evidence to achieve data triangulation (Wimmer & Dominick, 2013; Yin, 2014). By doing so, the findings or conclusions of the study were more likely to be accurate because multiple sources of information were used (Yin, 2014). Therefore, to answer the research questions for this study, two data collection instruments were used. First, an interview instrument was developed and used for an initial data gathering from each participant. The questions were open-ended, unstructured with the thought that it would be necessary to interview the participants a second time to build upon or explore the responses to the initial questions (Yin, 2014). The participants' response to the initial questions in the interviews were utilized as building blocks grouped into

patterns. In the study, follow-up interview questions were then used as needed to corroborate the information gathered during the initial interviews (Yin, 2014). The questions were established for the follow-up interviews after receiving and reviewing the initial responses from the participants. Each participant was given an explanation of the study and informed consent was obtained before starting the research. The informed consent form indicated participants have read and understood the details of the study**.** Furthermore, a statement about the maintenance of privacy, confidentiality, and the right to decline participation was included on the consent form and discussed with each participant prior to starting the interviews. Two copies of the consent form were be presented for signature with one copy provided to the participant and the remaining signed copy placed in safe storage. The method of utilizing the informed consent form instrument promoted trust that built the foundation of the interview process.

Study Procedures

The research case study utilized multiple sources of evidence to achieve data triangulation (Yazan, 2015). The findings or conclusions of the study thus achieved a higher level of accuracy by following this method of pursuing multiple sources and using two data collection instruments to answer the research questions for the study. Due to the nature of open-ended questions, it proved necessary to interview the participants a second time to build upon and explore the responses to the initial questions (Yazan, 2015). Participants' initial responses provided building blocks, which were then grouped into patterns, for identifying meaning through similar or different patterns and commonalities; a common technique that is preferred in case study analysis (Yazan, 2015). Based on the data collection design, qualitative software from Qualitative Solutions and Research (QSR), NUD*IST Vivo 10 (NVivo10) was used for coding, analysis, and theme identification from the interview data in this qualitative study.

Data Collection and Analysis

Data collection procedures for the qualitative research included interviews, with the potential participants contacted by telephone or email invitation for participation in the study. Participants were assigned a unique number, to identify the participants while maintaining records of anonymity and privacy (Yin, 2014). Initial interview data were transcribed and coded. During the collection of interview data, the process of identifying and differentiating themes that address the research question via identification of similar and dissimilar concept patterns and commonalities were identified and grouped in the interview transcripts (Yazan, 2015). Following initial data collection, the coding process began with initial coding or open coding, as a starting point that included a review of the data collected for patterns and themes, through pattern matching, which is an identified desirable technique for case study analysis (Holloway & Wheeler, 2013). By isolating these patterns, further analysis was able to be completed, through creating subsets from each pattern and reviewing in an effort to uncover patterns that were not immediately apparent during the collection process (Yazan, 2015). The qualitative data gathered was then further broken down into discrete parts, and comparisons for similarities and differences made. Upon completion of establishing all patterns and themes, the interview notes were transcribed via the necessary data analysis, utilizing the NVivo11 software to analyze the data through coding, query, theoretical sampling, and theory testing (Yazan, 2015). The design of NVivo software supported the researcher in performing qualitative research, along with the associated data analysis completed in the research effort (Yazan, 2015). Using the NVivo software allowed the data collected to be reviewed for patterns or themes and facilitate pattern matching, as this is one of the most desirable techniques for case study analysis (Holloway & Wheeler, 2013; Yin, 2014). Additionally, after

the patterns were isolated, further analysis was conducted using NVivo by creating subsets from each pattern. These results using NVivo were reviewed in an effort to uncover patterns that were not immediately apparent during the collection process (Yin, 2014). This process of looking for patterns and themes was utilized to ensure that the inconsistencies in the findings were not dismissed which could indicate barriers or concerns (Yin 2014). This facilitated the ability to sort the resulting pattern codes into both meaningful as well as parsimonious units for analysis, for use in the development of statements that described major themes, patterns, and interrelations from the data (Taylor, Bogdan, & DeVault, 2015). Once all the patterns and themes were established, they were presented and explained by reviewing the literature.

Analytic memo writing. A further method utilized in the coding of transcripts in the research effort was analytic memo writing; this method contributed to the quality of analysis by providing a rigorous reflection of the data gathered (Yin, 2014). The analytic memos allowed for linkages of the multiple case study data together into recognizable clusters that showed the data as instances of general concepts (Yin, 2014). Additionally, analytic memo writing provided an additional coding and category generating method. These pattern codes provided the necessary stimulus to develop statements that describe the major themes, patterns, and interrelationships from the data (Yazaz, 2015; Yin, 2014).

Triangulation. This qualitative study addressed concerns of two approaches for accuracy and credibility using triangulation (Yin, 2014). The first method was that of triangulation, a method accomplished in several ways. Triangulation according to Yin (2014) utilized two or more methods of data collection and was a technique to increase the validity and reliability of the data collection and interpretation of the data. The triangulation procedure involved comparing data from different informants, referred to as informant triangulation (Yin,

2014). Creswell (2014) referred to this form of triangulation of Synchronic Primary Data Source triangulation. A second approach included confirmation of the accuracy of the findings with clarification of the bias that the researcher brought to the study. Yin (2014) stated that a researcher should have a firm grasp of the issues being studied. However, while this firm grasp of the issues studied provided an advantage, there was potential for disadvantages of preconceived viewpoints, which could have led to the potential introduction of bias. In the study, the researcher reduced the risk of the introduction of bias through the development of an accurate and convincing case narrative. Research studies have assumptions, limitations, and delimitations from the start of planning through the completion of the research.

As this research study was qualitative in nature, there was a need to mitigate issues related to research integrity or quality (Lincoln & Guba, 1985; Trochim & Donnelly, 2008). There were four criteria that were considered in an assessment of the overall trustworthiness of qualitative research in relation to an alternative to criteria associated with conducting quantitative research. These alternative criteria included credibility, transferability, dependability, and confirmability.

Credibility. Credibility included properly ensuring that research results were believable or trustworthy from the research participants' perspectives (Trochim & Donnelly, 2008). Within the context of quantitative research, credibility was synonymous with internal validity. In this study, member checking was utilized to enhance credibility throughout the study. Following completion of the in-depth interviews and follow-up interviews, provided to each participant was the opportunity to review and modify his or her in-depth interview transcript and follow-up interview transcript to ensure response accuracy (Baškarada, 2014).

Transferability. Transferability represented the concept of applicability of the results to other contexts, or situations (Trochim & Donnelly, 2008). From a qualitative perspective, the responsibility of transferability was with the individual doing the transferring or generalizing the results of the study data (Trochim & Donnelly, 2008). Transferability for the study was enhanced by recruiting a sample of 2 individuals selected from each organization with positions as corporate managers who were experts in financial and control monitoring processes, and who had experience in financial risk or fraud risk and 1 manager from the financial fraud prevention or equivalent office in each of these organizations (Baškarada, 2014). Additionally, the diversity of the multiple cases increased the transferability or applicability of findings (Baškarada, 2014).

Dependability. Dependability referred to the given study's consistency and replicability (Baškarada, 2014; Trochim & Donnelly, 2008). In order to establish dependability for the study, the research process was clearly and explicitly described and documented. Dependability for the study was demonstrated by maintaining an audit trail in the form of a research journal to provide a detailed account of how the data is collected, analyzed, and interpreted (Lincoln & Guba, 1985; Trochim & Donnelly, 2008).

Confirmability. Confirmability referred to the degree to which other researchers were able to corroborate or confirm the findings of the study (Trochim & Donnelly, 2008). One method for establishing a systematic means of documenting credibility with the data collection, and identifying any inaccuracy with data for the study was through an audit of the data throughout the study (Trochim & Donnelly, 2008). Several noted categories for reporting this information included the raw data, data analysis, development, and synthesis of the data including procedure notes and summaries (Lincoln & Guba, 1985). For the study, a research

journal was provided that detailed the audit trail for the data collection, analysis, and interpretation phases completed (Trochim & Donnelly, 2008).

Assumptions

This study included the following assorted assumptions about participants:

- a company was a fortune 500 company with more than 100 employees,
- the organization structure included a compliance and/or enterprise risk management department,
- a CFO, CEO, or functional manager with knowledge of financial processes and compliance,
- moreover, understood that all data shared is kept confidential.

The primary assumption for this study was the categorization of participants associated with a given organization by their given role of compliance or enterprise risk management had the necessary experience or knowledge on a variety of control and compliance methodologies and provided information relevant to gaining answers for the research questions. Their experiences with control monitoring techniques, tools, and software, plus the inherent challenges with technology ensured a complete study was performed. This assumption applies to all participants interviewed.

Another assumption was that the participant's responses were truthful and correct. For an accurate understanding of the underlying concerns of adopting a continuous control monitoring approach, knowledge responses were necessary (Yazan, 2015). By identifying participants that were in the compliance and control community or those practicing the different control monitoring methodologies, this allowed empirical research data to be gathered. Further, through providing the knowledgeable responses, participants within these

professional risk management areas of organizations, information assumed to result in the study was beneficial for executive management to make better strategic business decisions (Yin, 2014). Participants thus were more likely to provide information for the study effort. These assumptions assisted in the identification of organizations that have an interest in the risk management process and shall be essential to the research efforts.

Limitations

One potential limitation of the continuous control monitoring research included other methods of complying with governance requirements, fraud detection and prevention methods. There was a need to address the issue regarding improving accuracy and credibility when performing the qualitative case study. For the given research study, it was important to address these issues using triangulation (Yazan, 2015). The research efforts utilized multiple methods of data collection and interpretation, via performance of the interviews of various corporate managers on the same topic to provide the necessary source triangulation (Creswell, 2014; Yazan, 2015).

Another potential limitation in the use of case study design for the study included the researcher's inexperience and the potential bias of the researcher. To mitigate the researcher's inexperience in conducting the study, a rigorous approach was followed (Yin, 2014). A lack of rigor with data handling and reporting could have resulted in negligence in research design or application or improper data manipulation (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Sciences, 1979). To mitigate the risk of negligence, the research followed established protocols for case study design and application developed by leading authors in the field of case study research. For example, a chain of evidence was maintained in the working papers of the study that provided an audit trail that can be followed to

reproduce the study (Yin, 2014). In addition, an in-depth literature review was completed and updated through completion of the project. Finally, research questions were based on the literature review and context of the study (Yin, 2014).

Delimitations

There was the collection of discussion of responses from organizations that utilized operational models for control monitoring and fraud prevention out of the scope of this research, which shall not be included in the final research report (Yazan, 2015). With the variety of control methodologies and regulatory mandates that organizations are required to adhere to the collection of data for every methodology and mandate was unrealistic. Thus, the primary focus of the research was on continuous control methodology. The main delimitation of this study was the inclusion of organizations that have proper experience with a continuous control monitoring methodology.

Since the Fortune 500 list changes continuously, after the approval of this case study was granted, a review was completed for the organizations identified for the study. The organizations identified for the study had more than 100 employees and a compliance or internal audit department. This review ensured the right participants were adequately selected for the study (Yin, 2014).

To increase the reliability of the study data gathered, a chain of evidence was maintained. This chain of evidence principle allowed an external person the derivation of any data from the study research questions to the conclusion (Yin, 2014). In addition, the validity of the research was of importance when providing the results. Observing and matching the patterns gathered from the study participants provided one method for addressing the internal validity of the research (Yin, 2014).

Ethical Assurances

Before the beginning of any data collection for the study, NCU's Internal Review Board granted approval (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Sciences, 1979). An Informed Consent Form was provided to participants that outlined the participation as voluntary and indicated no gained benefits were received for participating (Yin, 2014). Informed consent was an important human right principle (Rodhouse & Vanclay, 2016). Thus, informed consent approval was obtained prior to interviews, participants had the ability to leave the interview at any point, and all participants received a copy of the interview transcript. This ensured that participants were appropriately informed and that there was a full understanding of what will be involved with participation (Rodhouse & Vanclay, 2016). The researcher had the responsibility of protecting participants and demonstrating the ability to conduct research with ethical assurances in place. Multi-case study research required consideration of confidentiality, environment, and appropriate compliance with standards that correlate with the type of research design chosen (Yin, 2014).

All interview data and survey responses were handled with confidentiality and consistent with the Privacy Act of 1974 (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Sciences, 1979). The research data was stored on a computer within a password-protected file and only the researcher had access to the raw data. The research results were available upon request to any of the participants and provided in the format of an executive summary. The research results did not provide any correlation between the responses and participant or organization that participates in the study.

To address any potential concerns with a preconceived notion and prejudice applied to the research, it was imperative to reduce bias to every extent (Yin, 2014). Any positive or

negative personal comments were avoided that could influence the data gathered. The researcher was a member of professional accounting organizations and a corporate accounting team member that must adhere to the professional rules of ethics and business conduct.

Summary

The problem was that operational models utilized for continuous control monitoring implementations, which include processes, controls, and best practices, were not consistent, resulting in the diminished quality of corporate financial reporting, and an increased risk to organizations (AICPA, 2012). Continuous control monitoring has an important role to play within the business as a means to achieve increased operational efficiency, but also to increase productivity and competitive advantage within the accounting functions, including improvements in fraud prevention and risk management (Masli, Peters, Richardson, & Sanchez, 2010). The qualitative, multiple-case study explored the experiences and perceptions regarding the introduction of technical tools for continuous control monitoring processes.

The planned sample consisted of two participants from each of ten major organizations who had proper experience with a selection of technology for continuous control monitoring processes. Participants were knowledgeable in financial processes, technology, and had experience implementing continuous control monitoring solutions for enterprise risk management, or fraud prevention. The research involved open-ended interviews to explore continuous control monitoring processes, enterprise risk management, and regulatory compliance for each organization regarding the implementation and effectiveness of continuous control monitoring methods (Yin, 2014). Each participant was informed of the details of the study, the maintenance of privacy, confidentiality, and the right to decline participation prior to starting the interviews. Case-study methodology protocol and ethical assurances based on

Northcentral University Institutional Review Board protocols were followed. All interview data and survey responses were handled with confidentiality.

Chapter 4: Findings

The fourth chapter of the study contains the findings from the thematic analysis of the interviews with the 18 participants. The purpose of this qualitative, multiple-case study was to identify and explore the perceptions and experiences of corporate managers' regarding the use of new technology-related tools, which include control monitoring processes, business impacts, and requirements. Researchers suggested that managers encounter impediments to adoption, implementation, and use of continuous control monitoring procedures for fraud prevention controls to manage organizational risk in maintaining corporate requirements (Hardy & Laslett, 2015; Salvioni & Astori, 2014; Singh et al., 2014). The performance of a qualitative thematic analysis allowed the researcher to analyze the interviews. The method of analysis allowed the researcher to discover the most significant perceptions and experiences shared by the interviewed participants. NVivo11 by QSR further provided an aid in the systematic coding and tabulation of the data from the interviews. The data supported prior research beliefs that corporate managers encountered problems with continuous controls implementation that affect their collective ability to deal with enterprise risk management and fraud prevention (Hardy & Laslett, 2015; Salvioni & Astori, 2014; Singh et al., 2014).

The data collected was a descriptive, multi-case research design. Multi-case study design allows for research examining subtleties in an environment (Yin, 2014). The population of interest in this study consisted of business managers who have knowledge of corporate accounting or information technology governance processes relating to businesses. Therefore, the intent of the study was to obtain an understanding of the approaches, technology, and the indecision to adopt new continuous control monitoring methodologies. The Creswell (2014) structured and semi-structured participant interview format determined to be the most suitable

method for gathering research data and utilized for this study. Prior to use, a panel reviewed an interview guide for non- bias open-ended questions that ensured the interviews had a design to address the research questions, the purpose of the study, and extract responses from participants that addressed the goals of the study. The investigation occurred through 18 Skype or phone interviews with eligible voluntary participants, collecting primary data. As recommended by Yin (2014), using cross-case synthesis for the data analysis made it possible to verify whether the results of the case study were comparable (Yin, 2014). The decision to limit the number of participants to eighteen allowed the researcher to conduct comprehensive, in-depth interviews while still achieving thematic saturation. To ensure the credibility of the researcher's observations, the triangulation of the data was conducted (Yin, 2014). Data collection included and involved the collection of the participant responses during interviews captured through transcribed note taking. Participant interviews were recorded, transcribed, and NVivo11 software along with manual coding was utilized for data collection and analysis.

The practical management imperative addressed within the study was the need for improving understanding and knowledge regarding technology utilized for continuous control monitoring (Yin, 2014). In addition, the management decision related to enhancing business processes to achieve increased enterprise risk management, but also to increase competitive advantage within enterprise risk management (Deloitte, 2010). With this business decision in mind, along with the literature review, two main research questions addressed in this study were:

> **Research question 1.** What were the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts?

Research question 2. What were the perceptions of managers regarding the introduction of new technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods?

Participants were 18 corporate managers from Fortune 500 companies located within the Eastern United States. The participants recruited for the study had firsthand experiences on the nature of internal control and fraud prevention. There were experiences of the managers expected to be applied and shared completely during the interviews. The main interview questions focused towards exploring the experiences and circumstances encountered during the implementation of a continuous control monitoring methodology, and the overall manager's perception and expectations regarding new technology usage outcomes. The focus was towards broad questions that were refined to open discussion and allowed for the exploration of continuous control monitoring methodology. The formulation of additional interview sub-questions addressed internal and external factors related to continuous control monitoring approaches and related business approach expectations towards adopting new technology. Further, these interview questions allowed for the collection of data and the search for emergent themes within different industries. Data collected from the 12 participants were analyzed using a qualitative thematic analysis. As Braun and Clarke (2006) described, thematic analysis is a data analysis method in which the researcher works to "identify, analyze, and report patterns" (p. 79) found in the data. In this case, all 18 interview transcripts of the participants were carefully reviewed and analyzed to search for and determine the most common patterns in the participants' responses. Furthermore, there were patterns analyzed to create concepts strictly based on the words or perceptions of the participants, and the concepts with the same meanings were labeled, and grouped accordingly. With the help of NVivo11 by QSR, responses of the participants were

coded and the themes were tabulated efficiently. It must be noted that the themes that received the most number of references were considered as the major themes of the study.

This chapter includes the results of the research, an evaluation of the results, and a summary of the chapter. Included in the results are a sample of demographics of participants, followed by a discussion of the data collected and results. Further included is an evaluation of the conclusions, presented with respect to the research questions.

Trustworthiness of the Data

The study's trustworthiness was ensured through the four qualitative standards as proposed by Lincoln and Guba (1985). The first criterion was the credibility of the results. The researcher attained credibility by collecting the responses of the corporate managers across varying industries at the corporations, and by including some audit executives as participants. Their firsthand perceptions and experiences provided the much-needed details on the subject under investigation. Furthermore, member-checking also was performed to guarantee that the truthfulness of the recorded data and responses of the participants. The researcher accounted for all data gathering processes, coding, and analysis to completely describe the research context of the study. Transferability should then allow future researchers to employ the data with a similar subject to another setting and context. The third qualitative standard achieved was the dependability of the study. During the interviews, the researcher warranted that the participants were comfortable and were not experiencing any issues during the time of the interviews. This was to ensure that their answers were not affected or influenced by any external factors or influences. Further, during the data collections, the companies and all of the participants had an assigned generic identifier to ensure privacy and confidentiality (Rodhouse & Vanclay, 2016). Finally, confirmability was attained by producing an audit-trail that would be helpful in

examining data collection and analysis for any probable bias. The transcribed interview data results were analyzed through NVivo software to the group, categorize, and analyze the data. This software tool assisted in identifying themes present in which were in line with the research questions (Taylor, Bogdan, & DeVault, 2015).

Sample demographics and code selection. Each company chosen for the study had more than 100 employees and a corporate accounting department. There were originally 20 participants identified for the study that consisted of two members from each selected company. The participants were corporate managers who had knowledge of financial processes, technology and had experience implementing continuous control monitoring solutions for enterprise risk management, or fraud prevention. Due to scheduling conflicts and time constraints, 18 out of the 20 participants completed interviews. These participants were from different function levels to offer well-rounded responses for each organization (Yazan, 2015). The sample participant demographics are presented in Table 1.

Table 1
Sample Participation Demographics

Function	# Participants	Percentage
Accounting Manager	4	22.22%
Audit Lead	6	33.33%
Executive Manager, Director, CFO	8	44.45%
Overall	**18**	**100%**

Further, the participating companies varied in size and industries. Table 2 contains the sample demographics for the companies grouped by size and Table 3 contains the companies grouped by industry.

Table 2
Sample Company Size Demographics

Company Size	# Participants	Percentage
100-499	2	11.11%
500-1000	2	11.11%
1001-5000	8	44.45%
Over 5000	6	33.33%
Overall	**18**	**100%**

Table 3
Sample Company Industry Demographics

Company Industry	# Participants	Percentage
Healthcare	4	22.22%
Financial/Banking	4	22.22%
Industry	6	33.33%
Energy	4	22.22%
Overall	**18**	**100%**

The codes and subsequent strings were run throughout all participant interview notes, with each participant note marked to indicate where responses presented additional meaning or context (Taylor, Bogdan, & DeVault, 2015). Further analysis completed of the data gathered identified recurring themes. These themes allowed for the creation of codes in NVivo software. Examples of themes detected included: (a) lack of resources and resource management, (b) availability of data, (c) knowledge of technology, (d) budget/cost, and (e) environment.

Results

Research question 1. What were the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts? The first interview research question design focus

provided understanding regarding the experiences encountered through continuous control monitoring with financial audits, reporting, and regulatory compliance. The interview research question sub-questions were: (1) internal factors that motivate managers to employ continuous control monitoring capabilities, (2) external factors that motivate managers to employ continuous control monitoring capabilities, (3) internal factors that cause managers reluctance to employ continuous control monitoring capabilities, (4) external factors that cause managers reluctance to employ continuous control monitoring capabilities (5) are industry leaders reluctant to implement continuous control monitoring, (6) to what extent do managers rely upon evidence from continuous control monitoring resources for risk management and fraud prevention. The responses to these six questions aligned with research question 1. Responses to each sub-question provided data that answered research question 1 and showed that the experiences and perceptions of the corporate managers regarding continuous control monitoring, and motivations and barriers to implementation of the resources based upon perceptions including ease of use and perceived value. The sub-questions helped to drill down on the internal and external factors that motivated or caused reluctance to employ continuous control monitoring capabilities within the organizations.

Major Themes 1 and 4. Lack of resources and resource management associated with continuous control monitoring remains the key internal factor for reluctance to implement by managersand associated overall cost and budget. From the thematic analysis of the interviews discovered was that a lack of resources and management of resources were the greatest characteristics present, as the managers' perceived high set-up and implementation costs for continuous control monitoring as a barrier for the adoption of the technologies. Twelve of the 18 participants shared this perception or experience, in response to the factor within the organization

that causes reluctance to implement. Further indicated by six of the 18 managers was that executive management has continued to focus funds towards other information technology areas, resulting in the lack of support and availability of resources for the continuous monitoring implementations. Further, in regard to cost and budget, 10 of the 18 managers indicated internal reluctance factors of upfront expenses, time to establish new processes, resource management, and training, which is supported by the literature review (Hardy & Laslett, 2015; Salvioni, & Astori, 2014; Singh et al., 2014).

An initial perception was that continuous control monitoring was an expensive and risky endeavor, and requires significant investment and access to data; the participants identified management support as one of the top four themes during the interviews conducted (Taylor, Bogdan, & DeVault, 2015). As noted by responses from all 18 managers, the involvement of management in the adoption of continuous control monitoring is a fundamental internal factor within the organization that motivates the employment, and consideration for employment of continuous control monitoring. If management does not perceive continuous control monitoring as useful, stakeholders are not willing to risk investing in the technology or supporting any efforts made to the change in current processes (Lombardi et al., 2014; Singh et al., 2014).

Major Themes 2 and 3 Training and knowledge of technology. The majority of managers, 10 out of the 18 participants indicated that continuous control monitoring methodology requires high levels of investment in technology and training. Participant 3 indicated, "a lack of staff skilled in emerging technology contributes to the company reluctance to consider these resources." This factor has hindered some companies' adoption of continuous control monitoring. Additionally, indicated by 12 out of 18 participants, was that establishing automated monitoring required extensive training to lessen the learning curve, which is

expensive, and time-consuming, which is in line with the existing literature review (AICPA, 2012; Deloitte, 2010; ISACA, 2014; Malescu & Sutton, 2015).

Major theme 5 Environment. External factors that influenced or caused reluctance to the adoption of a continuous control monitoring approach were the demands levied on the organizations for compliance, supported by the study results and the literature review (AICPA, 2012; ISACA, 2014; Malescu & Sutton, 2015). Organizations were increasingly calling on accounting to improve performance by identifying areas of both operational inefficiencies and instances of fraud (AICPA, 2012; ISACA, 2014; Malescu & Sutton, 2015). Interviewed participants indicated that continuous control monitoring requires a paradigm shift from traditional control monitoring (Lombardi et al., 2014; Singh et al., 2014). Due to the legal requirements, some companies follow more than one mandate, therefore the question allowed more than one response. The results showed 20% must comply with HIPPA, 46.67% with SOX, and 26.66% with other laws such as GAO.

Table 5
Sample Mandates

Mandates	# Participants	Percentage
HIPAA	6	20.00%
SOX	14	46.67%
FFIEC	2	6.67%
Other (GAO, FDIC, SOA)	8	26.66%
Overall	**30**	**100%**

Participant 6 noted, "the regulatory environment continues to expand for us particularly in the area of healthcare and employment data requirements, so risk management is more today than just financial results, and fraud risk expands in those areas as they emerge." The companies chosen had various control monitoring methodologies in place as noted in Table 4 below. Eight

of the 18 participants indicated that management relies upon continuous control monitoring evidence for risk management and fraud prevention, on some level.

Table 4
Sample Audit Methodology Demographics

Audit Methodology	# Participants	Percentage
Risk-based	10	55.55%
Continuous	8	44.45%
Cyclical	0	0%
Other	0	0%
Overall	**18**	**100%**

Five out of 18 managers indicated as an external factor motivating organizations to consider continuous control monitoring as cyber risk and the increased level of enterprise risk management, including challenges for corporate management to focus on managing fraud prevention efforts in the area. Further noted by participant 9 as a key external factor was the ever-changing and expanding areas of risk, including the added risk of "cybersecurity, and hacking." The AICPA issued a cybersecurity guide in response to the need for involvement by the audit profession in the progressive evolution of cyber threats (AICPA, 2016). Cyber risk has had a serious effect upon the risk assessment process for all of the managers surveyed, which has become an even more important part of the audit process (AICPA, 2016) The most pressing topics noted by the five managers for cybersecurity-related to the need for new approaches for assurance. This need supports the further need for implementations of continuous control monitoring and that the traditional audit model, developed for the era of brick-and-mortar business, does not properly fit into the development of the smooth aggregation of assurance services that should exist in the arena of progressively automated multiple assurance processes. These processes are an essential part of the future corporate ecosystem, including enterprise risk

management and fraud prevention. In particular, one basic theme the participants noted of the traditional control-monitoring model was a need to reconsider the point-in-time reporting and control monitoring or testing of controls. This element was intrinsic to a different age, a different technology, and of a different need to the managers, and further to investors and other corporate stakeholders (No & Vasarhelyi, 2017).

Research question 2. What were the perceptions of managers regarding the introduction of new technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods? The focus of the second main research question provided information to understand the perceptions of executive management in regard to the introduction of new technology. Four interview sub-questions supported the overarching research question and helped to drill down on the approach, barrier, and organization outcome to employ continuous control monitoring capabilities within the organizations (Yazan, 2015). The research question interview sub-questions were: (1) what continuous control monitoring approaches are being used in your organization, does the organization use parallel scanning and risk scoring, (2) what extent has continuous control monitoring influenced your organization, positive and negative (3) what areas must enterprise risk management and other finance management work together, (4) what barriers (if any) were encountered when implementing continuous control monitoring? The responses to these four interview questions aligned with research question 2. Responses to each interview sub-question provided data that answered research question 2 and showed that the managers' perceptions of the introduction of new continuous control monitoring technology and that their perceptions for implementation decisions were based on a variety of factors.

Information provided by the research interviews related to the success that each company manager has made with continuous control monitoring implementation. This demographic offered a cross-section of data that assisted in avoiding bias based on the company success of the participating company (Yazan, 2015). Table 6. below shows the sample demographics based on the company success with a continuous control monitoring implementation. The implementation success represented in table 6 is only that of the research interviews that reported a continuous control monitoring methodology. Eight out of the 18 managers indicated companies had a continuous control monitoring approach.

Table 6:
Sample Continuous Control Monitoring Success Demographics

Continuous Control Monitoring Success Demographics	# Participants	Percentage
Extremely Successful	2	25.0%
Moderately Successful	5	62.5%
Marginally Successful	1	12.5%
Overall	**8**	**100%**

For those managers where implementation of continuous control monitoring was extremely successful, indicated was that continuous control monitoring has positively influenced the organization, with participant 5 noting, "through the use of exceptions and alerts we are able to be proactive in risk management rather than reactive." Participant 11 indicated that "due to an existing material weakness there was a need to invest in additional resources, and the continuous control monitoring implementation has allowed a method to resolve the lack of control in a key area of risk for the company." Participants indicated that risk scoring methodologies and system parallel scanning methods are part of the continuous control monitoring resources utilized, and included dashboards and alerts, key risk and performance indicators (KPIs), analysis pattern matching, and various case ware.

During this portion of the interviews, managers identified the same major themes of costs, knowledge, and training as barriers encountered when embracing the new technology, and achieving a successful implementation (Yazan, 2015). Some of the challenges identified when implementing included corporate managers lacking the guidance and skills necessary to implement continuous control monitoring along with access to company data. Managers must decide where continuous control monitoring fits within the business processes and how these can be linked to integrated risk management initiatives (Lombardi et al., 2014; Singh, et al., 2014). All 8 participant managers who indicated a company had implemented continuous control monitoring indicated a need for the various skill sets throughout the company to work together when implementing the resources, in order for the most success.

Summary

Chapter 4 of the study contains the presentation of findings from the qualitative thematic analysis of the interviews with 18 corporate managers across fortune 500 corporations. The purpose of this qualitative instrumental case study was to understand the perceptions the perceptions and experiences of corporate managers' regarding the use of new technology-related tools, which included control monitoring processes, business impacts, and requirements. The interview sub-questions allowed for expansion on the foundation of the study provided by the two main research questions and explored the internal and external factors that contributed to the managers' decision to implement continuous control methodology. The framework approach helped this qualitative research by beginning with the broader topic and refining the study to specific details and findings (Yazan, 2015). Alignment of the ten interview sub-questions allowed the researcher to explore the decision or influence factors, both internal and external, in which the given organizations had experience and the success of their introduction of new

technology for continuous control monitoring. The interviews identified 13 themes or greater occurrences each, with 223 phrases tagged (Taylor, Bogdan, & DeVault, 2015).

The largest barriers to adopting a continuous control monitoring methodology were found to be the mindset of the managers within the given organizations, the lack of understanding the technology available, and the lack of training and skills with the staff and corporate accounting members (AICPA, 2012; ISACA, 2014; Malescu & Sutton, 2015). The challenges identified by the managers centered on increasing training, improving control monitoring tools, and gaining executive management support. Related to the greatest risk factors and enterprise risk management, the key theme was the emerging level of increased cyber risk across all of the participant's companies. Implementing continuous control monitoring requires improving business controls, and the organization must demonstrate the value of continuous control monitoring to the executives.

Training was another area critical area within a domain that is constantly changing, and there were substantive differences in the level of training indicated by managers at the companies interviewed. New technology and tools to perform tasks of control monitoring and enterprise risk management could hinder the corporate managers' performance due to being unfamiliar with the new capabilities (AICPA, 2012; ISACA, 2014; Malescu & Sutton, 2015). Participant responses indicated that training should begin at the collegiate level with risk management and information systems courses addressing the continuous control monitoring domain and methodologies. They reported there was a need for staff with a cross skill set to both implement and manage the continuous control monitoring resources. The closing chapter of the study contains a more in-depth discussion of the findings, implications, recommendations, and conclusions.

Chapter 5: Implications, Recommendations, and Conclusions

In this study, the problem addressed was there were impediments to adoption, implementation, and use of continuous control monitoring procedures for fraud prevention controls to manage organizational risk in maintaining corporate requirements (Hardy & Laslett, 2015; Majdalawieh, et al., 2012; Salvioni, & Astori, 2014; Singh, et al., 2014). The purpose of this qualitative, multiple-case study was to examine corporate managers' perspectives and experiences regarding the impediments to adoption for the implementation and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts. Utilization of a multi-case research design satisfied the goal of the investigative research, and data gathered through in-depth individual interviews. The organization was the unit of analysis in the study. The participant selection strategy was purposeful and allowed for new perspectives while expanding upon developed theory (Benoot, Hannes, & Bilsen, 2016). Literature indicated a sample of six cases without newly present themes to reach saturation (Bowen, 2008). A total of 18 corporate managers were interviewed to explore their perceptions, experiences, and satisfaction regarding continuous control monitoring within their organization. Establishment of credibility required triangulation of the data (Yin, 2014). A qualitative case study method was appropriate as the research included questions of how and why examining the potential challenges present within the social sciences. The case study approach allows for the determination of future research opportunities (Gibbert & Ruigrok, 2010).

The study participants were corporate managers within the publicly traded organization. Males and females with ages between 18 and 65 offered to participate voluntarily in this research. Participant's interview sessions lasted approximately 30 to 60 minutes. Participants

answered interview questions, with data collected; transcribed, and recorded, limitations that could affect identified outcomes. Methods used throughout interviews included appropriate treatment for the purpose of the research ethics. The researcher urged open communication with all research participants and explained the research process, as recommended by Rodhouse & Vanclay (2016). Maintaining ethical standards during the research process was by informing each participant of their respective right to privacy, and the importance of maintaining privacy (Rodhouse & Vanclay, 2016). The participants signed consent forms prior to interviews (Appendix B).

During the research process, noted were limitations including the possibility that although there were two participants from each of the organizations identified, there could be an unbalanced total number from each given organization. Further, the level of expertise of each participant varied, resulting in another limitation. The overall research approach focused to balance the levels of expertise, so the results encompassed all levels in the range of manager experiences. The researcher encouraged participants to share their perceptions, previous experiences, and further comments. With the informed consent process, participants were confident about the interview process and understood the process (Rodhouse & Vanclay, 2016).

The results of the study corroborated with existing literature on certain aspects of continuous control monitoring methodology and helped to bridge the gap that existed due to the lack of studies on perceptions of continuous control monitoring (AICPA, 2012; Gonzalez, et al., 2012; Hardy & Laslett, 2015; Majdalawieh, et al., 2012; Mandru, 2016; Singh, et al., 2014; Steinhoff, et al., 2016). Although continuous control monitoring has been available for years, the managers interviewed noted ongoing levels of continued concerns regarding successful implementation related to the knowledge level of staff, and adoptions of new technology for

enterprise risk management, and fraud prevention due to the impediment of cost and the challenge of achieving buy-in of upper management. Further, it was indicated by the managers that the continuous control tools utilized still varied, with the process of implementation and levels of effort subject to varying costs and benefit levels. Corporate managers thus continue to have a need to consider the current technical environment, resources, and skill levels of staff in making decisions related to implementations of continuous control monitoring technologies.

Provided in this chapter are detailed discussions regarding the implications of the study, including findings, recommendations, and conclusions. Included are a summary of implications of semi-structured interview questions, with an interpretation of results, and recommendations to define opportunities for practice and future research, to expand the knowledge of manager perceptions of continuous control monitoring implementation challenges. The provided conclusions recap the research findings, followed by an overall summary of key points outlined throughout the research.

Implications

The specific problem was technology for enterprise risk management approaches, both automated and continuous processes, are not utilized by managers due to the reluctance of the managers to adopt a new or different approach. The implications of the study and the interpreted results of the findings can prove noteworthy for managers of organizations and their endeavors to achieve improved enterprise risk management and increase fraud prevention and detection efforts. As regulations become more prevalent, the demand for rapid and efficient control monitoring processes will increase (ACFE, 2017; Lombardi, Vasarhelyi, & Verver, 2014; Mandru, 2016).

The overarching research question developed was to determine how organizations managers implemented continuous control monitoring technology, decreased enterprise risk management, and kept business impacts to a minimum. Maintaining costs, including the technology and associated training expenses were the greatest characteristics identified as challenges managers face with implementing continuous control monitoring, followed by having the necessary knowledge of available new technology. Twelve of the 18 managers interviewed indicated that a major concern related to a lack of achieving the needed executive management support for moving to a new continuous control monitoring methodology.

The two research questions explored the experience and perceptions regarding the use and implementations of continuous monitoring. Managers interviewed indicated, based on the data gathered from the transcribed interviews, that approximately 78% of companies are using some form of continuous control monitoring. The most common resource in use were dashboards, which provided exceptions and alerts for identification of control monitoring efforts and was reactive in nature rather than preventative. Two managers indicated the companies had not implemented a continuous control monitoring approach; however, the companies had performed a business analysis to consider the resources.

Research Question 1. What were the experiences of corporate managers with impediments to adoption, implementation, and use of continuous control monitoring procedures for maintaining corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts? addressed the manager perceptions regarding the implementation and use of continuous control monitoring for maintaining corporate requirements with regulatory compliance, including enterprise risk management, and fraud prevention efforts. The subtext for analysis derived from the interview questions #1 through #6. The interview

process concerning these interview questions resulted in four derived major themes among the manager participants interviewed. These themes included resource management, budget, knowledge of their environment, and increased risk areas related to the area of cyber risk and hacking.

Resource management. The driving factor indicated clearly by the managers for reluctance towards implementation of continuous control monitoring resources, based upon the data from the participant interviews, was resource management. This included required justification of the total costs when compared to potential benefits of an implementation of continuous control monitoring resources. As companies evolve to meet risk management and financial needs and processes including technology are changing, managers indicated the special attention needed towards maintaining the people, skills, and technologies required (ACFE, 2017; AICPA, 2012; Deloitte, 2010; KPMG, 2012; ISACA, 2014). Lack of competency and appropriate skill sets, and retention of those staff in a market where there is a high level of competition for those skills were the second most area for key concerns when adding or changing an existing business process. Participant 11 shared their view regarding the challenges they faced related to the unique skill set and associated costs of training that:

> with the introductions of more complex information technology resource, there was a need for extensive training, which reduced the resources available to continue working towards the normal business schedules, targeted by management as of higher importance than that of focusing on improving through the implementation of new technology. Thus, another issue with resource management beyond the dollar cost value was managing the resource of staff.

Budget. A further factor that managers indicated contributing to the lower implementation of new technology for continuous control monitoring was the high cost associated with the change. With 44 occurrences, the budget was often a factor for the managers, considered when adopting a continuous control monitoring. The corporate managers noted that often management perceived a high initial set-up and implementation costs, and the executive management team must understand the full business impacts, including associated cost, training, and resources required to implement successfully a continuous control monitoring methodology. The cost factor as a deterrent to implementation was in line with the findings from the literature review that companies have not implemented continuous control monitoring resources for this reason (AICPA, 2012; Deloitte, 2010; Gonzalez, Sharma, & Galleta, 2012; ISACA, 2014; KPMG 2012; Mandru, 2016). While two of the managers interviewed indicated the implementation of the continuous control monitoring technology as a positive solution for the business, all indicated there were significant cost considerations. Further, managers indicated a major challenge area related to the amount of time devoted to the resources, training, and upgrading current infrastructure.

Knowledge of the environment. The majority of the managers, 16 of the 18, stated that an understanding of the current environment as well as the need to maintain both accurate and secure processes and systems, as necessary factors towards a decision to adopt a continuous control monitoring resource. The managers noted that their accounting organizations and the corporate managers had experienced significant changes since the turn of the millennium, largely due to the rapid changes in information technology environment and new regulatory requirements for financial reporting. The literature review supported that to ensure a successful implementation the enterprise risk management environment requires four standard principles of

integrity, security, availability, and maintainability (Gillespie, et al., 2014; Majdalawieh, et al., 2012; Masli, et al., 2010; Soltani, 2014; Steinhoff, et al., 2016). Further, the research literature indicated a concern when implementing new technologies into existing business systems was due to the possibility of masking underlying existing system problems (Elder, et al., 2014; Holtfreter & Harrington, 2014). The corporate managers indicated a need to rely on the competent staff or lead, to provide the overview of the environment, and ensure that the decision to introduce something new into the existing environment does not cause issues, or unforeseen costs, which was further supported by the literature review (Hardy, & Laslett, 2015; Lombardi, et al., 2014).

Increased risks. Most managers, 88.88% identified increased risks as a factor in the internal and external motivating factors for evaluating the implementation of continuous control monitoring resources. Five managers indicated the increased cyber risks as a factor, which agrees with recent literature review resource information related to emerging risk factors (No, & Vasarhelyi, 2017). Further, seven of the eighteen managers indicated a need to protect health data and other types of non-financial data as an added risk area of concern, motivating the consideration of continuous control monitoring resources. All managers indicated a trend towards a focus of wanting a more proactive enterprise risk management and fraud prevention approach, compared to a reactive approach.

Research Question 2. What were the perceptions of managers regarding the introduction of new technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods? addressed the perceptions of introducing new technology into the existing environment for continuous control monitoring purposes. For purposes of analysis, interview questions #1 through #4 provided the subtext and four major themes derived from the interview process concerning these sub-questions.

Budget or cost, training, management support, and knowledge of technology were driving thoughts among the corporate managers.

Budget or cost. As seen in the budget and cost concerns identified by managers for the first research question, similar themes occurred regarding those companies who had introduced new technology including parallel scanning and risk scoring methods. Further, the results supported the implications noted by the literature review that continuous control monitoring can provide improved enterprise risk management benefits including cost recovery, efficiency, and fraud-prevention benefits making this method a prudent choice for managers to adopt as part of their risk management strategy (ACFE, 2017; Majdalawieh, et al., 2012; Mandru, 2016; Singh, et al., 2014; Steinhoff, et al., 2016). In the study, five of the managers where continuous control monitoring resources were in place communicated a need to address concerns with the expense that was required when implementing or making a change to the existing business process for control monitoring efforts. Alternatively, two of managers indicated that having a strong board of director support for implementation initiatives supported the goal of increasing risk management efficiencies and fraud prevention efforts.

Training. When an organization adopts continuous control monitoring resources, the literature review indicated a requirement for a knowledgeable staff with both information systems and data analysis skills to effectively improve enterprise risk management (AICPA, 2012; Deloitte, 2010; ISACA, 2014; KPMG, 2012; Mandru, 2016). The managers' responses supported that focused training in the continuous control monitoring as needed, along with increased training in the operations of the wide variety of available tools. One aspect identified by all managers, as a need related to continuous control monitoring was the ability to create routine scripts for the testing performed on a continuous basis. Furthermore, of the managers

who have implemented a continuous control monitoring methodology, six of the eight managers identified training as a requirement for their company's successful implementation and use of continuous control monitoring methodology.

Management support. The published results from the continuous monitoring studies explained benefits and business process improvements but lacked in providing detailed guidelines and recommendations on financial reporting and regulatory compliance including enterprise risk management (AICPA, 2012; KPMG 2012; Mandru, 2016; Salvioni & Astori, 2013; Steinhoff, et al., 2016). For 5 out of 8 managers, a theme noted for those companies who had implemented parallel scanning or risk scoring methods, was an initial lack of upper management support on the introduction of a change to the business process. According to the managers, upper management supporting the effort to introduce change into the business processes showed commitment to the new technology and methodology, also in line with the noted area of importance in the literature review of a need for management buy-in for implementation success (ACFE, 2017; Mandru, 2016; Singh, et al., 2014; Steinhoff, et al., 2016). Further, the managers noted an importance for senior management to consider long-term strategy; and take definitive steps to translate that vision into a program of activities and improving the enterprise-risk management efforts. The literature review included support for the importance of long-term strategic planning to enterprise risk management and fraud prevention efforts noted by the managers in the study (ACFE, 2017; Majdalawieh, et al., 2012; Mandru, 2016; Singh, et al., 2014; Steinhoff, et al., 2016).

Knowledge of technology. The utilization of information technology in modem control monitoring efforts increased significantly in recent years due to both technological developments

in addition, a changing regulatory environment (ACFE, 2017; Mandru, 2016; Singh, et al., 2014; Steinhoff, et al., 2016). While the benefits of continuous monitoring may be high, 60% of the managers identified a barrier related to a lack of full understanding the current technology or continuous control monitoring approaches. Two of the biggest hurdles identified were with the stakeholder's buy-in and training of staff. The resources need to have an understanding of how the new tools or software related to the current systems in place. Another area of concern was how the new continuous technology accesses the business data through databases or systems. Participant #11 indicated, "it was critical to determine the foundation components for a continuous control monitoring methodology to ensure that the approach provides the validation of the business environment." The findings correlated with the significance of the study in that executive management make choices on continuous control monitoring implementations for the business. Additionally, the introduction of new legal and regulatory mandates has increased the need for dependable controls, as these regulations can invoke harsh sanctions upon those failing to comply (ACFE, 2017; Lombardi, et al., 2014). Each manager where continuous control monitoring was implemented indicated that understanding the business impact of continuous control monitoring on financial reporting and regulatory compliance are important to the success and future growth within the industry. This was supported by the literature review which noted a need for senior management to consider long-term strategy; define a clear vision and take definitive steps to translate that vision into a program of activities (AICPA, 2012; Salvioni & Astori, 2013; Steinhoff, et al., 2016).

Recommendations

All researchers should attain a goal of either offering practical application of the findings or provide recommendations for future research. The research study presented

here includes findings and interpretations for the foundation for future research. This portion of the study included the recommendations for applications of this study. First presented are practical applications, followed by the future research recommendations.

Recommendations for practice. The study findings have practical applications for managers because it was those individuals who generally make the business decisions. As a technology-driven methodology, the study agreed with the literature review regarding continuous control monitoring provided for timely identification of anomalies or control gaps for financial reporting purposes (AICPA, 2012; KPMG 2012; Salvioni & Astori, 2013; Steinhoff, et al., 2016). A wide range of predictive methodologies are now available and have been practically implemented (Siegel, 2013). Hence, it is natural that these methodologies evolve into the corporate measurement arena.

With any major investment, corporate managers must support the decision to implement new technology and processes. If managers do not perceive continuous control monitoring as useful, stakeholders are not willing to risk investing in the technology. What will lead to the adoption of continuous control monitoring technology to be evolutionary rather than revolutionary are the resolution of various impediments to continuous control monitoring implementation regarding people, processes, and technology (Lombardi, et al., 2014; Singh, et al., 2014). These impediments were identified and discussed with participants throughout this research study. Further research provides the corporate business community with guidance on new mandates and requirement changes, guidance for implementation of continuous control monitoring technologies, as well as the determination of consequences and benefits.

Continuous control monitoring is a proactive approach rather than a reactive approach. Continuous control monitoring assists management with allocating resources to focus on high

risk or significant areas of exposure to organizations. As organizations are expanding into global businesses, it is important for managers to have a global vision with the move towards a new control monitoring methodology. Managers have a need for greater understanding of the advantages and disadvantages of any new technology introduced into the business processes (AICPA, 2012; Salvioni & Astori, 2013; Steinhoff, et al., 2016). Understanding the characteristics of continuous control monitoring and the associated cost, training, and support required is necessary for managers to be successful with implementing a new control monitoring approach for enterprise risk management, and fraud prevention.

Recommendations for future research. Although continuous control monitoring tools, techniques and technology have been widely discussed over the years in regard to the impact continuous control monitoring has on process improvements, additional research would be beneficial (AICPA, 2012; Deloitte, 2010; KPMG 2012; ISACA, 2014; Malescu & Sutton, 2015). Strengths of qualitative case studies are the importance of the findings and recommendations (Creswell, 2014). Most of the larger organizations are becoming global businesses. By conducting this research with participants from global organizations, allow the opportunity to discover whether there are similar cases in other countries. By conducting a similar study outside of the United States, researchers may be able to generalize the findings to a wider audience.

Research into continuous control monitoring methodology has been performed and theoretically, as well as empirical research is needed to further educate managers in regard to continuous control monitoring resources. The introduction of new methodologies has both advantages and disadvantages to organizational goals pertaining to their current processes, technology platforms, and resources (Fatema, et al., 2014; Hardy, & Laslett, 2015; Lombardi, et

al., 2014). Needed future research is on a larger scale to analyze options and tools are available to make the paradigm shift to a continuous control monitoring methodology. Educating the managers on the options that are available to assist in enhancing their control monitoring approach provided them with research to make a sensible business decision. Noted impediments which are in line with the literature review were the areas of budget, technology, and resources for organizations moving to a continuous control monitoring approach (Fatema, et al., 2014; Hardy, & Laslett, 2015; Lombardi, et al., 2014; Vasarhelyi, Romero, & Kuenkaikaew, 2012).

Future research should address opportunities available with new technology that addresses updated mandates for financial reporting. Technology changes rapidly and future research would reveal supplementary opportunities for business executives to consider for their enterprise risk management solutions. Additionally, future research should focus on enhancements that have evolved to address enterprise risk management strategies on compliance mandates, cyber and fraud prevention efforts for that are of emerging risk noted by managers and the literature review (ACFE, 2016; No & Vasarhelyi, 2016; Steinhoff, et al., 2016). The accounting industry continues to provide guidance and standards to corporate managers at a common or high level; therefore, future research should focus on these changes and provide details that could assist in improvements to business strategies.

Conclusions

The results and findings of this study conclude that continuous control monitoring is not feasible for all organizations; however, with the proper stakeholder and manager support, budget, and training, continuous control monitoring could have benefits for enterprise risk management and fraud prevention. In today's regulatory environment, corporate managers find their staffing resources are consumed with the monitoring and testing of internal controls to meet the

regulatory and compliance demands (ACFE, 2016; AICPA, 2012; Vasarhelyi, et al., 2012; Steinhoff, et al., 2016). Organizations are continually exposed to significant errors, frauds, or inefficiencies that can lead to financial loss and increased levels of risk (No & Vasarhelyi, 2017; Singh, et al., 2014; Steinhoff, et al., 2016). An evolving regulatory environment, increased globalization of businesses, market pressure for improved operations, and rapidly changing business conditions are creating the need for more timely and ongoing assurance that controls were working effectively and risk was being mitigated (AICPA, 2012; No, & Vasarhelyi, 2017; Singh, et. al., 2014; Steinhoff, et.al., 2016). It was evident that a new control monitoring approach, one that provides a sustainable, productive, and cost-effective means to address the changes in technology and ongoing regulatory and compliance mandates, was essential. The biggest impediments appeared to be the mindset of the corporate managers, the lack of budget or resources, and the lack of skills or training of the resources, as indicated by manager responses, supported by the literature review (Fatema, et al., 2014; Hardy, & Laslett, 2015; Lombardi, et al., 2014; Majdalawieh, et al., 2012; Vasarhelyi, et al., 2012). One perception identified centered on the proper training with the new technology. A business analysis could help the organizations with identifying the value of continuous control monitoring to the enterprise risk management and fraud prevention efforts. Managers indicated that business analysis added benefits with the control monitoring paradigm shift, but it was not necessarily budgeted with a priority. Furthermore, the study concluded that if the organization could afford a change towards a continuous approach, they must have confidence that the new methodology ensures a more timely and efficient risk management program for their business.

Practical applications indicated that this study was important for managers in the

move towards new continuous control resources. Corporate managers must understand the advantages and disadvantages of any new technology introduced into their business process. For the managers to understand the characteristics of continuous control monitoring, it was important for them to understand the cost, training, and support required to be successful with implementing a new continuous control monitoring approach (Fatema, et al., 2014; Hardy, & Laslett, 2015; Lombardi, et al., 2014; Vasarhelyi, et al., 2012).

The future research, needed on a larger scale, is to discover what options and tools are available to make the paradigm shift to a continuous control monitoring methodology. Other studies including qualitative and quantitative studies should be conducted to validate results by exploring new technologies and new mandates for financial reporting. The findings, recommendations, and conclusions provide a broader insight into existing knowledge of continuous control monitoring and provide critical insight to assist managers in understanding the shift to new control monitoring methodologies for enterprise risk management.

References

Ajah, I., & Inyiama, C. (2011). Loan fraud detection and IT-based combat strategies. *Journal of Internet Banking & Commerce*, *16*(2), 1-13. Retrieved from http://www.icommercecentral.com/open-access/loan-fraud-detection-and-itbased-combat-strategies.php?aid=38252

American Institute of Certified Public Accountants (AICPA). (2016). *AICPA proposes criteria for cybersecurity risk management*. Retrieved from http://www.aicpa.org/Press/PressReleases/2016/Pages/AICPA-Proposes-Criteria-for-Cybersecurity-Risk-Management.aspx

American Institute of Certified Public Accountants (AICPA). (2012). *The current state of continuous auditing and continuous monitoring*. Retrieved from http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper_current-state-continuous-auditing-monitoring.pdf

Association of Certified Fraud Examiners. (2016). Report to the nations on occupational fraud and abuse: 2016 global fraud study, 1-79. Retrieved from https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

Baškarada, S. (2014). Qualitative case study guidelines. *Qualitative Report, 19*(40), 1. Retrieved from www.dtic.mil.

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology*, 1621. doi: 10.1186/s12874-016-0114-6

Bergeron, F., & Raymond, L. (1997). Managing EDI for corporate advantage: A longitudinal study. *Information Management, 31*, 319-333. doi:10.1016/S0378-7206 (97)00007-4

Bowen, G.A. (2008). Naturalistic inquiry and the saturation concept: A research note. *Qualitative Research*, 8(1), 137-152. doi: 10.1177/1468794107085301

Braun, V. and Clarke, V. (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3 (2). pp. 77-101. doi.org/10.1191/1478088706qp063oa

Chenail, R. J. (2011). Ten steps for conceptualizing and conducting qualitative research studies in a pragmatically curious manner. *The Qualitative Report*, 16(6), 1713-1730. Retrieved from http://nsuworks.nova.edu/tqr/vol16/iss6/13

Clerke, T., & Hopwood, N. (2014). Doing ethnography in teams. Cham, Switzerland: Springer. doi:10.1007/978-3-319-05618-0_2

Creswell, J.W. (2014). *Research design: Qualitative, quantitative, and mixed methods approach*. (4th ed.) Thousand Oaks, CA: Sage.

Coderre, D. (2005). *Global technical auditing guide: Continuous auditing implications for assurance, monitoring, and risk assessment*. Altamonte Springs, Fla.: Institute of Internal Auditors.

Davis, F. A. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*, 319-339. doi:10.2307/249008

Deloitte. (2010). Continuous monitoring and continuous auditing-From idea to implementation. Retrieved from http://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-aers-continuous-monitoring-and-continuous-auditing-whitepaper-102910.pdf

Dickins, D., & Reisch, J. T. (2012). Enhancing auditors' ability to identify opportunities to commit fraud: Instructional resource cases. *Issues in Accounting Education*, *27*(4), 1153-1169. doi:10.2308/iace-50178

Dull, R. (2014). What gets monitored gets detected. *Journal of Accountancy*, *217*(2), 1-6. Retrieved from https://www.journalofaccountancy.com/

Elder, R. J., Janvrin, D. J., & Caster, P. (2014). Peregrine--Twenty years of fraudulent cash balances. *Issues in Accounting Education*, 29(2), 337-348. doi:10.2308/iace-50690

Fatema, K., Emeakaroha, V. C., Healy, P. D., Morrison, J. P., & Lynn, T. (2014). A survey of cloud monitoring tools: Taxonomy, capabilities, and objectives. *Journal of Parallel & Distributed Computing*, *74*(10), 2918-2933. doi: 10.1016/j.jpdc.2014.06.007

Gheorghe, M. (2010). Audit methodology for IT governance. *Informatica Economica*, 14, 32-42. Retrieved from http://revistaie.ase.ro/

Gibbert, M. & Ruigrok, W. (2010). *The what and how of case study rigor: Three strategies based on published work.* Organizational Research Methods, 13, 710-737.

Gillespie, N., Dietz, G., & Lockey, S. (2014). Organizational reintegration and trust repair after an integrity violation: A case study. *Business Ethics Quarterly*, 24(3), 371-410. doi:10.5840/beq2014437

Goertz, G., & Mahoney, J. (2012). *A tale of two cultures: Qualitative and quantitative research in the social sciences.* Princeton, NJ: Princeton University Press.

Gonzalez, G.C., Sharma, P.N., & Galletta D. (2012). Factors influencing the planned adoption of continuous monitoring technology. *Journal of Information Systems*, 26 (2), pp. 53–69. doi:10.2308/isys-50259

Gupta, P. P., Weirich, T. R., & Turner, L. E. (2013). Sarbanes-Oxley and public reporting on internal control: Hasty reaction or delayed action? *Accounting Horizons*, 27(2), 371-408. doi:10.2308/acch-50425

Gutholc, R. (2008). 21st-century excellence in finance through continuous monitoring. *Business Management*, 9(1), 1-2. Retrieved from https://www.acl.com/pdfs/Success_Story_Healthcare_Memorial.pdf

Hardy, C. A., & Laslett, G. (2015). Continuous auditing and monitoring in practice: Lessons from Metcash's business assurance group. *Journal of Information Systems, 29*(2), 183-194. doi:10.2308/isys-50969

Holloway, I. & Wheeler, S. (2013). *Qualitative research in nursing and healthcare. (*3rd ed.) Malden, MA: Blackwell

Holtfreter, R. E., & Harrington, A. (2014). Will hackers win the battle? (cover story). *Strategic Finance*, *96*(1), 27-34. Retrieved from http://sfmagazine.com/

Hong, W., Thong, J.Y.L., Wong, W.M., & Tam. K.Y. (2002). Determinants of user acceptance of digital libraries: An empirical examination of individual differences and system characteristics. *Journal of Management Information Systems,* 18 (3): 97- 124. Retrieved from www.jmis-web.org/

Hsieh, C., & Lin, F. (2013). Applying digital analysis to detect fraud: An empirical analysis of US marine industry. *Applied Economics*, 45(1), 135-140, doi:10.1080/00036846.2011.605759

Hu, P. J., Chau, P. Y. K., Sheng, O. R. L., & Tam, K. Y. (1999). Examining the technology acceptance model using physician acceptance of telemedicine technology. *Journal of Management Information Systems*, 16, 91–112. doi:10.1080/07421222.1999.11518247

Huffman, A., & Crump, J. (2005). Applying continuous controls monitoring for achieving compliance and business improvement. *Financial Executive*, *21*(8), 54-56, Retrieved from http://www.financialexecutives.org

ISACA. (2014). *Relating the COSO internal control—Integrated framework and COBIT*, USA Retrieved on June 24, 2017, from http://www.isaca.org/Knowledge-Center/Research/Documents/Relating-the-COSO-Internal-Control-Integrated-Framework-and-COBIT_whp_Eng_0314.pdf?regnum=379385

Kafle, N. P. (2013). Hermeneutic phenomenological research method simplified. *Bodhi: An Interdisciplinary Journal, 5*(1), 181-200. doi:10.3126/bodhi.v5i1.8053

KPMG. (2012). Continuous auditing and continuous monitoring: The current status and the road ahead. Retrieved from https://www.kpmg.com/PT/pt/IssuesAndInsights/Documents/cacm2012.pdf

Kuhn Jr., J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. Journal of Information Systems, *24*(1), 91-112. doi:10.2308/jis.2010.24.1.91

Leavy, P., & Bryant, A. (2014). The grounded theory method. In P. Leavy (Ed.), *The Oxford Handbook of Qualitative Research*. New York, NY: Oxford University Press. doi:10.1093/oxfordhb/9780199811755.013.016

Lee, I. (2006). *E-business innovation and process management.* Hershey, PA: Cybertech Publishing. doi:10.1015/j.ipm.2005.02.005

Lin, C. S. (2013). Revealing the "essence" of things: Using phenomenology in LIS research. *Qualitative and Quantitative Methods in Libraries (QQML), 4*, 469-478.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry.* Beverly Hills, CA: Sage.

Lombardi, D. R., Vasarhelyi, M. A., & Verver, J. (2014). Continuous controls monitoring: A case study. *Journal of Emerging Technologies in Accounting*, *11*(1), 83-98. doi:10.2308/jeta-51006

Majdalawieh, M., Sahraoui, S., & Barkhi, R. (2012) Intra/inter process continuous auditing (IIPCA), integrating CA within an enterprise system environment', *Business Process Management Journal*, 18 (2), 2012, p. 304-327. doi:10.1108/1463715121125216

Malaescu, I., & Sutton, S. G. (2015). The reliance of external auditors on internal audit's use of continuous audit. *Journal of Information Systems*, *29*(1), 95-114. doi:10.2308/isys-50899

Mandru, L. (2016). How to control risks? Towards a structure of enterprise risk management process. *Journal of Public Administration, Finance and Law*, (9), 80-92. Retrieved from http://www.jopafl.com/

Masli, A., Peters, G. F., Richardson, V. J., & Sanchez, J. M. (2010). Examining the potential benefits of internal control monitoring technology. *Accounting Review,* 85(3), 1001-1034. doi**:** 10.2308/accr.200.85.3.1001

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1978). *The Belmont report: Ethical principles and guidelines for the commission for the protection of human subjects of biomedical and behavioral research,* Bethesda, MD

No, G. W. & Vasarhelyi, M.A. (2017) Cybersecurity, and continuous assurance. *Journal of Emerging Technologies in Accounting*, 14(1), 1-12. doi:10.2308/jeta-10539.

Nigrini M.J. (2017). Audit sampling using Benford's Law: A review of the literature with some new perspectives. *Journal of Emerging Technologies in Accounting In-Press.* doi:10.2308/jeta-51783

Olach, T. (2008). The PCAOB 101. *Internal Auditor*, *65*(3), 50-54. Retrieved from https://na.theiia.org/periodicals/Pages/Internal-Auditor-Magazine.aspx

Punch, K. F. (2013). *Introduction to social research: Quantitative and qualitative approaches.* London, UK: Sage.

Ramamoorti, S., & Dupree, J. (2010). Continuous controls monitoring can help deter fraud. *Financial Executive*, *26*(2), 66-67, Retrieved from http://www.financialexecutives.org

Richardson, M. (2012). Regulating Wall Street: The Dodd-Frank Act. *Economic Perspectives*, (3), 85-97. Retrieved from http://www.chicagofed.org/index.cfm

Rodhouse, T., & Vanclay, F. (2016). Review: Is free, prior and informed consent a form of corporate social responsibility? *Journal of Cleaner Production*, *131*785-794. doi:10.1016/j.jclepro.2016.04.075

Salvioni, D. M., & Astori, R. (2013). Sustainable development and global responsibility in corporate governance. *Symphonya: Emerging Issues in Management*, (1), 28-52. doi:10.4468/2013.1.03salvioni.astori

Schermann, M., Wiesche, M, & Krcmar, H. (2012) The role of information systems in supporting exploitative and exploratory management control activities, *Journal of Management Accounting Research, 24*, p. 31-59. doi:10.2308/jmar-50240

Siegel, E. 2013. *Predictive analytics: The power to predict who will click, buy, lie, or die.* New York, NY: John Wiley & Sons. ISBN 978-1-1183-5685-2.

Singh, K., Best, P. J., Bojilov, M., & Blunt, C. (2014). Continuous auditing and continuous monitoring in ERP environments: Case studies of application implementations. *Journal of Information Systems*, *28*(1), 287-310. doi: 10.2308/isys-50679

Soltani, B. (2014). The anatomy of corporate fraud: A comparative analysis of high profile American and European corporate scandals. *Journal of Business Ethics*, *120*(2), 251-274. doi: 10.1007/s10551-013-1660-z

Steinhoff, J. C., Price, L. A., Comello, T. J., & Cocozza, T. A. (2016). Ten steps to sustainable enterprise risk management. *The Journal of Government Financial Management*, *65*(2). Retrieved from http://www.agacgfm.org.

Taylor, S. J., Bogdan, R., & DeVault, M. (2015). *Introduction to qualitative research methods: A guidebook and resource.* New York, NY: John Wiley & Sons.

Trochim, W., & Donnelly, J. (2008). *The Research Methods Knowledge Base* (3rd ed.) Mason, OH: Cengage Learning

Vasarhelyi, M. A. (2012). Financial accounting standards should not matter: It's just a layer. *Journal of Information Systems, 26*(2), 1-11. doi:10.2308/isys-10280

Vasarhelyi, M. A., Romero, S., & Kuenkaikaew, S. (2012). Adopting continuous auditing/continuous monitoring in internal audit', *ISACA Journal*, 3, p. 1-5. doi:10.1016/j.accinf.2012.06.011

Whiting, D. G., Hansen, J. V., McDonald, J. B., Albrecht, C., & Albrecht, W. (2012). Machine learning methods for detecting patterns of management fraud. *Computational Intelligence, 28*(4), 505-527. doi:10.1111/j.1467-8640.2012.00425.x

Wimmer, R., & Dominick, J. (2013). *Mass media research: An introduction* (8th ed.). Belmont, CA: Thomson.

Wu, C. V., & Beaunae, C. (2014). Personal reflections on cautions and considerations for navigating the path of grounded theory doctoral theses and dissertations: A long walk through a dark forest. *International Journal of Social Research Methodology*, *17*(3), 249-265. doi: 10.1080/13645579.2012.729392

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report, 20*(2), 134-152.

Yin, R. (2014). *Case study research: Design and methods*. London: Sage.

Zenker O., & Kumoll, K. (2010). *Beyond writing culture: Current intersections of epistemologies and representational practices.* New York, NY: Berghahn Books.

Appendices

Appendix A: Interview Questions

Demographic Questions

The interview will start with some demographic questions:
(1) What is your current position and title within the organization?
(2) How long have you been employed by the organization?
(3) Have you held another position with the organization? If yes, what was the position?
(4) In what category would you place your organization?
(a) Healthcare
(b) Government
(c) Financial/Banking
(d) Education
(e) Industry
(5) What is the primary function or service provided by your organization?
(6) Approximately how many individuals does your company employ?
(a) 1 - 9 9
(b) 100 - 499
(c) 500-1000
(d) 1000-5000
(e) Over 5000
(7) What control monitoring/auditing methodology or approach does your organization follow to ensure regulatory compliance?
(a) A risk-based monitoring/auditing
(b) A continuous control monitoring/auditing
(c) A cyclic approach
(d) Other, please explain
(8) Does your organization have formal written financial reporting and control monitoring/auditing policies?
(9) To your knowledge is your organization subject to legal, regulatory, or industry mandates? If yes, what are they?
(a) HIPAA
(b) SOX
(c) FISMA
(d) FFIEC
(e) Other (Identify and describe the mandates)
(10) On a scale of 1 to 10, how would you rate your knowledge of the principles and practices of a continuous control monitoring/auditing environment? How did you determine your rating on the above scale?

Research Questions and Sub-questions

The overarching question, "How can an organization implemented continuous control monitoring, maintained their corporate requirements, and improve enterprise risk management?" will be answered by the following interview question responses:

Interview Question Q1. *What is the experience of executives with the implementation and use of continuous control monitoring procedures for maintaining their corporate requirements with regulatory compliance, including enterprise risk management and fraud prevention efforts?*

Ql-1. What internal factors within your organization would motivate, or motivated, you to employ continuous control monitoring/auditing capabilities in your organization?
Ql-2. What factors external to your organization would motivate, or motivated, you to employ continuous control monitoring/auditing capabilities in your organization?
Ql-3. What internal factors cause you to be reluctant to employ continuous control monitoring/auditing capabilities in your organization?
Ql-4. What external factors cause you to be reluctant to employ continuous control monitoring/auditing capabilities in your organization?
Ql-5. Are you of the opinion that industry leaders in general are reluctant to implement continuous control monitoring/auditing capability? Why?
Ql-6. What extent may management rely on continuous control monitoring evidence generated for risk management and fraud prevention?

Interview Question *Q2*. What are the perceptions of managers regarding the introduction of new technology for continuous control monitoring, including the use of systems parallel scanning, and risk scoring methods?

Q2-l.What continuous control monitoring/audit approaches are being used in your organization? To what extent does your organization utilize system parallel scanning, and risk scoring methods? What were your original reactions to this process and why?
Q2-2. What extent has continuous control monitoring/auditing influenced your organization, positive and negative?
Q2-3. In what areas must the enterprise risk management and other finance management work together in the implementation of a continuous control monitoring program?
Q2-4. What barriers (if any) were encountered when implementing continuous control monitoring/auditing?

Appendix B: Informed Consent

Introduction:

My name is Cynthia Davidson. I am a doctoral student at Northcentral University. I am conducting a study on ways companies ensure their policies meet federal laws and how computer tools can help in that effort. I am completing this research as part of my doctoral degree. I invite you to participate.

Activities:

If you participate in this research, you will be asked to:

1. You will be asked to complete an interview about controls, and fraud. This interview would last 30 minutes.
2. Another interview would follow to discuss the topic in more detail. The session will last 20 minutes.

Eligibility:

You are eligible to participate in this research if you:

1. Are a manager in an accounting role with 2 years experience
2. Located within the United States
3. Between the ages of 18 and 65

You are not eligible to participate in this research if you:

1. Have no understanding of finance or controls
2. Have no experience with fraud risk
3. 17 years old or younger or 66 years old or older

I hope to include 20 people in this research.

Risks:

There are minimal risks in this study, which include confidentiality of business information. To decrease the impact of these risks, you can: Skip any question, or stop answering questions at any time.

Benefits:

If you decide to participate, there are no direct benefits to you. There may be some benefits of adding to the field of business in control and fraud areas.

Confidentiality:

The information you provide will be kept confidential to the extent allowable by law. Some steps I will take to keep your identity confidential are: I will use a number to identify you.

The people who will have access to your information are: I will have access. My chair will have access. The Institutional Review Board may also review my research and view your information.

I will secure your information with these steps: Personal identifiers will be removed. Data will be maintained on a secure computer. Data will be password protected. I will keep your data for 7 years. Then, I will delete electronic data and destroy paper data.

Contact Information:

If you have questions for me, you can contact me at: Cynthia Davidson (C.Davidson6253@email.ncu.edu; 740-248-3380)

My dissertation chair's name is Henry Luckel, PhD. He works at Northcentral University and is supervising me on the research. You can contact him at: Henry Luckel (hluckel@ncu.edu; 719-330-3342).

If you have questions about your rights in the research, or if a problem has occurred, or if you are injured during your participation, please contact the Institutional Review Board at: irb@ncu.edu or 1-888-327-2877 ext 8014.

Voluntary Participation:

Your participation is voluntary. If you decide not to participate, or if you stop participation after you start, there will be no penalty to you. You will not lose any benefit to which you are otherwise entitled.

Audiotaping:

I would like to use an audio recording of your actions. Because this tape will record your voice, these extra steps will be taken: tapes will be securely stored in a locked safe and labeled with a code. Data will be password protected. I will keep your data for 7 years. Then, I will delete electronic data. You can still participate if you do not wish to be recorded.

Please sign here if you will allow me to atape you:

Signature:

A signature indicates your understanding of this consent form. You will be given a copy of the form for your information.

Participant Signature	Printed Name	Date
_____	_____	_____

Researcher Signature	Printed Name	Date
_____	_____	_____