2015-01-01

Enterprise Systems, Information Security Management Systems and Their Impact on Enterprise Risk: A 3-Essay Dissertation

Fernando Parra Reyes
University of Texas at El Paso, f@fernandoparra.com

ENTERPRISE SYSTEMS, INFORMATION SECURITY MANAGEMENT SYSTEMS AND THEIR IMPACT ON ENTERPRISE RISK: A 3-ESSAY DISSERTATION

FERNANDO PARRA REYES

DOCTORAL PROGRAM IN INTERNATIONAL BUSINESS

APPROVED:

Laura L. Hall, Ph.D., Chair

Leopoldo A. Gemoets, D. Sc.

Rafael S. Gutierrez, Ph. D.

M. Adam Mahmood, Ph.D.

Charles Ambler, Ph.D.
Dean of the Graduate School

DEDICATION

To the loving memory of my Mother

To the endless support, strength and love of my Father and Julia

To the unconditional love from my beautiful sisters, nephews and nieces:

Lupita, Veronica, Gina and Joanna

Aurelio, Melissa, Paulina, Giovanni and Angelique

To my pillar: Adrienne

To my strongest supporters and dear friends

Abby, Aida, Adriana, Alma, Belal, Brenda, Delia, Emmanuel, Han, Laura, Lorena, Norma, Suzanne, Tricia

To endless nights and days with Lola and Rocco

To my entire Family

To the unwavering support and inspirational drive of Dr. Laura Hall

To the invaluable guidance from my Committee Members

To the selfless mentoring of all my Professors

To the treasured support of my colleagues and coauthors

To the Ph.D. Project's guidance

To my all my students

To President Dr. Diana Natalicio's leadership

To all those that have been able to touch my life

To the generous clemency of the judiciary and my community

To those that will travel through this same journey

To Rehabilitation and Resilience

ENTERPRISE SYSTEMS, INFORMATION SECURITY MANAGEMENT SYSTEMS AND THEIR IMPACT ON ENTERPRISE RISK: A 3-ESSAY DISSERTATION

by

FERNANDO PARRA REYES

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

DOCTORAL PROGRAM IN INTERNATIONAL BUSINESS

THE UNIVERSITY OF TEXAS AT EL PASO

May 2015

ACKNOWLEDGEMENTS

I am extremely fortunate to have been awarded the tremendous opportunity of being able to pursue my Ph.D. at UTEP. I am greatly indebted to my professors' kind overtures and their continuous directive throughout the program. My ability to yield positive results would have been impossible without their unwavering support and their prudent advice.

I am exceptionally honored and grateful to have Dr. Laura L. Hall as my dissertation committee chair who has been a solid pillar of support, an inspirational and principled compass and a strong influential advisor. My decision to pursue a doctoral degree and a life in academia was inspired by her unsurpassed passion to serve students and her inquisitive drive to use technology to transform lives.

I am particularly grateful to Dr. Leopoldo Gemoets, Dr. M. Adam Mahmood and Dr. Rafael S. Gutierrez for their unparalleled wisdom, strong mentoring and rigorous feedback in the development of this dissertation. Their commitment to academic research and students teaching will have a long lasting effect on me.

I am also extremely thankful to Dr. Kallol Bagchi, Dr. Peter Kirs, Dr. Richard Posthuma and Dr. Ousmane Seck, Dr. Godwin Udo and Dr. Pradja Vidyarthi for having guided me selflessly throughout my doctoral studies to noble projects and for sharing their invaluable knowledge; but more so for reminding me of the humility of our share in an ever-expanding universe of wisdom.

I deeply appreciate the tremendous support and the our College of Business Administration Dean, Dr. Robert Nachtmann, our Graduate School Dean, Dr. Charles Ambler, our Director, Dr. Fernanda Wagstaff, and all the academic advisors who have worked endlessly to make this such a successful doctorate program.

I am especially thankful to Dr. Diana Natalicio for having uniquely transformed our university under her exceptional tenure and resilient leadership; her vision will forever touch thousands of lives who sought education as the driver to personal growth, the impact of her governance will transcend generations to come.

I am deeply grateful and humbled by all the inspiration from the students I have been privileged to serve as an instructor, they have been my source of motivation to continue serving in academia.

I enormously appreciate Ms. Mary Hernandez who managed to find every bit of support, even when undeserved, while we coursed through this journey; more so, for having carried all of us in their arms throughout our most difficult times.

I also want to express my deep gratitude to my dear colleagues who extended their wisdom and advice during this time, particularly Dr. Abby Peters, Dr. Belal Abdelfattah and Dr. Thaung Han. I believe that they walked side by side with me through this journey sharing unparalleled motivation, inspiring me to commit my absolute best every step of the way.

Last but not least, I would like to thank the Ph.D. Project and its members for their amazing support and mentorship. My batteries were always recharged every time I had the opportunity to seek their advice or guidance. The dedication to the advancement of minority doctoral students has been an inspiring driver to my commitment to excellence, as an ambassador of generations that will follow.

ABSTRACT

This 3-essay study offers a comprehensive examination of hypothetical concepts related to the behaviors, attitudes, outcomes, processes, experiences, manifestations and indicators connected with an organization's design, implementation and management of a coherent set of policies, processes and systems to manage risks to its information assets. Network analysis tools are used to examine the relationships found in Information Security Management Systems (ISMS) literature published within the last decade. This study examines the effect of upgrades and implementations of enterprise systems on enterprise risk, as perceived by external investors. Finally, this study also assesses the impact of external IT governance certifications on enterprise risk, as perceived by investors and as reported by publicly traded companies. The 3-essay structure of the study also considers the moderating effects of certain system characteristics and certification types.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

THE DISSERTATION

CHAPTER 1 – INTRODUCTION

1.1 Research Background

The innovation of revolutionary information systems over the last few decades, combined with a reduction of trade barriers across countries and aggressive worldwide corporate activism and decisive governmental trade action, has sparked a vast ocean of organizational information that mandates the adaptation of security management paradigms in this new Information Age. Given the volatility of digital information, organizations need to ensure that they manage risks effectively by integrating security initiatives in their daily operations as well as their overall governance. This is a particularly serious mandate given the constant and deliberate attempts to disrupt businesses by a myriad of global security breaches that have been motivated by ill-defined ideologies, state-sponsored international conflict or traditional illicit enterprise (Snow, 2011).

As reported to in a special congressional report and a subsequent U.S. Senate hearing before the Subcommittee on Crime and Terrorism, the U.S. has experienced a significant rise in computer security breaches that are estimated to have caused losses due to virus, worms, and other forms of information security breaches ranging from $13 billion to $226 billion (Cashell, Jackson, Jickling, & Webel, 2004; PrivacyRights.org, 2013). These efforts have not subdued; in the U.S. alone, the Privacy Rights Clearinghouse has documented a total of 3,704 security breach incidents affecting at least 600 million records over the last 9 years (PrivacyRights.org, 2013). The lack of security systems that can deter information breaches not only impact the livelihood of corporations, but as stated by Defense Secretary Leon E. Panetta (Bumiller & Shanker, 2012), they represent a national security threat that could "cause physical destruction and the loss of life…and could shock the nation and create a profound new sense of vulnerability." Risk, although sometimes not detected or recognized, is existent in every business. Thus, it is critical that enterprises have an effective risk management system to sustain the viability of commerce as we know it.

Risk management is a critical objective of Information Security Management Systems (ISMS) and it encompasses financial and operational exposure, data integrity and identification of and containment of

strategies for risk (Sherwood, Clark, & Lynas, 2005). Risk defines the possibility that an event will interfere with the achievement of a firm's objectives; as such, its proper mitigation requires risk awareness by top management, appraisal of a firm's tolerance, allowance for regulatory compliance demands, identifying exposure, and establishing responsibilities (Wilkin & Chenhall, 2010). The increasing dependence of business performance on information technology requires an impetus for proper ISMSs that can effectively manage the risk that exists from the operation of information technology.

Several legislative actions in the U.S. and across the world have been aimed to strengthen the information security management systems in publicly traded companies and other critical infrastructure companies such as the Cybersecurity Act of 2012 which aimed to mandate the sharing of information between government and businesses. Other legislature in the U.S. such as the Sarbanes-Oxley Act have inadvertently led to better internal controls by improving information for external stakeholders, identifying and rectifying control weaknesses in the reporting systems (Feng, Li, & McVay, 2009). While government legislates corporate governance laws, consumers and client businesses are seeking assurance that their vendors and partners have the proper controls and protections in place to safeguard information assets from security risks and are taking necessary measures to ensure business continuity (Saint-Germain, 2005). Guarantees aimed at increasing client and partner confidence can be obtained through security management certifications administered by third-party global inspectors. Among such standard certifications, ISO/IEC 27001, is a standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that is intended to bring a security framework under management control that can be subsequently audited and certified by a number of accredited registrars worldwide.

Enterprise System (ES) vendors also recognize the business need to provide a level of security trust to both clients and partners; as such, vendors market their software bundles highlighting key built-in features that serve as internal control components that are well adopted to a firm's functional structure. Such features are marketed to facilitate compliance with auditing standards such as SAS 94, titled "The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit", a norm published by the American Institute of Certified Public Accountants to provide

auditors with guidance on assessing the internal controls, with a focus on the increasing role of information technology on meeting financial reporting objectives. SAS 70, an auditing standard by the same international body, places similar emphasizes on ensuring auditors are able to assess the role of information technology in the internal controls of service organizations. Therefore, business integration of enterprise systems affects risks and internal controls, ideally, in a positive format.

1.2 Purpose

This dissertation will provide a comprehensive review of the research in the area of information security management systems conducted between 2000 and 2013. Subsequently, this manuscript will provide an analysis of the impact on risk, as perceived by external investors, upon the implementation of enterprise systems that contain built-in internal security controls. This manuscript will also assess the impact on perceived investor risk of enterprises that obtain information security management systems certifications recognized worldwide.

1.3 Motivating Applications and Research Questions

This dissertation is motivated by the inevitability that enterprises face the risk of security breaches and the necessity to assess adequate measures to mitigate the impact of such events. This collection of three essays will describe the most relevant academic contributions in the stream of information security management systems; and, it will explore the perceived risk-reduction effectiveness of two different signals that are disseminated by enterprises to provide investors with reassurances that the ISMSs in place are sufficient to minimize the risk associated with their enterprise. The application of three sets of research questions in the area of information security management systems are further described below.

1.3.1 Nomological Network Analysis of Information Security Management Systems Research

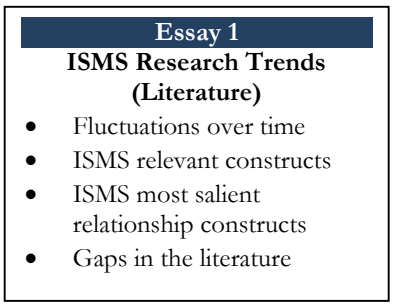

Figure 1.1 Purpose of Essay One

Information technology over the last century combined with information security breaches with massive losses has called for the better design, development and implementation of Information Security Management Systems (ISMS). The literature has not afforded a broad review of its contributions over time in spite of the critical importance of the subject matter. In order to effectively analyze the academic contributions over the last decade, it would be important to analyze the effect of the relationships among key factors, encapsulated in the literature in the form of constructs, to describe the contributions of the literature. To this effect, a global network analysis of the relationships between ISMS constructs allows the exploration of a multitude of relationships and their respective salience that would otherwise be ignored through a tunneled lens of a meta-analysis or an overly generalized thematic review of the literature. A nomological network analysis of research trends would collect hundreds of research literature into one dataset and inter-connect the constructs used in those different manuscripts. This would afford an opportunity to look at this network of relationships through several angles, enabling the subsequent focus on those relationships that have more network centrality power. Chapter 2 contains a study that borrows the constructs from previous contributions to conduct a nomological network analysis of the research trends in ISMS since the year 2000—offering an alternative methodology that is intended to advance the insight on the direction of this stream of research as well as to assist practitioners to easily identify relevant expertise drawn from applied science.

Through the review of a substantial part of the literature in ISMS, special focus is placed on the following research questions:

- Has ISMS research garnered increased academic attention in the last decade?
- What are the most salient ISMS construct relationships?
- Which ISMS constructs are most centric and relevant?
- Which referents are used for the top relevant constructs?
- Which ISMS constructs are most isolated and seem to merit further academic attention?

1.3.2 Impact of Enterprise System Implementations on Enterprise Risk

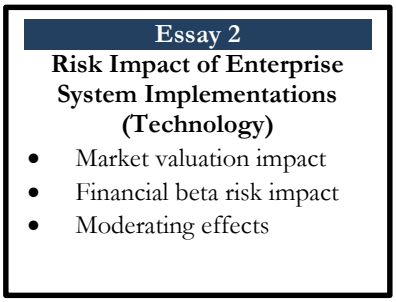

Figure 1.2 Purpose of Essay Two

Enterprise systems are integrated software packages that automate core corporate functions such as finance, human resources, and logistics. Organizations normally implement ERP systems to integrate their data flows and improve their business operations including supply chain management, inventory control, manufacturing scheduling and production, sales support, customer relationship management, financial, cost accounting and human resources (Hitt, Wu, & Xiaoge Zhou, 2002). In addition, enterprise systems can optimize the control of identity and access management. Industrial and professional reports often claim that the basic drivers motivating the adoption of enterprise systems include: cost reduction, improved efficiency, reduced product cycle time, improved customer service and satisfaction, the ability to change and configure business in response to changing market, and enabling e-commerce (Cao, Nicolaou, & Bhattacharya, 2010).

Enterprise systems, however, provide unique risk issues because of tightly interlinked business processes and customization through configuration choices and extensions from integrating enterprise systems with other applications. Key enterprise systems characteristics that impact security and internal control include degree of standardization, centralization, authorization and access to functions, as well as automation of controls versus existing internal control structure (Scapens & Jazayeri, 2003). An important research finding is that enterprise systems-based firms rarely determine the effectiveness of security and control by auditing system outputs (only 9 percent of firms). Rather, firms with enterprise systems predominantly used process audits (77 percent) and reviews of controls (95.5 percent) to ensure security

and controls (S. Wright & Wright, 2002). Managers point to the critical need for auditor involvement during the implementation process and user training to avoid errors, which rapidly proliferate through the system and then require extensive efforts of collaborative problem-solving to resolve (S. Wright & Wright, 2002).

Many issues remain, including how to evaluate the adequacy of existing enterprise systems internal control mechanisms; more importantly, is the perception of risk by external stakeholders influenced by a company's announcement that it has adopted an enterprise system that integrates internal security controls. Ultimately, signaling to external stakeholders that internal controls exist in a company is imperative to the development of trust with both clients and partners. Thus, the evaluation of perceived risks by investors would be a viable measurement of a company's risk status. Chapter 3 focuses on the analysis of the impact on investors' perception of risk, through market valuation and financial beta risk, the index measuring the volatility of an asset in relation to the overall financial market (Treynor, 1962), upon public announcement of the adoption of enterprise systems.

The following research questions are explored in this study:

- Does the adoption of enterprise systems result in an increase of market valuation for a publicly traded company?
- Does the adoption of enterprise systems result in a decrease of the financial risk of a publicly traded company?
- Which firm characteristics moderate the impact on enterprise risk?

1.3.3 Impact of IT Governance Certifications on Enterprise Risk

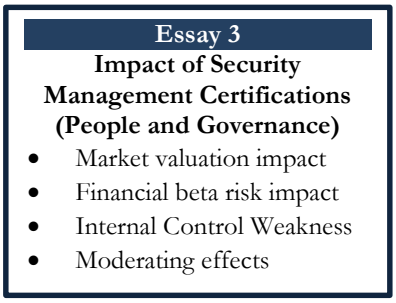

Figure 1.3 Purpose of Essay Three

Businesses all around the globe are increasingly concerned with the cyber risks that exist today given the advent of new technologies that are dependent on an interconnected world wide web. National efforts in the U.S. have aimed to monitor the increasing dependence on information technology through the enactment of legislative initiatives that create a partnerships between the public and private sector to protect enterprises. Post 9/11 efforts included the enactment of the Federal Information Security Management Act (FISMA), establishing comprehensive information security requirements for the federal government and contractors. In addition, the National Institute of Standards and Technology was made responsible for developing technology standards and compliance guidelines. As a result, NIST developed a broad risk-management framework (RMF) that would serve as a vehicle for federal agencies to use in building information security into an organization's infrastructure (Ross, 2007). NIST security standards and guidelines are developed through an open, public vetting process from both public and private stakeholders. While FISMA inducted the creation of key security standards and guidelines, e.g. FIPS 199 & 200, NIST publications 800-37, 800-53, 800-53a, 800-59 & 800-60, their efforts have expanded to address organizational issues, governance, and specific information asset protection.

Among such efforts, international standard ISO 17799 is one of the most prominent which established "guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization" (ISO/IEC, 2005). These authoritative statements aimed to provide best practices in information security and the procedures necessary to achieve information security in the modern organization. Since then, this norm has been revised to become ISO/IEC 27001:2013 (ISO/IEC, 2013), which is intended to provide control objectives to meet the requirements identified by a risk assessment, setting a common basis and practical guideline for developing organizational security standards and effective security management practices. Such practices are aimed to build confidence in inter-organizational activities, providing assurances to clients, suppliers and other stakeholder assurances of the organizational systemic systems to mitigate risks. Its companion standard, ISO 27001, specifies the requirements for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks" (ISO/IEC, 2013). Such standard is suitable to be

used by different types of organizations, and can be used by external agents as an auditing guide that lays out controls that an organization must address in order to obtain a certification of assurance.

Similar to ISO 27001, COBIT 4 (ITGI, 2007) is a normative framework for control and governance of information technology that is broader in scope and assess the degree of management direction for controlling the businesses IT processes, overall achievement and organizational goals. While both ISO 27001 and COBIT 4 both encompass the auditing aspects of ISMS, ISO 27001 focuses more on security and caters to mid-management implementations of an ISMS. COBIT 4 on the other hand, targets IT governance at the top-level needs of an enterprise. As a result, IS researchers have increased their research focus on information security governance (Debreceny, 2013). Given that ISMS aim to provide an organization with a coherent set of policies, processes and systems to manage information asset risks, ensuring acceptable levels of information security risk, the certification of such measures would signal external stakeholders that internal controls exist in a company. Thus, the evaluation of perceived risks by investors would be a viable measurement of a company's risk status upon obtaining an ISMS certification. Chapter 4 focuses on the analysis of the impact on investors' perception of risk, through market valuation and financial beta risk (the index measuring the volatility of an asset in relation to the overall financial market; Levinson; 2006), upon public announcement of the certification of such security certifications.

The following research questions are explored in this study:

- Does the external assurance of a company's ISMS result in an increase of market valuation for a publicly traded company?
- Does the external assurance of a company's ISMS result in a decrease of systematic risk for a publicly traded company?
- What ISMS characteristics moderate the impact on systematic risk?

1.4 Dissertation Organization

In this first chapter, I discuss the salient characteristics of information security management and the motivating research. The second chapter presents a nomological network analysis of research in the field of information security management systems. Given the interrelationship of technology, people and

governance, controls cannot be analyzed independently of the technology or its context of use. As such, this dissertation focuses on the impact of these two areas on financial and risk outcomes. Figure 1.4 and Figure 1.5 map the thesis model and structure, with their overall objectives. Chapter 3 presents the impact of public announcement of the adoption of enterprise systems on investors' perception of risk. Chapter 4 reviews the impact of security assurances on investors' perception of risk. Chapter 5 provides appendices and references relevant to this dissertation.

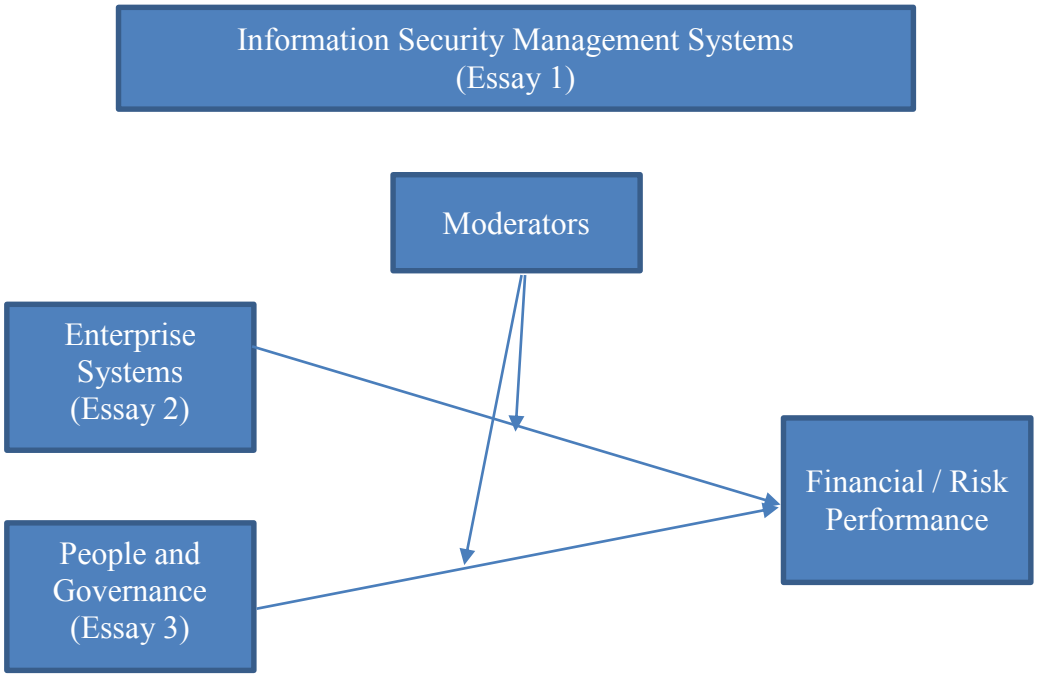

Figure 1.4 Dissertation Model

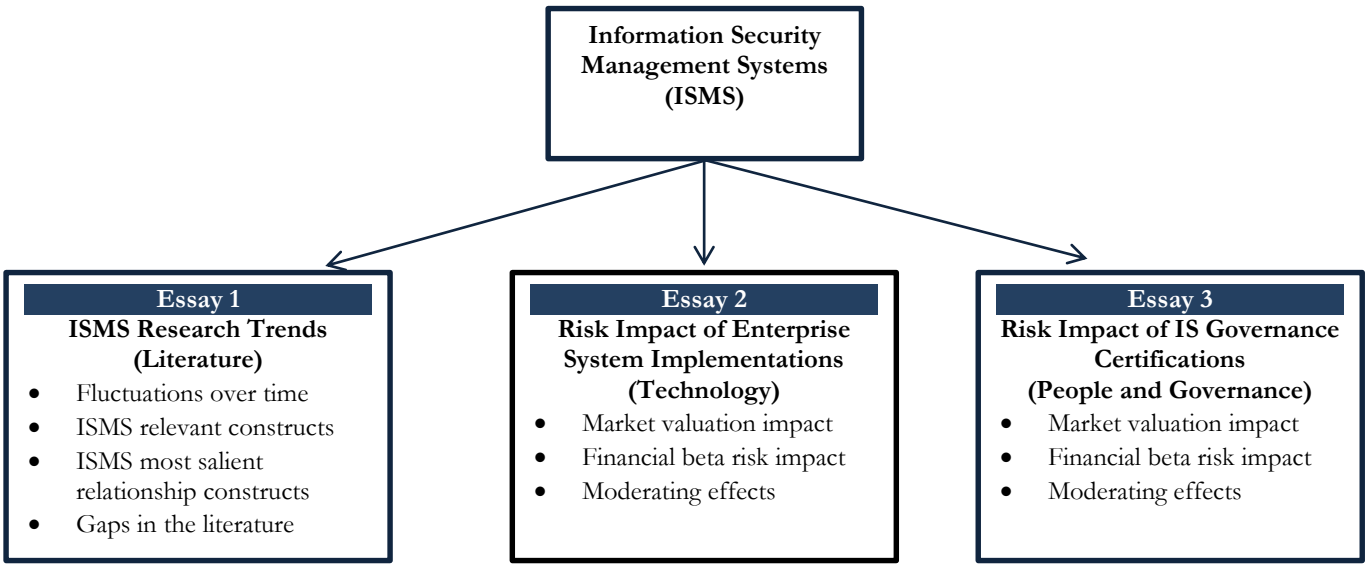

Figure 1.5 Dissertation Structure

CHAPTER 2 – A NOMOLOGICAL NETWORK ANALYSIS ON INFORMATION SECURITY MANAGEMENT SYSTEMS RESEARCH

2.1 Research Background

Information Security Management Systems (ISMS), as defined by the International Organization for Standardization in its 27001 standard, is a set of policies concerned with information security management with purpose of managing risk with the goal of implementing, monitoring, reviewing, maintaining and improving information security (ISO/IEC, 2013). More specifically, an ISMS encompasses "an organization's design, implementation and management of a coherent set of policies, processes and systems to manage risks to its information assets, ensuring acceptable levels of information security risk" (ISO/IEC, 2013). Basic concepts of security management have focused on setting the minimal security standards that are determined based on a classification level information sensitivity. Such measures are applied to technology, processes and people that have access to information objects.

Over the last century security policy models for accomplishing these goals included the Bell-La Padula model (Bell & LaPadula, 1973) and the lattice model (Denning & Denning, 1977) which focused on protecting information confidentiality. Other models such as the Biba model (Biba, 1977) focused on protecting the integrity of information in any organization. Under these basic models, information security policies are set forth by a priori classifications based on the security classification level of information objects. Contemporary approaches to security management expand on this approach and take risk management as a driving factor in setting up policies (Jaquith, 2007). As such, its requirements have a dynamic character that is influenced by risk assessment. This emerging concept of information security embodies a broader scope of information security policy that is interdependent with other management domains, such as institutional variables and environments.

While a myriad of relevant information security management driving issues have garnered increasingly important attention as they are streamed into the information systems literature, no specific research has been developed to summarize the trends in this field of research. In order to effectively analyze the academic contributions over the last decade it would be indispensable to analyze the effect of the relationships among key constructs to describe the most salient and trending contributions in the literature. This manuscript includes a network analysis of the relationships between ISMS constructs

allowing the exploration of a multitude of relationships and their respective salience by collecting hundreds of research articles into one dataset and subsequently interconnecting the constructs used in those manuscripts since the year 2000.

2.2 Development of Research Questions.

Recent drastic economic changes, dramatic institutional stability changes and revolutionary technology innovations, such as the emergence of the cloud, raise important issues that mandate a review of new contributions. While scholars have placed particular attention to several constructs related to the management of information security, the discipline is limited in scope at a minimum because it has not taken a broader approach in operational issues (Steinbart, Raschke, Gal, & Dilla, 2013). Most valuable research articles in this field have not described key ISMS construct interactions from a macro-to-micro level of approach; such contributions, like most research articles, concentrate on a set of narrow dynamics within this field. A broader picture of the literature is necessary to further advance any discipline (e.g. Parra, Han, Peters, & Vidyarthi, 2012; Parra, Kirs, & Udo, 2012); the application of such a broader analysis would offer an alternative methodology that is intended to advance the insight on the direction of this stream of research as well as assist practitioners to easily identify relevant expertise drawn from applied science.

Through the review of a substantial part of the literature in ISMS, focus is placed on the following research questions:

- Has ISMS research garnered increased academic attention in the last decade?
- What are the most salient ISMS construct relationships?
- Which ISMS constructs are most centric and relevant?
- Which referents are used for the top relevant constructs?
- Which ISMS constructs are most isolated and seem to merit further academic attention?

2.3 Justification for Nomological Network Analysis

2.3.1 Meta-analysis

As reviews are conducted to summarize contributions in the literature, scholars resort to a variety of techniques to effectively bring answers across diverse disciplines. Although the answers to research questions can normally be posited by single research articles, the resulting estimates of the effects of small samples sizes can often generate a statistical bias that is reduced with large-sample studies (Field & Gillett, 2010; Hunter & Schmidt, 2000). In addition, being able to replicate results is an important means of dealing with the possibility of measurement errors (Fisher, 1935). As different studies address the same research questions, it is possible to aggregate statistical information regarding the hypothesis testing of different studies through the use of a meta-analysis. Thus, a meta-analysis contrasts and combines results from different studies, with the aim of combining patterns and conflicts among those studies, by identifying and measuring the weighted average of a measure of the strength of any given phenomenon, defined as the effect size (Kelley & Preacher, 2012). Thus, a meta-analysis can provide a more statistically powerful estimate of the true effect size of a population. As more samples are aggregated into a meta-analysis, the mean and the variance of underlying population effects, the variability in effects across studies and the moderating variables become statistically stronger (Hunter & Schmidt, 2000). However, a meta-analysis is intended to provide a focused assessment of a particular relationship that has already been identified in the literature with the purpose of providing clarification to a conflicting set of results or to provide a robust, validated summary of previous findings (Hunter & Schmidt, 2000). While this is an effective tool to look for a particular research question, it requires the formulation of such questions before gathering the literature. This approach would narrow the scope of this study by limiting the research questions to only those that can be defined before conducting the literature search.

2.3.2 Thematic-review

A thematic review looks to stimulate and guide further research that will contribute to a research discipline by organizing an extensive range of previously published articles around general topics or issues. Unlike a meta-analysis, a thematic review summarizes the literature pinpointing, examining, and recording patterns or themes that are important to the description of a set of phenomena associated with

general specific questions (Guest, MacQueen, & Namey, 2011). Patterns found in the data are normally used as categories for analysis based on a general familiarization with the literature and a subsequent use of such categories to organize the literature. The codification of articles based on categories or themes can provide descriptive information regarding frequencies in categories, sources, theory, and other meaningful patterns. While thematic reviews tend to be useful in capturing the intricacies of meaning within a broad set of articles, most reviews experience a structural fallacy that originates from the coding of relevant manuscripts into "best fit" categorization, which forces manuscripts to be coded to specific themes, ignoring the possibility that manuscripts may be relevant to multiple themes. More importantly, given that certain themes may be interrelated in a complex manner, the non-granular analysis of articles ignores the specific dynamics of the interaction effects of the constructs within the analyzed articles. While it is useful to provide a broader picture of the literature, this approach would not be adequate for this study because it ignores the critical relevance of the interaction among relevant constructs across the literature. Thus, an alternative method is consequently proposed below.

2.3.3 A Nomological Network Analysis: between a meta-analysis and a thematic review

Using an a posteriori approach to analyze the contributions within a particular field of study would remove any prejudice that might otherwise be placed on the relevance of any themes. As described earlier, however, creating broad categories to codify contributions at the article-level would ignore the rich interactions that exist in multiple studies. Valuable alternative approaches in discovering interesting patterns on text documents have been offered by information systems scholars (Feldman & Dagan, 1995; Lent, Agrawal, & Srikant, 1997), such cataloging may be expanded by focusing on the interaction between constructs rather than individual constructs.

Cronbach and Meehl (1955) first contributed the idea of a nomological network in order to examine the construct validity of psychological measures. According to the authors, a nomological network consists of observable items, theoretical constructs, and the relationships between the theoretical constructs and the observable items. Most studies use a nomological network in order to test the validity of a construct within new scales; however, certain studies have used this concept to analyze relationships among constructs within specific topics (C. C. Chen, 2011; Le, Schmidt, Harter, & Lauver, 2010; Parra,

Han, et al., 2012; Parra, Kirs, et al., 2012). In essence, by using a nomological network analysis, patterns and trends can be analyzed at the construct level, rather than a manuscript level. A nomological network can serve as a unique dataset used to "explore construct relationships, their magnitudes and significances, and their positions in the network" (C. C. Chen, 2011). By aggregating a broad scope of literature that focuses on ISMS and using a nomological network analysis, this study navigates the complex interrelations between constructs. Thus, this study proposes an alternative and novel approach to analyzing such construct interaction through the use of a network analysis of such construct relationships, or dyads, across publications, time and journal tiers.

2.3.4 Nomological Network Analysis guidelines

Kenny, Kashy and Cook (2006) provide specific guidelines for dyadic data analysis, proposing the Actor-Partner Interdependence Model as the main method to analyze dyadic relationships. In this methodology, both members of a dyadic relationship are assumed to have actor and partner effects. It is essential to note that most research articles are derived from cross-sectional data; as such, it is appropriate for the dyads to lack an actor-partner effect direction. In undistinguishable models such as the case of constructs in this study, the partner and actor effects are assumed to be equal. Based on this premise, I propose to explain deeper phenomena patterns in previous literature by analyzing the prevailing relationships in the form of ties (relationships) of nodes (constructs) rather than the individual constructs themselves. This study borrows from Kenny et al.'s (2006) methodology in order to conduct an analysis as recently used in Parra et al.'s studies (Parra, Kirs, et al., 2012, 2012).

Short, Broberg, Cogliser and Brigham (Short, Broberg, Cogliser, & Brigham, 2010) highlight deficiencies in text-based content analysis studies that lack content validity and recommends that a researcher should use deductive content validity. Among the steps to avoid this issue and validate the use of content-analysis methodology, the authors suggest the following steps to conduct this type of analysis:

(1) Researchers should create a working definition of the constructs of interest using a priori theory when possible.

(2) An initial assessment of construct dimensionalities to properly relate constructs should be conducted.

(3) An exhaustive list of keywords should be developed, considering the proper terminology to relate constructs.

(4) Word lists should be validated using content experts to assess rater reliability, suggesting Holsti's (1969) method for assessing inter-rater reliabilities.

(5) Commonly used words from narrative texts should be identified as synonyms of constructs using available software packages and the previous steps should be repeated to validate them.

(6) Finally, the authors suggest the assessment of the terms' ability to predict theoretically related variables not captured via content analysis using regression or structural equation modeling.

2.4 Methodology

Observing these guidelines and advancing on previous academic studies (C. C. Chen, 2011; Cronbach & Meehl, 1955; Feldman & Dagan, 1995; Parra, Han, et al., 2012; Parra, Kirs, et al., 2012), the following major steps were thus conducted to address my research questions:

(1) the creation of a taxonomy of keywords into conglomerations of information security management systems' constructs using a priori theory and relevant ISMS literature;

(2) a systematic selection of articles that study information security management systems;

(3) an extraction of keywords provided by authors at the time of publication;

(4) identification of relationships among constructs for each article;

(5) highlight of relevant trending patterns through descriptive statistics and network analysis.

2.4.1 Identification of nomological constructs

Based on the recommendations of Short and colleagues (2010), an authoritative taxonomy of constructs was created by matching keywords as referrers of specific construct dimensions to define constructs of interest a priori. While no specific unified theory exists for ISMS, the following theories have been used to explain the underlying principles of ISMS (Hong, Chi, Chao, & Tang, 2006): Risk Management Theory (M. Wright, 1999), Control and Auditing Theory (Weber, 1998); Contingency Theory (Drazin & Ven, 1985). An excerpt of theories that are reported by the Association for Information Systems (Schneberger, Wade, Allen, Vance, & Eargle, 2013) as having been used in IS research were also

included (Alchian & Demsetz, 1996; Bandura, 1977; Coase, 1937; Compeau & Higgins, 1995; Selznick, 1948; Simon, 1959; Stoneburner, 2001). In addition, relevant constructs were also extracted from relevant literature on ISMS including ISO/IEC's 27000 series (ISO/IEC, 2013), COBIT (*COBIT 5: Enabling Information*, 2013) and SSAE 16 (AICPA, 2012). Table 2.1 provides an excerpt of the 230 a-priori nomological constructs offered by theory or relevant literature.

Table 2.1. Excerpt of theory-based constructs

Construct	Theoretical Grounding
Agency Theory (Alchian & Demsetz, 1996)	alignment of interests, contracts, efficiency, information asymmetry, moral hazard, risk sharing, successful contracting, trust
Behavioral Decision Theory (Simon, 1959)	biases, choice, cognitive processes, data completeness, decision processes, decision support, individual differences, inputs, judgmental heuristics, processing, risk assessment, strategy, tasks
Information Systems Control and Auditing Theory (Weber, 1998)	audit, controls, data resources, tests, effectiveness, efficiency, inputs, integrity, operations, processing, output, performance, processes, programming, quality assurance, safeguards, security management, systems development, top mgmt.
Risk Management Theory (M. Wright, 1999)	assessment, assets, awareness, compliance, controls, effectiveness, impacts, policies, risk assessment, risk management, safeguards, standards, threats, vulnerabilities
ISO/IEC 27000-Series (ISO/IEC, 2013),	acceptance, access controls, assets, audit, authorities, authorization, awareness, change management, compliance, confidentiality, continuity, coordination, impacts, cryptography, disciplinary, process, forensics, human resources, incident management, operations, policies, information classification, risk, redaction, monitoring, organization, measurements, organizational citizenship, physical security, tests, planning, processes, processing, property rights, regulations, training, response, responsibilities, risk assessment, risk factors, risk management, risk preference, safeguards, security failures, segregation of duties, stakeholders, third-parties, vulnerabilities

2.4.2 Systematic selection of sources for articles related to ISMS

Given the interdisciplinary nature of ISMS and the relatively scarce number of publications in the subject, the sources for articles were defined by selecting relevant national and international peer-reviewed journals in business management, information systems and security that were indexed by the major academic databases: Academic Search Complete, Psychology and Behavioral Sciences Collection, Business Source Complete and Inspec. In order to assess a journal's relative importance within its field, the average number of citations to its recent published articles was used as a proxy for relative ranking. SCImago' Journal Rank & Country Rank (SJR indicator) has been established as a reputable measure of scientific influence of scholarly contributions that is based on both the number of citations received by its publications as well as the level of prestige of the citing source.

In alignment with this study, the SJR indicator bases its algorithm on network analysis similar to the widely known algorithm Google PageRank, which bases its values for citations according to a journal's scientific influence. This approach uses a three-year citation window that sufficiently covers both the citation peak of a significant number of journals and reflects the dynamics of the scholarly communication process (González-Pereira, Guerrero-Bote, & Moya-Anegón, 2010). A total of 180 journals were ultimately selected as the target source for articles related to ISMS. All journals were ranked based on their SJR indicator for 2011. All journals were subsequently grouped into three tiers: Tier 1 journals had an SJR of 1.0 or above which indicate those journals which have the highest academic status based on the impact of their scholarly contributions; Tier 2 contained those with a lower SJR than 1.0; and, Tier 3 contained all those journals without an SJR indicator. Table 2.2 provides an excerpt of these selected sources.

Table 2.2. Journal Sources

Journal	SJR
Tier 1	
ACM Computing Surveys	9.93
ACM Transactions on Database Systems	4.20
Administrative Science Quarterly	5.65
IEEE Transactions on Industrial Electronics	3.12
IEEE Transactions on Software Engineering	3.29
Information Systems Research	3.65
Journal of the ACM	5.95
MIS Quarterly	5.14
Organization Science	5.47
Strategic Management Journal	5.22
Tier 2	
Behaviour & Information Technology	0.55
IBM Journal of Research & Development	0.59
Information Management & Computer Security	0.46
Information Technology & People	0.48
Journal of Computer Information Systems	0.52
Journal of Computer Sciences	0.52
Multimedia Tools & Applications	0.58
Technology Analysis & Strategic Management	0.55
Telecommunications Policy	0.59
Total Quality Management & Business Excellence	0.51
Tier 3	
Information Systems Security	-
International Journal of Computer and Network Security	-
Journal of Accountancy	-
Journal of Digital Forensics, Security & Law	-
Journal of Information Privacy and Security	-
Journal of Information Processing	-
Journal of Service Science	-
Journal of Strategic Security	-
Studia Informatica	-
Theoretical & Applied Economics	-

My selection of publication dates was motivated by the rise of prominent cyber security incidents beginning with the year 2000, the technology significant technological events of the last decade, and the intent to limit the scope to the most relevant research studies in this era. As such, a search for scholarly manuscripts was conducted ranging from January 2000 to May 2013 based on the following full-text phrases: "information security risk", "information security risk management", "information security management" and "information security management systems". The abstracts from the identified articles were examined to determine whether an ISMS theme was addressed by the study. Journal articles that were not peer-reviewed were excluded; several other articles were excluded on the basis of relevance or duplication across indexing databases. The search query yielded a total of 439 peer-reviewed articles pertaining to ISMS research within the specified range of dates.

2.4.3 Extraction of keywords and correlation to nomological constructs

Keywords provided by authors were extracted using the EBSCO Host digital librarian tool. These keywords were compared with original text for accuracy. Keywords were imported into a relational database that captured normalized information into different tables, including articles, keywords, constructs, theories, and journals.

Keywords extracted from research articles were analyzed for association with pre-defined constructs that were previously defined by theory and relevant literature. Specifically, a total of 2,815 keywords were examined to determine whether they matched a dimension of any ISMS construct, defined for purposes of this study as referents related to the behaviors, attitudes, outcomes, processes, experiences, manifestations and indicators connected with an organization's design, implementation and management of a coherent set of policies, processes and systems to manage risks to its information assets.

Holsti's (1969) method for assessing inter-rater reliabilities was used to validate the association of keywords and constructs. As different constructs emerged in the analysis of keywords, the list was revised by a committee of academic experts in this field of research; for disagreement in coding, a discussion was held to arrive to a consensus. If a keyword could refer to more than one construct, a group discussion was

held and the most relevant construct was used. Table 3 provides a representative sample of extracted keywords and how they were aligned to constructs.

Table 2.3. Keyword-Construct Correlation

Referents/Keywords (examples)	Construct
adoption, assimilation, adoption levels	Adoption
accreditation, assurance services, certification, certified organisations, certified security professionals	Assurances
confidentiality, data privacy, privacy, sensitive information	Confidentiality
corporate culture, cultural aspects, cultural differences, cultural dimensions, culture	Culture
security investment	IT investment
continuous improvement, six sigma (quality), quality management	Quality Assurance
risk analysis, risk assessment, risk forecasting, risk perception, risk quantification, risk assessment class	Risk Assessment

2.4.4 Identification of relationships among constructs for each article

Using a relational query that matched each article's keywords with a given construct, I obtained a dataset that resulted in a set of constructs for each article. In essence, upon alignment of keywords, each article was assigned the corresponding constructs. A small representative sample of articles and their respective constructs is shown in Table 4. Hovav and D'Arcy's (2012) research examined whether national culture influenced the "deterrent capabilities of security policies, security education, computer monitoring, and awareness programs" (p. 99). The article contained several keywords, some of them were aligned to the following specific constructs: culture, international environment, people, policies, security management, training, and value. Similarly, Mookerjee, Mookerjee, Bensoussan and Yue's (2011) contribution contained keywords that were aligned to security management, security failures, security, policies, people, organizational, behavior, industry, deviant behavior and assessment. Bodin, Gordon and Loeb (2008) contribution, included keywords that were aligned to security management, security, risk management, policies, information system types, industry and access controls. Therefore, a matrix for these articles would display an interconnected association amongst all constructs as displayed in Figure

1. Such matrix, contains crossover construct relationship between security, security management, policies, people, and industry. However, the most relevant relationship across all articles is security management and policies, which was addressed by the three articles. This processes is further detailed in the next section.

Table 2.4. Article Construct Relationships

Article	Construct Relationships
Hovav and D'Arcy (2012)	culture, environment-international, people, policies, security management, training, value
Mookerjee,Mookerjee,& Bensoussan (2011)	security management, security failures, security, policies, people, organizational behavior, industry, deviant behavior, assessment
Bodin, Gordon & Loeb (2008)	security management, security, risk management, policies, information system types, industry, access controls

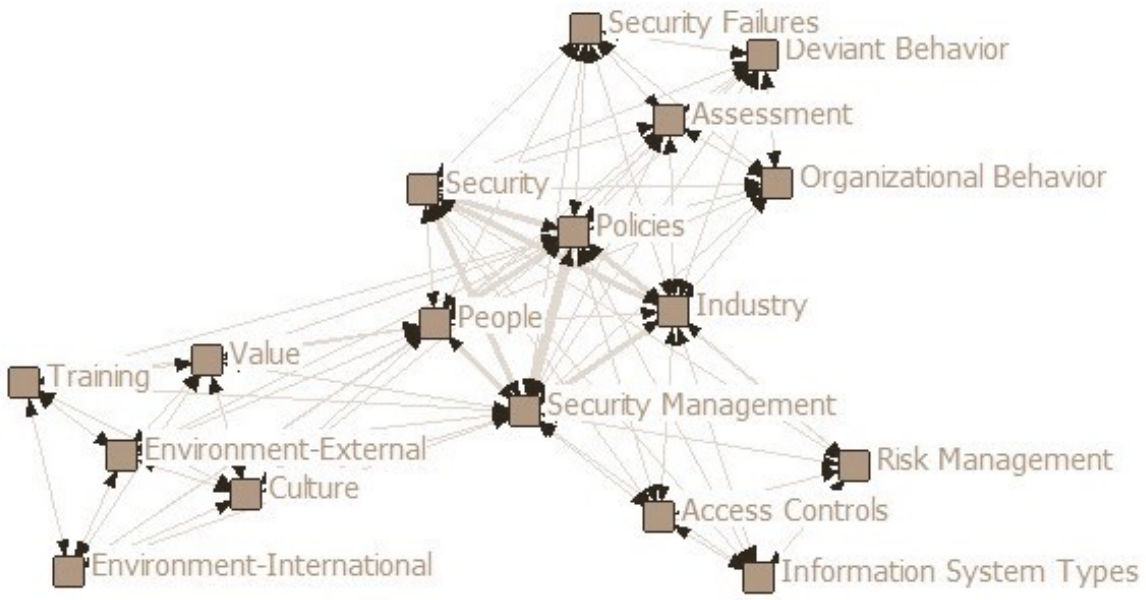

Figure 2.1 Sample construct matrix

2.4.5 Highlight of relevant trending patterns through descriptive statistics and network analysis

Various descriptive statistics are given based on the grouping by elements captured in the dataset including construct frequencies, authorship, and constructs. Given the network relationship approach of this study, I borrowed the methodology used by Parra et al. (2012; 2012) and Chen (2011), and constructed a matrix of the ISMS construct dyads. This social network is represented by dyad frequency observations. Using UCINET 6.0 software (Borgatti, Everett, & Freeman, 2002), four different types of analysis provided insight on the ISMS literature.

First, centrality measures were utilized to identify those constructs that have the most connections with other nodes. As described by Freeman (1978), the degree of centrality provides the sum of the values that a given node holds to its neighbors, a higher degree represents a more powerful influence. Similar to an individual in a social network with many connections or friends would be considered an influential person, a construct with a higher degree of centrality would be considered to affect ISMS phenomena because it has been studied more frequently with other constructs.

Second, a degree of betweenness was assessed to identify those constructs that are more critical in the literature. The degree of betweenness, also a measure of a node's centrality, was offered by Freeman (1978) to describe the number of shortest paths from all vertices to all others that pass through that node inside a network. Betweenness is a useful measure of both the load of importance of a node. The higher the degree of betweenness a node displays, the more critical it is in connecting other constructs because it plays a core position in the network (C. C. Chen, 2011). In a network of individuals, a person through which more individuals depend on in order to connect from one side of a network to another in the most efficient way, the more important it is. As such, a construct with higher betweenness would namely play a core position in ISMS research.

Finally, my study analyzed structural holes, or those within the network with missing links. This degree of structural deficiency may suggest a gap in the network, which in turn suggests that particular phenomena relationships might merit further exploration in the literature.

2.5 Results

To address whether ISMS research has garnered increased academic attention in this millennium, I first conducted a descriptive analysis which confirms a growing trend in the number of research studies conducted per year. Figure 2.2 summarizes this trend; and, it displays the proportional contribution of articles based on their tier. The trend exhibits a cumulative growth in publications over the last 12 years. While all tiers display a rise in the importance of ISMS phenomena, Tier 2 exhibits a higher linear slope of growth ($\beta_{Tier2} = 1.83$) followed by Tier 3 journals ($\beta_{Tier3} = 1.51$). Tier 1 Journals exhibit a moderate rise in attention ($\beta_{Tier1} = 0.43$).

Network analysis tools were utilized to address all other research questions. A total of 8116 unique construct dyads were incorporated in a network. Figure 2.3 displays a net diagram highlighting the most relevant construct relationships across the literature with bolder connections, weaker ties ($f < 4$) are not displayed to provide more visual clarity.

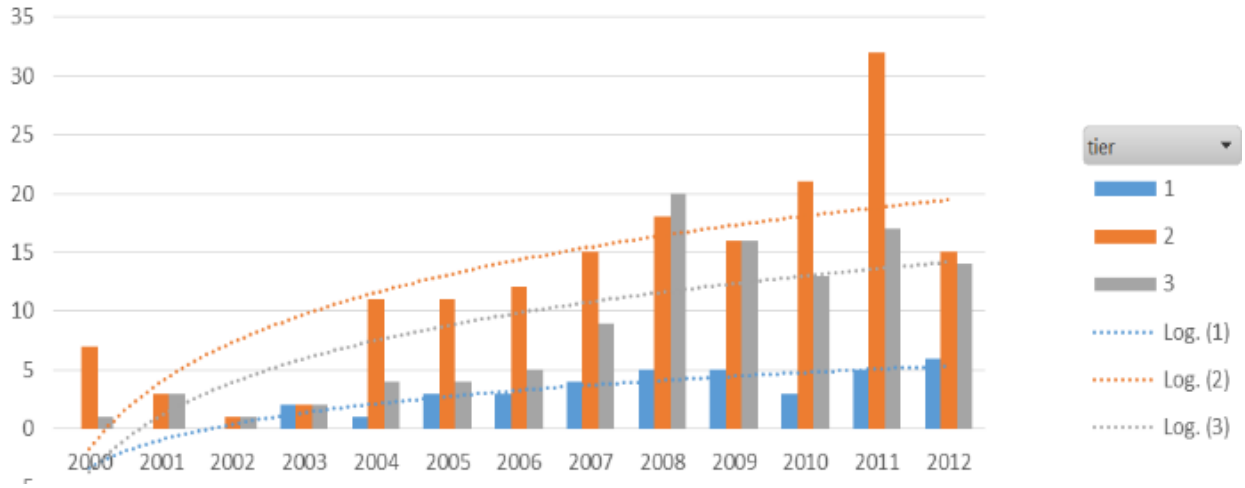

Figure 2.2 Publication trends by journal tier.

Figure 2.3. ISMS network diagram.

In order to underline the most salient ISMS construct relationships, I reviewed the full nomological matrix with an effect size of at least 23 ties. I found that the most relevant construct relationships are concentrated in the interaction of 14 different constructs highlighted in red (Figure 2.3). Such constructs have asymmetric interactions across this core network. Table 2.5 provides the 10 most salient ISMS construct relationships that have dominated the academic research interest in this millennium. Such interactions are further discussed in the next section.

Table 2.5. ISMS most salient relationships

Construct	Construct	Ties
Security	Information System Types	35
Security	Industry	30
Industry	Information System Types	26
Governance	Security	25
Information System Types	Risk Management	25
Policies	Security	22
Organizational Behavior	Security	22
Security	Resources	21
Security	Risk Management	20
Risk Management	Industry	18
Organizational Behavior	Information System Types	17
Security	Risk Assessment	17
Standards	Information System Types	17
Organizational Behavior	Industry	16
Security	Standards	16

To feature the ISMS constructs that have been more relevant, I utilized network centrality measures. Normalized degree of centrality measures reveal the constructs that are more relevant in ISMS due to the frequency in which they have been researched with other constructs. Betweenness measures reveal the constructs with a suggested core position in ISMS research. Table 2.6 displays the top 15 most relevant constructs and the top 15 which are suggested to have played a core position in research in this new millennium. In order to explicate these results, Table 2.7 provides an excerpt of the referents for the top 5 constructs, further expanding on the original research questions.

Table 2.6. Top constructs with centrality measures

Centrality	Betweenness
Information System Types (0.779)	Security (0.093)
Security (0.779)	Information System Types (0.089)
Governance (0.683)	Governance (0.051)
Information (0.683)	Risk Management (0.05)
Policies (0.683)	Risk Assessment (0.046)
Industry (0.625)	Policies (0.045)
Organizational Behavior (0.625)	Regulations (0.04)
Risk Management (0.625)	Information (0.039)
Risk Assessment (0.606)	Organizational Behavior (0.035)
Standards (0.587)	Industry (0.034)
Organization (0.567)	Standards (0.029)
Resources (0.548)	People (0.024)
People (0.51)	Organization (0.023)
Environment-International (0.481)	Resources (0.023)
Decision Processes (0.452)	Environment-International (0.016)

Table 2.7. Referents for top constructs

Construct	Referents
Security Management	computer security mgmt., information systems security mgmt., patch mgmt., power system protection, power system security, safety mgmt., security mgmt., security of data, security systems, optimal security mgmt.
Security	data protection, enterprise info. sec., data sec., computer network sec., cyber sec., computer sec., database sec., firewalls, industrial safety, sec., information sec., information systems sec., internal sec., IT sec., network sec., telecommunication sec.
Information System Types	applications, communication syst., client-server syst., courseware, decision support syst., document imaging syst., electronic syst., email syst., extranets, expert syst., medical syst., groupware, enterprise syst., intelligent syst., and 65 others.
Governance	I.S. governance, health care org. administration, I.S. management, ISMS, IT Governance, QA admin, organization and administration
Policies	measures, security policies, policy formation guidelines, economic policies, educational policies, incentive schemes, and 12 others

Finally, this study applied structure holes using effective sizes and efficiencies to explore the missing links in ego networks to identify the ISMS constructs that were most isolated and seem to merit further academic attention. Ego networks with a smaller efficiency value suggest there are more missing links. Table 2.8 provides the top 10 ISMS constructs which were found to have the most missing links in their structural network.

Table 2.8. Network structural gaps

Construct	Degree	Effect Size	Efficiency
IT Domains	11	1	0.091
Usage	11	1	0.091
Availability	10	1	0.1
Compatibility	9	1	0.111
Effort Expectancy	9	1	0.111
IT investment	9	1	0.111
Trust	10	1.2	0.12
Infrastructure	14	1.714	0.122
Requirements	14	1.714	0.122
Goals	8	1	0.125

2.6 Discussion

2.6.1 Summary of Findings

The main purpose of this study was to provide an examination of the relationships prevailing in the Information Security Management Systems literature published in the new millennium. The findings suggest that there has been a significant expansion in the research of ISMS-related phenomena. Such streams of research have been mainly focused around the interaction of different aspects of security management with risk management principles in a variety of security domains, but mainly in the following 10 areas: Security and Information System Types, Security and Industry, Industry and Information System Types, Governance and Security, Information System Types and Risk Management, Policies and Security, Organizational Behavior and Security, Security and Resources, Security and Risk Management, Risk

Management and Industry. Scholars have explored a variety of security management issues experienced in different industry settings and different types of information systems. Scholars have also focused on the organizational aspects and organizational standards as they relate to security management.

The findings highlight the most relevant constructs of the stream of research suggesting that security management and security issues are naturally the most relevant constructs. Interestingly, a variety of different system types were used in connection with ISMS studies, suggesting an attempt by scholars to duplicate findings in different application settings. Governance and policies, were also evidenced to be trending constructs in the literature. These findings should serve as a guide for those researchers that aim to provide a comprehensive summary of the literature organized around constructs and their interactions.

Security management issues still merit further discussion which will be evidenced by the future rise of related publications in the next decade. More importantly, my study suggests there is a need to further explore both threats and technology adoptions and their effects on ISMS. I further suggest that scholars should examine the value of ISMS-related investments; for example, the value of obtaining a third party ISMS assurance certifications or the risk mitigation value of implementing an enterprise system. Finally, my study also suggests that more research is needed in the human element of ISMS.

2.6.2 Limitations of Results

This study is limited by the accuracy of keywords provided by authors as construct referents. As such, it is possible that the keywords listed on each one of the articles might not sufficiently reflect all the constructs discussed in the underlying studies. Future studies may include a comparison of the validity of the methodology I offered with methods based on the manual extraction of constructs from the literature.

2.6.3 Conclusion

The overall results provide an extensive mining database that may be dissected and aggregated in multiple dimensions to provide further insight of this global phenomenon. Future research should expand on this study and include a literature review of those salient relationships and the intricacies identified through the analysis described herewith. Given the recent contributions to these areas, it would be prudent to organize such knowledge for practitioners and scholars alike. The trends identified through this study will emphasize the critical influence of certain constructs. The results expand on previous research

contributions by displaying the interaction of constructs across the literature. Future research should expand on the specific areas highlighted by the results of this study to advance the insight on the direction of this stream of research as well as to assist practitioners to easily identify relevant expertise drawn from applied science.

CHAPTER 3 – IMPACT OF ENTERPRISE SYSTEM IMPLEMENTATIONS ON A FIRMS'S SYSTEMATIC RISK

3.1 Research Background

Today's business environment is complex, volatile, and exposed to substantial global risks that consistently affect the day-to-day operations and decision making process of any organization. Given the increasing complexity of most markets, in addition to the increasing dependence on digital information, risk mitigation can no longer limited to uncoordinated efforts surrounding core business functions. Isolated compliance, valid internal controls and risk-transfer practices can no longer protect an enterprise from today's real market risks. Instead, businesses must transform traditional procedures into strategic, enterprise-wide, risk management methodologies that identify, manage, and minimize risks in order to ensure business success and continuity.

Enterprise systems are integrated software packages that automate core business functions such as finance, human resources, and logistics. Organizations normally implement enterprise systems to integrate their data flows and improve their business operations, including supply chain management, sales support, customer relationship management, inventory control, manufacturing scheduling and production, financial and cost accounting, human resources (Hitt et al., 2002). Enterprise systems can also optimize the control of identity and access management. Industrial and professional reports often claim that the basic drivers motivating the adoption of enterprise systems include: improved customer service and satisfaction, cost reduction, improved efficiency, reduced product cycle time, the ability to change and configure business in response to changing market, and enabling e-commerce (Cao et al., 2010). More complex motivations include better regulatory compliance, business process reengineering, integration of operations and management decision support (Robey, Ross, & Boudreau, 2002) as well as the goals of creating lasting shareholder value and safeguarding the organization from the consequences of information system disasters (Debreceny, 2013; Parent & Reich, 2009).

The use of such sophisticated software systems compels changes in the underlying processing, leading to reengineering efficiency improvements that are normally compounded by the benefits of automation. Enterprise systems, however, present unique risk issues because of tightly interlinked business processes and customization through configuration choices and extensions from integrating

enterprise systems with other applications. As organizations integrate their data flows and improve their business operations and decision making process, organizations face a unique set of new risk components derived from the tightly-linked interdependencies of business processes (M.-K. Chang, Cheung, Cheng, & Yeung, 2008) and the possibility of implementation failure (Ngai, Law, & Wat, 2008). On the other hand, it also presents a distinctive opportunity for the integration of enterprise-wide risk management efforts that support internal control processes (Debreceny, 2013; Parent & Reich, 2009; S. Wright & Wright, 2002). Key enterprise systems characteristics that impact security and internal controls include degree of standardization, centralization, authorization, and access to functions, as well as automation of controls versus existing internal control structure (Scapens & Jazayeri, 2003). Earlier studies suggest that enterprise systems impact an organization's management control systems by increasing the centralization of system coordination and homogenization of control practices (Granlund & Malmi, 2002; Kallunki, Laitinen, & Silvola, 2011); and, it is further suggested that firms that have implemented enterprise system are less likely to report internal control weaknesses than those firms without such enterprise technology (Morris, 2011). Based on the well-established premise that enterprise systems can provide organizations with competitive advantages through improved operational, tactical and strategic business performance (Chand, Hachey, Hunton, Owhoso, & Vasudevan, 2005; Dehning, Richardson, & Zmud, 2007; Gefen, 2005; Häkkinen & Hilmola, 2008; Hayes, Hunton, & Reck, 2001; Hunton, Lippincott, & Reck, 2003; Nicolaou, 2004; Nicolaou & Bhattacharya, 2006), publicly-traded company investors have been demonstrated to react positively to enterprise system implementation announcements (Hayes et al., 2001; Hendricks, Singhal, & Stratman, 2007; Hitt et al., 2002; Wier, Hunton, & HassabElnaby, 2007). Furthermore, the market has been demonstrated to award enterprise system investments even further upon full implementation, reflecting an inherent stock discount due to the existence of substantial enterprise risks that are eventually outperformed by the benefits of this technology (Hitt et al., 2002).

3.2 Research Purpose

More than a decade of transformational software development and implementation improvements have taken place since most of these studies were conducted, possibly undermining the authority of previous findings. In addition, over the last decade, U.S. legislative changes have significantly increased

the disclosure requirements regarding publicly-traded companies' internal material weaknesses, providing a significant factor in a company's market-adjusted cost of equity and information risks (Ashbaugh-Skaife, Collins, Kinney Jr, & Lafond, 2009). Given the current dialogue in the literature surrounding the impact of enterprise system implementations on risk mitigation in addition to this decade's technology and regulatory developments, this study aims to examine enterprise risk net-effects caused by the changes in the interdependencies in business process and internal controls caused by such implementations. Although both internal and external methods have been offered by the literature to evaluate the value of technology, studies suggest that the relationship between technology investment and financial performance is "marginally, but significantly, stronger in studies that employ market measures rather than accounting measures of financial performance" (Lim, Dehning, Richardson, & Smith, 2011). Thus, the evaluation of perceived risks by market measures would be a viable measurement of a company's risk status. This study explores the impact on the perception of risk by external stakeholders. The rest of this study is organized as follows: a summary of the literature is presented on the business value and risk of enterprise systems; a theory-based research model is offered; proposed hypotheses are developed; the methodology is detailed; and, results are offered followed by the study's contributions and suggestions for future research.

3.3 Business Value of Enterprise Systems

Enterprise systems became prevalent in the 1990s as a means to provide integration and functionality across multi-functional organizations (Holland & Light, 2001). Within the last two decades, such systems have injected innovation that has propelled them with the capacity to support higher level decision-making and business intelligence. Their complexity, however, has led to a varying degree of cost, scope and benefit (Gattiker & Goodhue; 2000). The literature that examines the value of information systems highlights both, diverse performance measures including productivity, profitability, cost reduction, competitive performance and market valuation, (Melville, Kraemer, & Gurbaxani, 2004), as well as the intangible, capability-building value that drives better business processes and business performance (e.g. Kohli & Grover, 2008). Studies addressing the specific business value of enterprise system are guided by such prior research. Su and Yang (2010) organize enterprise system benefits into

three main categories: operational, which include the benefits experienced as a result from the cross-functional processing, the effective planning and management of resources, and the assessment of financial performance of products and services; business processes and management (tactical), which reflect the business processes improvements that lead to improved customer satisfaction, responsiveness, and improved decision making; and, strategic benefits, which focus on increasing a firm's competency and knowledge.

Table 3.1 provides a summary of the most relevant research articles that assess the value of enterprise systems with a diverse set of performance variables and research methods.

Table 3.1. Summary of Literature on Value of Enterprise Systems

Research	Description	Findings
(Baskerville, Pawlowski, & McLean, 2000)	Assesses impact of ES on organizational knowledge	ES make business knowledge become convergent from the perspective of the organization and divergent from the perspective of the individual.
(Becker, Greve, & Albers, 2009)	CRM process-related performance. Offers performance measures. Proposes a conceptual model linking tech & org. implementation	Implementations affect initiation and maintenance performance, which is moderated by its users' support. Interaction of organizational implementation and management support has a significant effect on initiation performance only.
(Bose, Pal, & Ye, 2008)	Impact of integration of SCM and ERP system	The e-SCM transformed processes at firm's manufacturing facilities provided real time inventory information update, better picking activities, and establishment of effective collaboration with vendors and customer. Reduction in lost sales and inventory.
(Chand et al., 2005)	ERP Scorecard to evaluate ERP system's strategic contributions.	ERP scorecard to assess ERP impact on firm's automation, knowledge and innovation at different stages. ERP system impacts a firm's business objectives. Study provides a new ERP framework for valuing the strategic impacts of ERP systems.
(Cotteleer & Bendoly, 2006)	ES impact on operational performance, focusing on changes in process dynamics	ERP supports significantly reduced order lead times; and, more efficient production flow.
(Dehning et al., 2007)	Financial benefits of investments around newly adopted IT-based supply chain management systems	SCM systems increase inventory turnover, market share, gross margin, return on sales, and reduce selling, general, and administrative expenses. Process improvements around supply chain initiatives combine to improve overall performance. Industry and scope of ES moderate financial performance.
(Gefen, 2005)	Examines business characteristics of manufacturing firms and their perceived benefits from ERP system investments.	Business characteristics explain can explain assessed value of an ERP system at the module level (40%) and overall system level (6.9 – 11.5%).
(Häkkinen & Hilmola, 2008)	Takes a longitudinal view (at 0 & 2 years) of the use and evaluation of an ERP system.	Poorest ERP assessments were given early during shakedown phase but problems existed after 2 years. Assessments depended on user type and the business processes in which they participated.

(Hayes et al., 2001)	Examines market response to firm announcements of enterprise resource planning (ERP) system implementations.	The market react significantly and positively to the ERP announcements, moderated by a firm's health/size characteristics. Announcements involving large ERP vendors were significantly more positive than others
(Hendricks et al., 2007)	The effect of enterprise systems investments on stock price and profitability.	ERP systems exhibit improvements in profitability, but not in stock returns. Profitability is stronger for early adopters. Over the five-year period, stock price performance is no different than control group. SCM: positive abnormal stock price performance; improvements in ROA and ROS. CRM had little effect on the stock returns, ROA and ROS are generally positive but combined periods are statistically insignificant
(Hitt et al., 2002)	The benefits of ERP implementation versus costs and risks. Examine adoption decision and the extent of adoption by examining which modules were implemented	ERP systems can provide the organization with competitive advantage through improved business performance; Investors award implementations on completion, reflecting the existence of a substantial, but not overwhelming, risk of implementation. Greater use of ERP components is associated with higher performance, but the higher level implementations may result in diseconomies of scale. Adoption risks do not exceed the expected value.
(Hunton et al., 2003)	Longitudinal impact of ERP adoption on firm performance by peer-matching non-adopters.	Greater firm performance for adopters based on ROA, ATO, and ROI. Large/unhealthy adopters experience better ROI than large/healthy adopters given efficiency and effectiveness gain potential. Small/healthy firms can anticipate greater future benefit from ERP adoption than small/unhealthy firms given potential growth results.
(Madapusi & D'Souza, 2012)	Investigates ERP system implementation by analyzing each system module's influence on operational performance as well as its implementation status.	Implementation status of the ERP system increases, operational performance is significantly influenced. Certain modules (Financials, Controlling, Production, Logistics, Plant Maintenance, Quality Mgmt., Planning) were significantly correlated to increases in performance measures. Quality Mgmt. only module that impacts all.
(Nicolaou, 2004)	Long-term adoption and use of ERP relationship to firm's financial performance.	Firms who adopted ERP systems exhibited higher differential performance after 2 Years. Implementing a system from a larger vendor, having system-led objectives, and implementing a specific type of module, enhanced a firm's financial performance.
(Nicolaou & Bhattacharya, 2006)	Examines impact on firms' ability to deliver long-run financial performance based on changes to ERP systems over a post-implementation time-frame.	ERP-adopting firms, with timely add-ons and updates enjoy superior financial performance. Late enhancements and abandonments lead to financial performance deterioration for those firms.
(Poston & Grabski, 2001)	Examines ERP's impact on long term firm performance.	COGS, Labor Force benefits, No SG&A benefits or Residual Income.
(Roztocki & Weistroffer, 2009)	Examined market reaction to both ERP & enterprise application integration announcements across markets (bull and bear) & firm financials.	Financial markets differentiate among technologies in which companies invest to integrate their information systems. Influential factors include technology maturity, financial health of the investing company, & stock market conditions.
(Su & Yang, 2010)	Examines the impacts of the ERP benefits on SCM competencies through a proposed conceptual framework	Operational process competencies are positively impacted by operational, managerial, and strategic benefits of ERP. SCM planning and control process competencies are positively impacted by the operational, managerial, and strategic benefits of ERP. Managerial and strategic benefits of ERP have the most impact on SCM competencies.
(Wier et al., 2007)	Links ERP adoption market returns with non-financial performance incentives in executive compensation.	Firms with both non-financial performance incentives & ERP obtained significantly higher short-term & long-term ROA and stock returns than either of these single conditions. Used theory base of cybernetic control theory and agency theory.

3.4 Enterprise Systems, Internal Controls and Risk

Businesses across the globe are faced with a variety of events that have the potential of creating business losses that may range from project failures on the lower end, to the complete disruption of a company's operations and the ultimate obliteration of a company. The auditing community has established three different categories of risks: business interruption risks, which refer to the likelihood that endogenous or exogenous factors will disrupt a company's ability to timely process transactions, process interdependency risks, which refer to those risks arising from the transit of information from one process to another; and system security risks, which are based on the organizational behavior or external mischief (Hunt et al., 2004) and can be further segmented into the classical CIA Framework (ISO/IEC, 2013). While business interruption risks are considered to be inherent to any business, both process interdependency and system security risks are considered risks that can be controlled with policies, procedures and information tools that may mitigate their damage.

A holistic approach toward managing such organization's risk, commonly known as enterprise risk management (ERM), is suggested to improve an organization's performance contingent upon the appropriate match with its contextual variables specific to each organization (Gordon, Loeb, & Tseng, 2009). Authors suggest ERM efforts benefit firms by decreasing volatility in earnings and stock prices, decreasing external capital costs and increasing capital efficiency (Gordon et al., 2009; Hoyt & Liebenberg, 2011; Nocco & Stulz, 2006). As enterprise systems continue to interlace with broader, enterprise-wide operations, decision management and internal controls, they often interact and impact an organization's ERM efforts. These systems share data across functional divisions and hierarchy levels which can be turned into valuable information for an organization's decision making, intelligence and risk management capability goals. As such, the operational uncertainties derived from non-standard processes and lack of access on a real-time basis to relevant information can be minimized by the proper data exploitation strategies (Mathrani & Mathrani, 2013). Enterprise systems can thus be critical to improve the organization's knowledge and its ability to make more informed decisions (Grabski, Leech, & Schmidt, 2011). The very same nature of enterprise systems that may systematically align them to monitor and mitigate risks at an enterprise level, also makes them unique to challenges beyond the scope of project failure, that rise from the integration of external consultants, simultaneous integration and reengineering

of processes (Grabski et al., 2011; Somers, Nelson, & Sprague, 2001). The interdependency of business processes may very well heighten the potential risk of financial misstatements and defalcations (S. Wright & Wright, 2002).

As summarized by Table 3.2, a scholarly focus has recently emerged on examining the impact of enterprise systems on organizational controls and risks that go beyond the scope of assessing potential implementation failures and critical success factors. Such studies have yielded mixed results. Enterprise systems are posited to permit the standardized control of user knowledge, role and system privileges, improving information quality (Häkkinen & Hilmola, 2008), management controls (Chapman & Kihn, 2009; Elmes, Strong, & Volkoff, 2005; Kallunki et al., 2011), accessibility to continuous auditing (S.-I. Chang, Wu, & Chang, 2008; Kuhn Jr. & Sutton, 2010) and financial reporting controls (Mundy & Owen, 2013). However, opposing evidence also suggests that enterprise systems do not materialize in more effective internal controls (Granlund & Malmi, 2002), even suggesting that the increased forecasting capacity from the systems may lead to manipulation of earnings forecast disclosures (Brazel & Dang, 2008). O'Leary (2000) suggest that the degree of improved management controls may be attributed to whether a system is initially configured to provide such benefits, citing the circumvention and override of controls often due to implementation timeline demands. As such, enterprise systems may allow the unfettered access to information and processes if controls are not set in place (Grabski et al., 2011).

Regulatory requirements that compel companies to reduce enterprise risk by providing stronger internal controls and information systems security (e.g. Sabanes-Oxley Act, Health Insurance Portability and Accountability Act) have opened an opportunity for vendors to respond with enhanced audit modules and continuous audit support. Notable trends in risk management and regulatory research explore the role of enterprise systems play in reducing risk by supporting compliance (Grabski et al., 2011; Maurizio, Girolami, & Jones, 2007; Mundy & Owen, 2013). Multinational corporations are subjected to an expanded set of regulations, making this area of research even more relevant. Nonetheless, security risks continue to be prevalent due to the interconnectivity, integration, and automation of business processes, whereby a single user may be able to trigger enterprise-wide reactions in both data and processes (Ko Hsu, Sylvestre, & Sayed, 2006). In addition to control elements that affect enterprise risks, such as centralization, authori-

Table 3.2. Summary of Literature on Enterprise Systems, Internal Controls and Risks

Research	Description	Findings	Controls	Risks
Aloini, Dulmin, & Mininno (2007)	Examine the organizational relevance and risk of ERP implementation projects, highlighting the key risk factors and their impact on project success.	Most risk factors occur early and have a pervasive impact during all the ERP project life cycle.		+
Brazel & Dang (2008)	Investigate impact of ES on manage earnings management and release dates.	ES increase the extent of earnings management.	- , +	
Chang, Wu, & Chang (2008)	Explores the crucial control items of the purchasing and expenditure cycle in meeting the SOX 404 conditions and develops a computer auditing system based on SOX 404.	ERP-based systems may comply with SOX 404 requirements, improve correctness of auditing activities, and increase the reliability of the company's investment and management environment.	+	
Dechow & Mouritsen (2005)	Analyses the integration of management and control through ERP systems	ERPs incur a *techno-logic* that conditions how control can be performed through financial and non-financial representations, as they differentiate between an accounting mode and a logistics mode.	+ , -	
Dewan & Ren (2007)	Examines wealth and risk effects associated with electronic commerce announcements (not exclusive to ES).	Wealth effects were found to be not significant after controlling for contemporaneous risk changes. Significant economic events can affect more than the mean of the returns distribution, omitting other effect factors can result in biased estimates of wealth effects.		+
Dewan & Ren (2011)	Investigated the impact of IT investments (not exclusive to ES) on firm return and risk financial performance. Focused on the moderating role of firm boundary strategies of diversification and vertical integration.	Boundary strategies significantly moderate the impact of IT investments on firm risk and return performance. Studies should consider both, value and risk, on measuring IT impact on firm performance.		+
Dorantes, Li, Peters, & Richardson (2013)	Examines ES impact on quality management earnings forecasts.	ES positively associated with accuracy of management earnings forecasts based on better access to decision-relevant internal information.		-
Elmes, Strong, Volkoff (2005)	Explore the ES-enabled changes in organizational control that emerge after implementation.	ES enhances organizational control and employee empowerment through access to information.	+	
Grabski, Leech, & Schmidt (2011)	Review ERP literature contributions, including risk.	ES ability to impact business risks and regulatory compliance is evident, impact on management control must be further explored	+ , -	+ , -
Granlund & Malmi (2002)	Explores the effects of integrated, enterprise-wide information systems on management accounting and control systems.	No significant direct or indirect impact at the time on management accounting or management control systems of a firm.	ns	
Hunton, Wright, & Wright (2004)	Examines the extent of heightened risks associated by ERPs in the presence of weak controls as perceived by auditors.	Suggests that financial auditors may be overconfident in their ability to assess ERP system risks, given the significantly higher business interruption, process interdependency, and overall control risks with the ERP, as otherwise perceived by IT auditors.		+

Kallunki, Laitinen, & Silvola (2011)	Explores the effects of enterprise system adoptions on non-financial and financial performance based on the role of formal and informal management control systems as mechanisms as mediating factors.	The use of enterprise systems results in improved firm performance in the long run. Formal rather than informal management controls help firms achieve future performance goals.	+	-
Kobelsky, Hunter, & Richardson (2008)	Investigates the impact of IT investments and firm's contextual variables on the volatility of future earnings	IT investments increase the volatility of future earnings, moderated by sales growth (amplifies), unrelated diversification (reduces), and firm size (reduces).		+ , -
Kuhn & Sutton (2010)	focus on current technological options and ERP structures for continuous assurance models	Highlights ES ability to improve internal controls through continuous audits based on embedded audit modules or monitoring control layers	+	
Mathrani & Mathrani (2013)	investigates how ES data were transformed into knowledge and how this knowledge was used to manage risks by utilizing an ES data	ES data transformation process resulted from knowledge-leveraging actions at both executive and operational levels, reducing operational risks		-
Maurizio, Girolami, Jones (2007)	Reviews factors and methods used to integrate multiple ERP systems to comply with SOX in an enterprise application integration environment	Compliance with SOX in ERPs requires the use of EAI. Recommendations are made to the ERP environment at the time to ensure compliance	+	
Morris (2011)	Examines the impact of ERP systems on the effectiveness of internal controls over financial reporting	ERP-implementing firms are less likely to report material weaknesses, after controlling for other ICW-contributing variables.	+	-
Morris and Laksmana (2010)	Examines the impact of ERP systems on earnings management.	ES reduce earnings management	+	
Mundy & Owen (2013)	Investigates ERP"s role in facilitating control over reporting processes, thereby ensuring compliance with regulatory requirements	ERPs can be used in a number of ways to establish and maintain internal control processes over financial reporting. Use of case study vendor could increase the confidence of SOX auditors in a company's IT processes	+	
Roztocki & Weistroffer (2009)	Examines market reaction to public announcements of enterprise application integration (EAI) investments	Resulting changes in stock prices are insignificant suggesting investors largely ignore announcements of EAI investments	n/s	
Rubin & Rubin (2013)	Examines business intelligence systems reduction of stock return volatility.	Significant reduction in stock return volatility subsequent to BI deployment, reducing the financial risk of an organization.		-
Sia, Tang, Soh, & Boh (2002)	Examines ES implications on traditional power distribution in an organization	ES have potential of imposing organizational control manifested at the business process level, moderated by formative contexts and distribution of authority	+	
Stratopoulos, Vance, & Zou (2013)	Examines ES forecasting tools impact on manager's decision to manipulate reported performance	Managers may be encouraged to manipulate reported performance by using smaller magnitude adjustments in cases of impending shortfalls unless a significant internal control strengths are instituted with the ES		+
Wright & Wright (2002)	Examines the unique risks associated with the implementation and operation of ES systems	ES increase the potential for control weaknesses, financial statement errors or inaccurate internal information		+

zation levels, automation of controls (Hunton, Wright, & Wright, 2004; Scapens & Jazayeri, 2003), studies have shown enterprise systems can provide managers with the ability to manipulate reported performance by using smaller magnitude adjustments in cases of impending shortfalls unless a significant internal control strengths are instituted (Stratopoulos, Vance, & Zou, 2013), increase the potential for control weaknesses (S. Wright & Wright, 2002) or fail to provide separation of duties if inappropriately configured (McCollum, Lightle, & Vallario, 2003). In comparing risk assessments performed by IT auditors versus financial auditors, Hunton and colleagues (Hunton et al., 2004) suggest that both auditors "indicate significantly higher business interruption, process interdependency and overall control risks" (p. 7) with enterprise systems in comparison to legacy systems; and, IT auditors recognize significantly higher network, database and application security risks while financial auditors do not, suggesting that financial auditors may fail to adequately assess the appropriate degree of risk of those companies using enterprise systems.

Yet, other studies strongly suggest that enterprise systems changes an organization generating knowledge-leveraging actions at both executive and operational levels that reduce operational risks (Mathrani & Mathrani, 2013). After controlling for variables that usually contribute to internal control weaknesses, Morris (2011) suggests firms are less likely to report material weaknesses after implementing an enterprise system. Dorantes el alia (2013) suggest that enterprise systems can provide managers with enhanced accuracy of management earnings forecasts based on better access to decision-relevant internal information. Even if a previous study can be used to manipulate earnings reports (Brazel & Dang, 2008), others studies find contradictory evidence in that regard (Dorantes et al., 2013; Morris & Laksmana, 2010). Studies also suggest that the cited risks associated with enterprise systems exhibited across life cycles are predominantly manifested only in those organizations that exhibit issues during the early stages of implementation, citing lack of organizational readiness (Aloini, Dulmin, & Mininno, 2007). Combined with formal management controls, enterprise systems have also been evidenced to improve firm performance and reduce risks (Kallunki et al., 2011).

Furthermore, enterprise system vendors have also evolved tremendously in the last decade, providing additional access control, compliance auditing and risk management modules that respond to

their clients' evolving security and regulatory compliance needs (Grabski et al., 2011). In addition to evidentiary support of risk mitigation, compliance and internal control benefits, the literature is abundant with support of operational (Cotteleer & Bendoly, 2006; Dehning et al., 2007; Hunton et al., 2003; Madapusi & D'Souza, 2012; Poston & Grabski, 2001; Su & Yang, 2010), tactical (Bose et al., 2008; Dehning et al., 2007; Madapusi & D'Souza, 2012; Su & Yang, 2010), strategic (Chand et al., 2005; Su & Yang, 2010) and financial performance benefits (Hendricks et al., 2007; Hunton et al., 2003; Nicolaou, 2004; Wier et al., 2007).

Although both internal and external methods have been offered by the literature to evaluate the value of technology, studies suggest that the relationship between technology investment and financial performance is "marginally, but significantly, stronger in studies that employ market measures rather than accounting measures of financial performance" (Lim, Dehning, Richardson, & Smith, 2011). Thus, the evaluation of perceived risks by market measures would be a viable measurement of a company's risk status. To this effect, studies have shown stock market reaction to implementations of enterprise systems with mixed results (Hayes et al., 2001; Hendricks et al., 2007; Roztocki & Weistroffer, 2009; Rubin & Rubin, 2013). While other research on the effect of IT investments on stock prices have been intensively researched, studies on the effects of volatility have only recently emerged(Rubin & Rubin, 2013). For the exception of Rubin and Rubin (2013)'s study, these studies have focused mainly on abnormal stock returns, not financial risk. Furthermore, as suggested by Dewan and Ren (2007), these studies are based on a consistent risk level and ignore the compounding risk effects of the event itself by not jointly examining both wealth and risk impacts that affect the market in the same direction and cannot be separated absent of explicit controls for risk effects. Dewan and colleagues evidence that abnormal returns are associated with IT by incorporating IT risk measures (Dewan, Shi, & Gurbaxani, 2007). Tanriverdi and Ruefli (2004) further support this notion and observe that

> *"Studies that examine the business value of IT only from the return perspective are overlooking risk/return tradeoffs. Incorporating risk into the analysis is critical for developing a more complete understanding of the performance effects of IT. At a minimum, studies focusing on the return implications of IT should control for associated risks." (Tanriverdi & Ruefli, 2004, p. 441)*

As such an event study methodology that "extends the estimation window to include both pre-event and post-event data and allows for the market model parameters α and β to change following the event" (Dewan & Ren, 2007, p. 374) would provide further insight.

Given this ongoing scholarly discussion regarding the impact of enterprise systems on organizational value and risk in addition to the evolving capabilities of enterprise systems since most studies took place, This study aims to answer Otim et alia's (2012) call to examine the impact of investments in enterprise technology on risk, as perceived by external stakeholders by adopting a methodology that may improve on previous deficiencies.

3.5 Theoretical Framework and Hypotheses Development

The Resource-Based View (RBV) of the Firm (Barney, 1991; Bharadwaj, 2000) posits that firms derive competitive advantages from resources that are rare and valuable. As exemplified by the literature review, this framework has provided a theoretical basis from which IS capabilities have been examined to explore competitive advantages (D. Q. Chen, Mocker, Preston, & Teubner, 2010). Thus, I draw from the RBV to analyze firm performance in terms of risk in comparison to the overall market to conduct this study.

Financial economics provides a perspective of risk that can be conceptualized in two dimensions: systematic, which represents the risk associated with general market conditions, and unsystematic risk, which is unique and specific to a firm (Dewan & Ren, 2007). Using this perspective, unsystematic risk is perceived to be insignificant given the ability to diversify unsystematic risk away. The capital asset pricing model or CAPM (Treynor, 1962) provides a framework in which risk and return are positively related. The theory contends that all assets have a discount rate at which future cash flows produced by such assets should be discounted given the relative risk of the asset. CAPM makes certain assumptions about the investors (e.g. cost-free transactions, risk-averse investors and unlimited investment capacities), and it asserts that all asset-specific risks can be paired by a beta index relative to the market beta of one. This perspective contends that systematic risk, measured by the sensitivity of the expected asset returns to the expected excess of market returns, cannot be mitigated. Thus, a measure of the success of enterprise risk management initiatives can be assessed by its reduction in its beta (Gordon et al., 2009). CAPM

remains fairly popular given its simplicity and utility in a variety of scenarios despite its flaws when compared to more robust methodologies (Fama & French, 2004). Another theoretical basis of this study is the Market Efficiency Hypothesis, in which financial markets are presumed to be information-efficient. As such, investors cannot consistently achieve returns in excess of average market returns on a risk-adjusted basis, given the information available at the time the investment is made (Fama, 1970). This study presumes that information in the U.S. travels rather efficiently; thus, the potential effect of any public announcements made by publicly traded companies should be reflected in stock market reactions.

Although the financial view holds that firm-specific risk can be diversified away, strategic interventions such as IT investments can affect the risk/return profile of a firm (Otim et al., 2012; Tanriverdi & Ruefli, 2004). Given that enterprise systems affect several processes that are transformative to an organization, the timing of such investments in relation to the rest of the firms in an industry have been evidenced to downside reduce risk and provide strategic value in comparison to lower performing firms (Otim et al., 2012). The authors contend that this strategic management view of risk does in fact matter to a firm, even if it is firm-specific and often associated with unsystematic risk. However, if an event has affected the return of the security, there is no theoretical reason to believe that it has not affected the systematic and unsystematic risk of the security's return. As such, this study adopts Dewan and Ren's (2007)'s position and contends that if an investment event is so transformational for an organization, changes in systematic risk should be examined.

Figure 3.1 depicts the proposed model for this study, based on Dewan and Ren's (2007)'s Risk-Adjusted Market Model and expanded as follows:

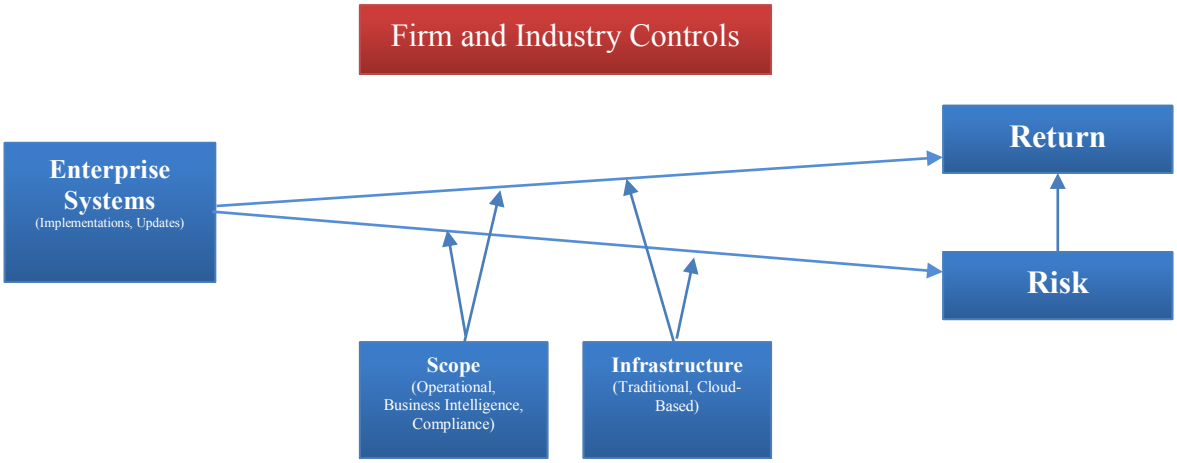

Figure 3.1 Proposed Model.

3.5.1 Value of enterprise system implementations and updates

As summarized in previous sections, there is an extensive stream of literature that has investigated the impact of information technology investments on an organization's financial and non-financial performance (e.g. Bharadwaj, 2000; Brynjolfsson & Hitt, 2003; Dehning et al., 2007; Kohli & Devaraj, 2003; Otim et al., 2012). Specific enterprise system implementation research have validated the valuable impact of these systems in spite of all cited costs and risks associated with these enterprise implementations (Grabski et al., 2011). Operational benefits are evidenced to include higher operational knowledge and more efficient inventory turnover, production flow, order lead times, processing times, as well as, reduced cost of goods sold, inventory turnover and availability of products (e.g. Baskerville, Pawlowski, & McLean, 2000; Bose, Pal, & Ye, 2008; Cotteleer & Bendoly, 2006; Dehning, Richardson, & Zmud, 2007; Gefen, 2005; Madapusi & D'Souza, 2012; Poston & Grabski, 2001). Tactical benefits include significant improvements in customer vendor collaboration, decision making, scheduling, quality management, change management, process management, resource planning, transparency and organizational standardization (e.g. Becker, Greve, & Albers, 2009; Bose et al., 2008; Chand et al., 2005; Cotteleer & Bendoly, 2006; Gefen, 2005; Häkkinen & Hilmola, 2008; Madapusi & D'Souza, 2012). Strategic benefits cited include market growth, capitalization, new markets, better forecasting, as well as higher competitive advantages in return-on-assets, return on investments (e.g. Chand, Hachey, Hunton,

Owhoso, & Vasudevan, 2005; Dehning, Richardson, & Zmud, 2007; Hayes, Hunton, & Reck, 2001; Hendricks, Singhal, & Stratman, 2007; Hitt, Wu, & Xiaoge Zhou, 2002; Nicolaou & Bhattacharya, 2006; Nicolaou, 2004; Su & Yang, 2010). Thus, the following hypothesis is offered:

> *H1: Firms with public announcements of enterprise system implementations will exhibit an increase of market valuation as measured by abnormal market returns.*

3.5.1 Risk Effect of enterprise system implementations and updates

As previously summarized, enterprise systems have been evidenced to provide better internal control that are derived from data processing integration, access and security centralization, and system usage standardization (Sia, Tang, Soh, & Boh, 2002), permitting the standardized control of user knowledge, role and system privileges, improving information quality (Häkkinen & Hilmola, 2008). When configured appropriately, they can support management control (Chapman & Kihn, 2009; Elmes et al., 2005; Kallunki et al., 2011) auditing (S.-I. Chang et al., 2008; Kuhn Jr. & Sutton, 2010), and compliance purposes (Grabski et al., 2011; Maurizio et al., 2007; Mundy & Owen, 2013). Although dissenting literature disputes the ability to materialize such benefits (Brazel & Dang, 2008; Granlund & Malmi, 2002), enterprise systems have also been evidenced to improve firm performance and reduce risks (Kallunki et al., 2011). The literature also suggests that enterprise systems can serve as management control system packages integrating various accounting and non-accounting control systems (Granlund, 2009). Given that enterprise systems have been evidenced to be a part of enterprise-wide risk management efforts that can decrease volatility in earnings and stock prices, decreasing external capital costs and increasing capital efficiency (Gordon et al., 2009; Hoyt & Liebenberg, 2011; Nocco & Stulz, 2006), the financial economics would offer support to examine the impact of enterprise systems on systematic risk. Thus, the following hypothesis is offered:

> *H2: Firms with public announcements of enterprise system implementations will exhibit a decrease in a company's systematic risk.*

Given the magnitude of enterprise system implementation, a myriad of challenges (e.g. insufficient technical expertise, organizational fit factors, project management issues) have been historically found to

impact the overall success of a new risk ERP implementation (Sumner, 2000). Organizations, however, tend to acquire resources with time and overcome learning challenges. Furthermore, studies have differentiated the value obtained from initial implementations from subsequent upgrades and updates suggesting that enhancements that occur within a few years of the post-implementation may signify that the system is well adopted and that any additional initiatives serve strategic purposes (Nicolaou & Bhattacharya, 2006; Otim et al., 2012; Roztocki & Weistroffer, 2009). While this study posits that implementation of enterprise systems will reduce the systematic risk in a firm, such reduction should be affected by the history of enterprise system implementations by that firm. Thus, the following hypothesis is offered:

> *H3: A firm's systematic risk reduction exhibited after a public announcement of an enterprise system will be affected by whether the firm is engaging in a new project or an update to an already existing system.*

Studies suggest that investors may discern the purpose of system implementations at the time of the announcement and react differently if such purpose is meant to serve transformational, strategic and innovative purposes for an organization, as opposed to automation purposes (Dos Santos, Peffers, & Mauer, 1993; Otim et al., 2012). During the last decade, vendors have transformed their enterprise systems to include modules that go beyond the integration of business functions; such capacities include, but are not limited to, business intelligence, compliance and risk management (Grabski et al., 2011; Mathrani & Mathrani, 2013; Rubin & Rubin, 2013). In addition to these enhancements, vendors have emerged with cloud-based and hybrid systems that offer on-demand, scalable enterprise software online. SAP Business ByDesign and Sage 300 ERP Online are a few examples of these platforms. Research also suggests that the scope of an enterprise system can moderate financial performance (Dehning et al., 2007). The purpose of system implementations at the time of the announcement, the development of more sophisticated software capacities in to support an organization, and the availability of cloud-based infrastructure may cause moderating effects on risk interactions. Thus, the following hypotheses are offered:

> *H4: A firm's systematic risk reduction exhibited after a public announcement of an enterprise system will be affected by whether the firm is implementing a cloud-based system.*

H5: A firm's systematic risk reduction exhibited after a public announcement of an enterprise system will be affected by whether the firm is implementing a system that includes a business intelligence module.

H6: A firm's systematic risk reduction exhibited after a public announcement of an enterprise system will be affected by whether the firm is implementing a system that includes a government regulatory compliance module.

3.6 Methodology

The target sample of this study was U.S. publicly traded companies who announced the upgrade or implementation of an enterprise systems on or after the year 2002. To collect this sample, a search was performed on the Lexis/Nexis Academic service and Google News. The search terms "implement", "choose", "select", "purchase", "install", "upgrade", "update" in junction with the terms "NYSE", "AMEX","NASDAQ", in junction as well with the terms "enterprise system", "ERP", "enterprise resource management", "CRM", "customer relationship manager", "SCM", "supply chain management", "BI", "business intelligence", "manufacturing management", "procurement", "warehouse management", "inventory management", "planning", "order management", "compliance management", "risk management", "forecasting", "decision support", "financial management", "cloud-based", "eCommerce", "distribution management", "material requirement planning" and 3 major software brands (e.g. SAP, Oracle, Microsoft). Subsequently, each press release were inspected to verify that a U.S. publicly traded company was implementing or upgrading a system and for collection of corporation name, trading ticker, date of announcement, scope, venue, degree of implementation, vendor and purpose. Announcements within 30 days of each other were consolidated to the 1st occurrence. Consistent with prior studies (Dewan et al., 2007), announcements were eliminated if the Company had less than 120 days of trading history prior and after the events, no data existed at the Center for Research in Security Prices (CRSP) or confounding announcements within a three-day window. After elimination of several announcement due to cited factors, a total of 118 announcements were rendered valid for analysis.

3.6.1 Risk-Adjusted Market Model and Analysis

In order to jointly examine the effect of risk and return for the events, this study adopts Dewan and Ren's (2007)'s Risk-Adjusted Market Model and expands it as follows:

$$R_{it} = \alpha_i + \alpha'_i D_t + \beta_i R_{mt} + \beta'_i D_t R_{mt} + \beta_i R_{mt} + \varepsilon_{it} \quad (3.1)$$

Under this model, R_{it} represents stock returns on the market portfolio R_{mt}. The dummy variable Dt represents the pre (value 0) and post event (value 1) window, providing an opportunity to measure the parameters α'_i and β_i' to measure the value of alpha and beta respectively. The analysis uses 120 trading days to calculate the pre-event and post-event estimation window to allow the segregation of return and risk effects. The event window is conducted based on t, t±1 trading days. Since both risk and return are considered to be closely correlated, heteroscedasticity may be suspected. As such, an OLS regression with robust standard errors that estimates the asymptomatic covariance matrix of the estimates is a more adequate methodology to address normality, heteroscedasticity and large residual concerns (White, 1980). The model is applied to the data set for each firm in order to obtain parameter estimates. Once the model contained in equation 3.1 was applied to all the firms, the resulting coefficients α_i and $\beta_i R_{mt}$ along with the actual realized return R_{it} were used to calculate the corresponding abnormal returns (AR_{it}), or the deviation of realized returns from the expected returns, for each firm. Equation 3.2 depicts the calculation of abnormal returns:

$$AR_{it} = R_{it} - (\alpha_i + \beta_i R_{mt}) \quad (3.2)$$

For purposes of this study, the cumulative abnormal return (CAR_i) variable for firm i was calculated by summing the abnormal returns for the 3-day event window containing the announcement day plus and minus 1 day (-1,0,1). This variable is subsequently aggregated as an average ($\bar{CAR}$) across all firms or across firms within subgroups (e.g. firms that implemented new systems versus updates) as depicted in Equation 3.3:

$$\bar{\text{CAR}} = \frac{1}{N}\sum_{i=1}^{N} CAR_i \tag{3.3}$$

To provide further insight into the results, a cross sectional analysis relating risk changes to various event and firm characteristics is conducted. This analysis will examine the determinants of total risk as depicted in Equation 3.4:

$$\begin{aligned} \Delta SysRisk_{it} \;=\; & \alpha_0 + \alpha_1 PreSysRisk_{it} + \alpha_2 Ret_{it} + \alpha_3 New_{it} + \alpha_4 BI_{it} + \alpha_5 Cloud_{it} + \alpha_6 GRC_{it} \\ & + \alpha_7 FirmSize_{it} + \alpha_8 Leverage_{it} + \alpha_9 NewCloud_{it} + \alpha_8 NewBI_{it} + \varepsilon_{it} \end{aligned} \tag{3.4}$$

Where for each company i at time t: "PreSysRisk" represents the systematic risk that existed in the estimation period prior to the event as calculated by equation 3.1. "Ret" represents the average return over the prior 120 days, included given the hypothesis that returns are associated with risk. "New" represents a dummy variable of 1 for a new system implementation or 0 for an update to an existing system. "Cloud" represents a dummy variable coded with 1 for cloud-based systems and 0 for traditionally in-house systems. "GRC" represents a dummy variable coded with 1 for systems containing government regulatory compliance modules and 0 without such modules. Similarly, "BI" represents a dummy variable coded with 1 for systems containing business intelligence modules and 0 without them. "NewCloud" represents a dummy coded 1 for the implementation of new cloud systems, and "NewBI" for the implementation of new business intelligence systems, as opposed to updates of the same. Finally, previous literature suggests that certain firm characteristics may influence a company's overall risk (Bharadwaj, Bharadwaj, & Konsynski, 1999; K. C. W. Chen & Lee, 1993; Dewan et al., 2007; Otim et al., 2012); For control variables, Leverage is included as the ratio of total long term divided by the total assets of the company during the event's fiscal year; and FirmSize, operationalized as the logarithm of market value of the firm on the event day.

3.7 Descriptive Statistics

3.7.1 General Descriptive Statistics

Table 3.3 contains a classification summary by industry and enterprise system characteristics contained in the 118 public announcement collected for analysis.

Table 3.3. Classification Summary by Industry and System Characteristics

	Manufac.	Transport	Retail	Financial	Services	Other	Total
New	42	11	18	4	10	0	***85***
Update	13	2	7	4	5	2	***33***
Cloud	12	2	2	5	6	2	***29***
Non-Cloud	43	11	23	3	9	0	***89***
BI	11	2	11	0	1	0	***25***
Non-BI	44	11	14	8	14	2	***93***
GRC	8	1	0	1	0	0	***10***
Non-GRC	47	12	25	7	15	2	***108***
	55	**13**	**25**	**8**	**15**	**2**	***118***

3.7.2 Moving Average Variance of Stock Market Returns

Figure 3.2 illustrates the average variance of stock market returns after enterprise system implementations. This moving average is based on the average of the prior 120 days before the trading day depicted in the graph, relative to the announcement day. The graph displays a downward departure in total stock variance, normally considered a firm's total risk which encompasses both systematic and unsystematic risk. Figure 3.3 illustrates the average variance of stock market returns after updates versus new enterprise system implementations. The graph displays a sharper decline in total variance for those companies that implement updates to a system as opposed to a brand new implementation.

Figures 3.4, 3.5 and 3.6 display the average variance of stock returns after announcements of enterprise system implementation systems containing business intelligence, government-regulatory compliance and cloud-based modules respectively. While business intelligence modules do not seem to

have a visual difference, absent of appropriate statistical analysis to be conducted in the next section, government regulatory compliance containing systems as well as cloud-based enterprise systems seem to display a contrast in the moving average of the stock return variance for the firms contrasted in the graphs.

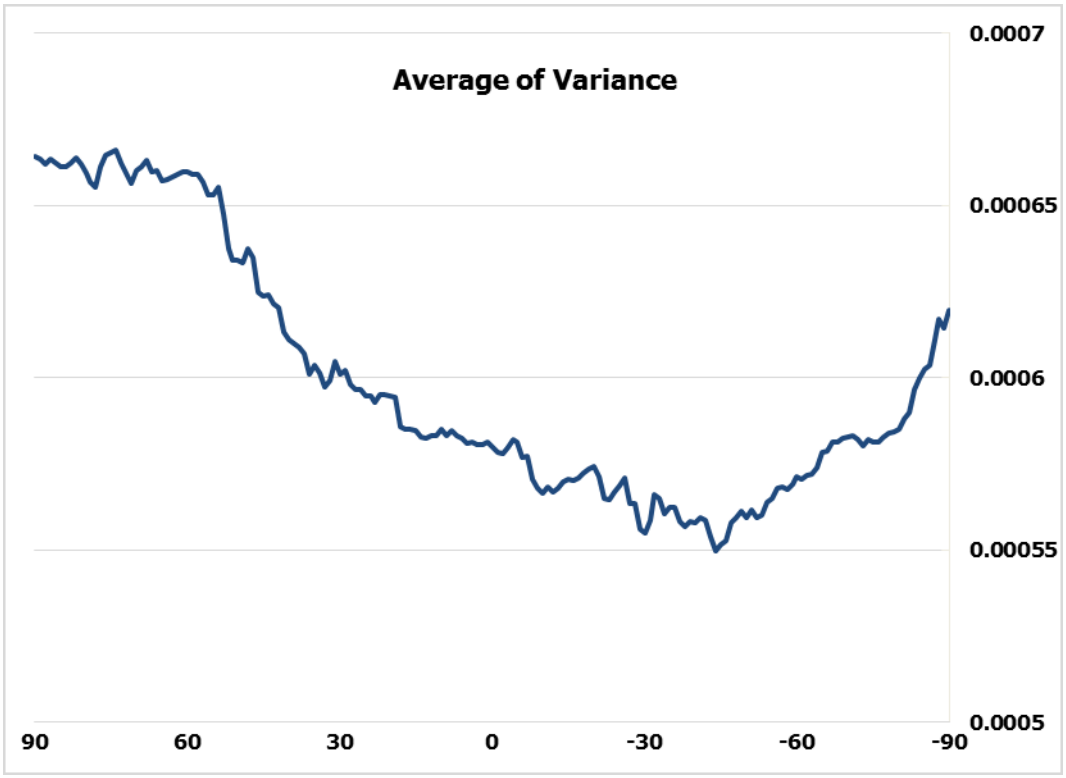

Figure 3.2 Average of Return Variance after System Implementations

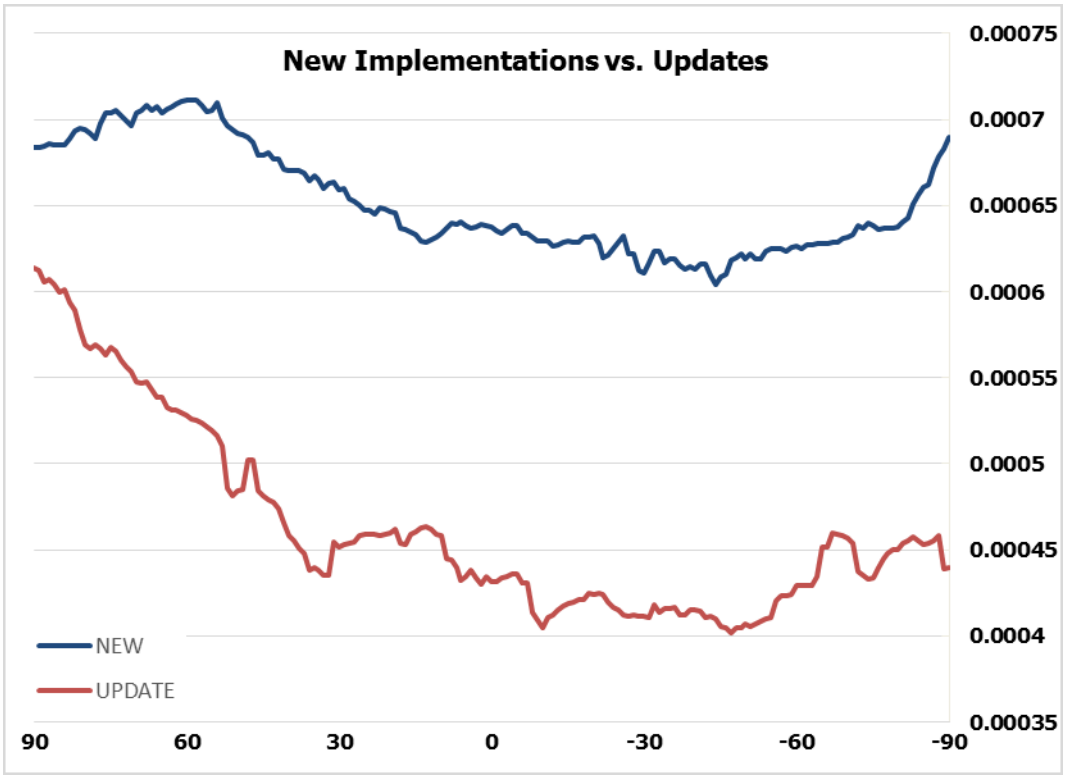

Figure 3.3 Average of Return Variance after System Implementations-New vs. Updates

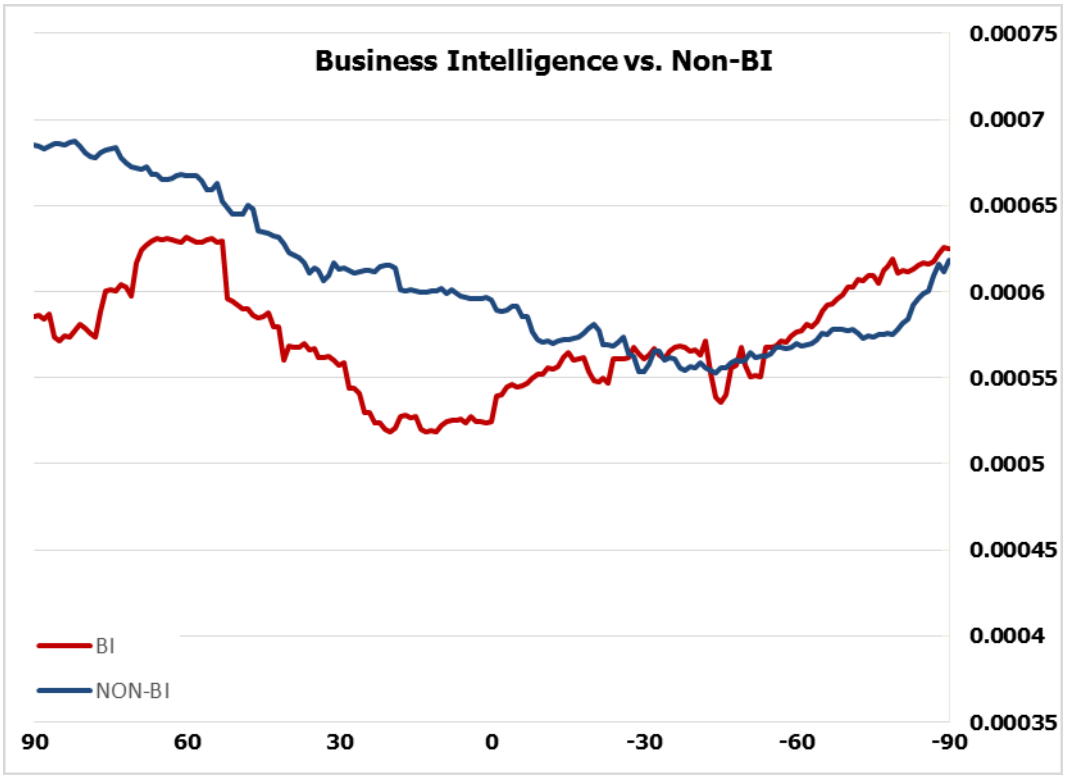

Figure 3.4 Average of Return Variance after System Implementations-BI vs. Non-BI

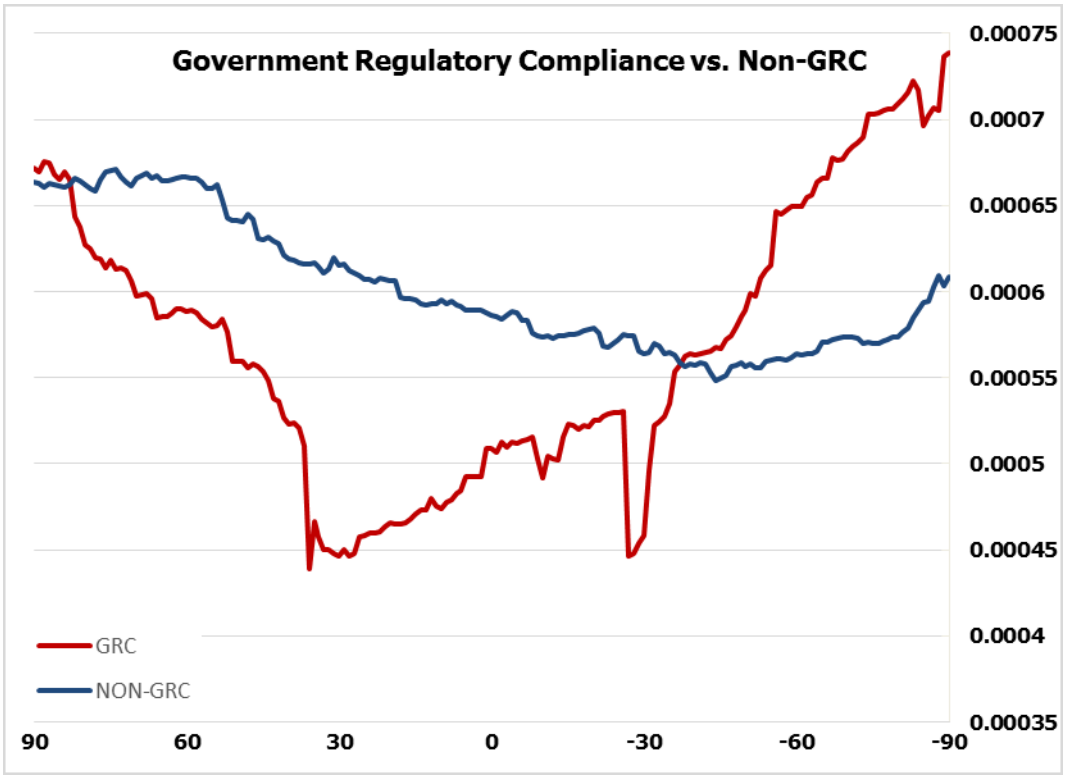

Figure 3.5 Average of Return Variance after System Implementations-GRC vs. Non-GRC

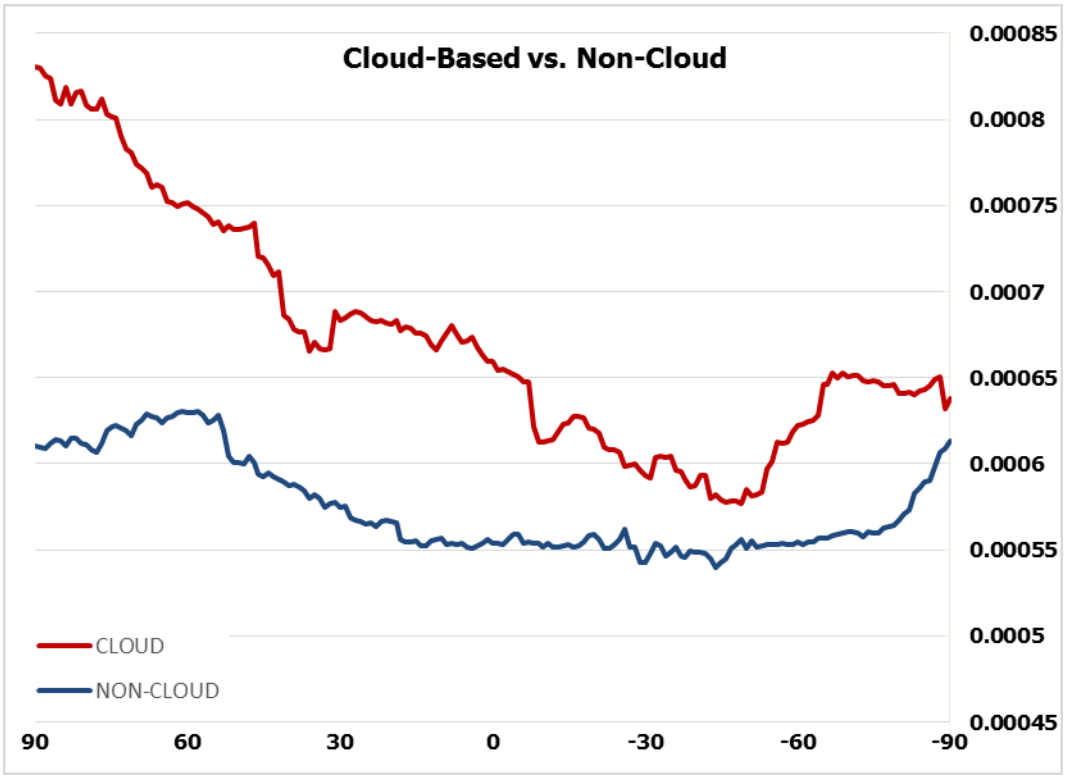

Figure 3.6 Average of Return Variance after System Implementations-Cloud vs. Non-Cloud

3.7.3 Abnormal Returns and Cumulative Abnormal Returns

The risk-adjusted marked model contained in equation 3.1 was applied to the collected sample in order calculate each firm's parameter estimates. Once the model was applied to the data set for each firm to calculate the corresponding expected returns and the beta coefficients, Equation 3.2 and 3.3 to calculate the corresponding abnormal returns and CĀR for the entire group of firms. In addition, firms were grouped according to the system characteristics of interest to derive further information. Table 3.4 depicts a summary of the abnormal returns averaged by the different classifications of system characteristics, as well as the trading day relative to the announcement day 0. The table also contains the minimum and maximum abnormal returns observed in the respective classification group. The largest abnormal returns observed for any given announcement are -23.9% on the negative side 10.1% for the positive side. The corresponding CĀR are -27.9% and 19.1%.

Table 3.4. Summary of Abnormal Returns and CĀR classified by system characteristics

	t= -1			t=0			t=1			CĀR		
	$\bar{x}$	Min	Max	$\bar{x}$	Min	Max	$\bar{x}$	Min	Max	$\bar{x}$	Min	Max
All Firms	0.002	-0.046	0.065	-0.002	-0.239	0.101	-0.001	-0.061	0.061	0.000	-0.279	0.191
New	0.002	-0.046	0.065	-0.004	-0.239	0.097	-0.002	-0.061	0.057	-0.003	-0.279	0.191
Update	0.002	-0.019	0.028	0.004	-0.048	0.101	0.003	-0.047	0.061	0.009	-0.076	0.170
Cloud	0.006	-0.046	0.043	0.000	-0.101	0.101	-0.002	-0.061	0.057	0.004	-0.120	0.170
Non-Cloud	0.001	-0.046	0.065	-0.002	-0.239	0.097	0.000	-0.055	0.061	-0.001	-0.279	0.191
BI	0.003	-0.036	0.038	-0.002	-0.055	0.030	0.000	-0.047	0.050	0.001	-0.076	0.056
Non-BI	0.002	-0.046	0.065	-0.002	-0.239	0.101	-0.001	-0.061	0.061	0.000	-0.279	0.191
GRC	-0.001	-0.031	0.027	0.004	-0.013	0.043	0.001	-0.028	0.039	0.004	-0.032	0.041
Non-GRC	0.003	-0.046	0.065	-0.002	-0.239	0.101	0.001	-0.061	0.061	0.000	-0.279	0.191

3.8 Hypotheses Testing and Empirical Results

3.8.1 Effect of Enterprise System Implementations on Market Value

In order to test Hypothesis 1 (H1) which posits that firms with public announcements of enterprise system implementations will exhibit an increase of market valuation as measured by abnormal market returns, a t-Test with an upward 95% confidence interval is conducted on the abnormal returns on days -1, 0 and 1 as well as the cumulative abnormal return for the sample size of 118 companies. In addition, to further explore the system characteristics of interest, the same t-test is applied to eight subgroups that follow the system characteristics classification described before. Table 3.5 provides a summary of the statistical analysis to test H1. The average abnormal return for the sample group was 0.002, -0.002 and -0.001 on days -1, 0 and 1 respectively, all with non-significant p-values (0.12, 0.70, 0.61). The average cumulative abnormal return for the sample is not different than 0, also with non-significant p-value (0.49). Furthermore, for the exception of day -1 for the subgroup of cloud-based enterprise systems implementations which exhibited a 0.6% higher abnormal return than expected (p-value of 0.05), none of the other treatment tests provide support for H1.

This finding may merit a qualified discussion, however, it is not sufficient to support the underlying hypothesis. As such, the H1 is not supported; public announcements of enterprise system implementation did not exhibit an increase of market valuation as measured by abnormal market returns. Given that some of the average abnormal returns were observed in the opposite hypothesized direction, and for robustness purposes, a t-test with a 95% confidence interval from the mean was also conducted. Such efforts yielded similar non-significant results.

Table 3.5. T-Test Results for Abnormal Returns and CĀR classified by system characteristics

	day=-1			day=0			day=1			CAR		
	$\bar{x}$	*t*-value	Pr > t	$\bar{x}$	*t*-value	Pr > t	$\bar{x}$	*t*-value	Pr > t	$\bar{x}$	*t*-value	Pr > t
General	0.002	1.20	0.12	-0.002	-0.54	0.70	-0.001	-0.27	0.61	0.000	0.02	0.49
New	0.002	0.88	0.19	-0.004	-0.96	0.83	-0.002	-0.74	0.77	-0.003	-0.57	0.72
Update	0.002	1.20	0.12	0.004	0.80	0.21	0.003	0.73	0.23	0.009	1.12	0.13
Cloud	0.006	1.67	**0.05**	0.000	-0.03	0.51	-0.002	-0.39	0.65	0.004	0.45	0.33
Non-Cloud	0.001	0.49	0.31	-0.002	-0.61	0.73	0.000	-0.08	0.53	-0.001	-0.21	0.58
BI	0.003	0.87	0.20	-0.002	-0.39	0.65	0.000	-0.13	0.55	0.001	0.12	0.45
Non-BI	0.002	0.94	0.17	-0.002	-0.45	0.67	-0.001	-0.24	0.59	0.000	-0.02	0.51
GRC	-0.001	-0.23	0.59	0.004	0.70	0.25	0.001	0.21	0.42	0.004	0.51	0.31
Non-GRC	0.003	1.30	0.10	-0.002	-0.65	0.74	0.001	-0.33	0.63	0.000	-0.05	0.52

3.8.2 Effect of Enterprise System Implementations on Systematic Risk

Hypothesis 2 (H2) posits that firms with public announcements of enterprise system implementations will exhibit a decrease in a company's systematic risk. Equation 3.1 was applied to the entire sample group containing 238 trading days (-120 to -2 and 2 to 120) for 118 companies, for the exception of 2 companies missing data for 15 and 16 trading days. A total of 28,055 observations were used for this equation. The beta coefficients for both $\beta_i R_{mt}$ and $\beta'_i D_t R_{mt}$ were used to compare the pre-event and post-event systematic risk. The analysis of variance for the model was found statistically adequate with an F-Value of 3,170 (Pr > F of <.0001), and an adjusted R^2 of 0.2531. The resulting beta coefficients the pre-event were found to be significant at a Pr > |t| value of less than 0.0001 with corresponding betas of β_i=1.0420 and $\beta'_i D_t$ =0.1209, a reduction in systematic risk (β) of 0.92109 after the announcement. To further test this hypothesis, Equation 3.1 was applied to each one of the companies to generate individual firm estimates for pre-event and post-event beta coefficients. A t-test analysis with a 95% confidence interval from the mean was conducted to determine the significance of their difference. Figure 3.7 displays a graph with the mean agreement points of systematic risk before the announcement

and after the announcements. While significant findings were found, q-q plots and a subsequent univariate analysis based on a Anderson-Darling Method (>.005) of both variables revealed there was a violation of the normality distribution assumption. As such, a Wilcoxon signed-rank test was conducted providing supporting results with a median systematic risk reduction (β) of 0.8767 and a mean systematic risk reduction (β) of 1.008 (Wilcoxon's W = 93, n=118, Pr >= |S| <.0001). H2 is supported is thus supported, firms with public announcements of enterprise system implementations exhibit a statistically significant reduction in a company's systematic risk (β).

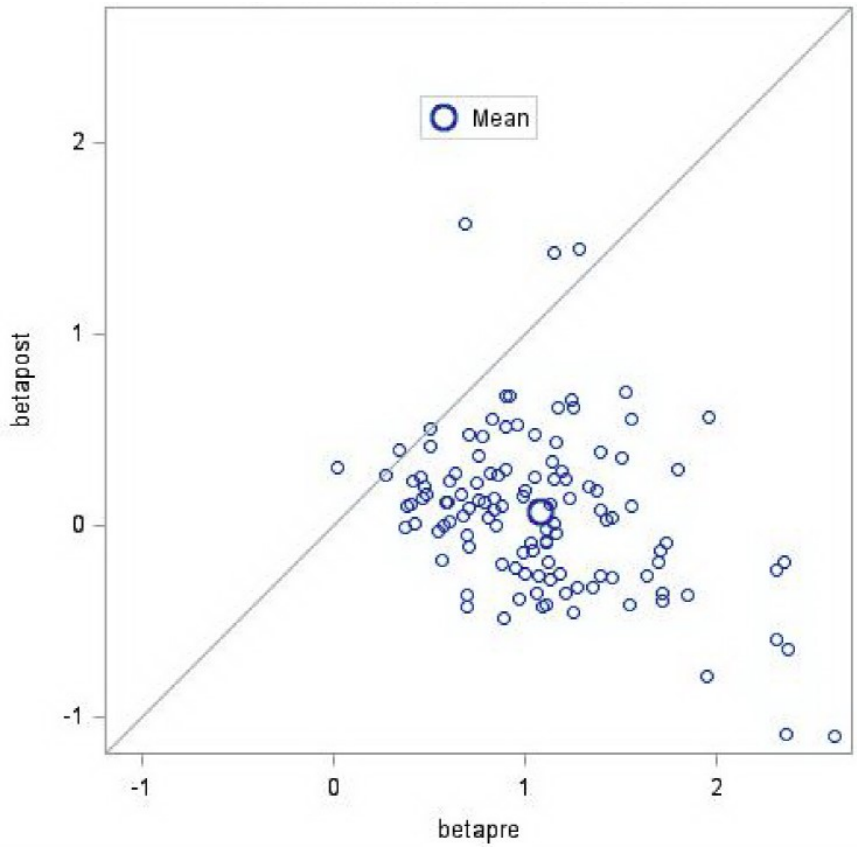

Figure 3.7 Systematic Risk Pre-Event and Post-Event Agreement Graph

3.8.3 Effect of Enterprise System Characteristics on Systematic Risk

Hypotheses 3, 4, 5 and 6 posit that a firm's systematic risk reduction exhibited after a public announcement of an enterprise system will be affected by the certain system characteristics, including

whether the system is a new system or an update (H3), a cloud-based system (H4), a business intelligence system (H5), and a government regulatory compliance system (H6). In order to test these hypotheses, Equation 3.4 was applied as described in the methodology section. A correlation analysis was conducted to test for multicollinearity. Table 3.6 illustrates the correlation matrix of the variables contained in the equation. As expected, the interaction variables NewBI and NewCloud exhibited high correlation coefficients. However, no other variables exhibited problematic correlations that may distort the precision of coefficient parameters

Table 3.6. Correlation Matrix of Predicting Variables for Systematic Risk Difference

Pearson Correlation Coefficients, N = 118 Prob > |r| under H0: Rho=0											
	SysRisk Diff	BetaPre	RetSUM	New	BI	Cloud	GRC	NewBI	New Cloud	Firm Size	Leverage
SysRisk Diff	1	-0.85998	-0.11099	0.04155	-0.00074	0.22425	-0.13564	0.01722	0.17925	0.11582	0.14023
		<.0001	0.2315	0.6551	0.9936	0.0146	0.143	0.8532	0.0521	0.2117	0.1299
BetaPre	-0.85998	1	0.12737	0.00269	-0.02513	-0.19768	0.11881	-0.01744	-0.19816	-0.10811	-0.16968
	<.0001		0.1693	-0.01822	0.7871	0.032	0.2	0.8513	0.0315	0.2439	0.0662
RetSUM	-0.11099	0.12737	1		-0.03157	0.13845	0.07955	-0.05652	0.12714	0.12663	0.12501
	0.2315	0.1693		0.8447	0.7343	0.1349	0.3918	0.5432	0.1701	0.1718	0.1774
New	0.04155	0.00269	-0.01822	1	0.09202	-0.12673	-0.28497	0.28148	0.26435	-0.26149	0.07186
	0.6551	0.977	0.8447		0.3216	0.1715	0.0018	0.002	0.0038	0.0042	0.4394
BI	-0.00074	-0.02513	-0.03157	0.09202	1	-0.00694	-0.0833	0.87131	0.06844	-0.01661	-0.10185
	0.9936	0.7871	0.7343	0.3216		0.9405	0.3698	<.0001	0.4615	0.8583	0.2725
Cloud	0.22425	-0.19758	0.13845	-0.12673	-0.00694	1	-0.03234	0.00445	0.74325	0.05488	0.09157
	0.0146	0.032	0.1349	0.1715	0.9405		0.7281	0.9619	<.0001	0.555	0.324
GRC	-0.13564	0.11881	0.07955	-0.28497	-0.0833	-0.03234	1	-0.05636	-0.1291	0.17254	0.01011
	0.143	0.2	0.3918	0.0018	0.3698	0.7281		0.5444	0.1635	0.0617	0.9135
New BI	0.01722	-0.01744	-0.056552	0.28148	0.87131	0.00445	-0.05636	1	0.12245	-0.00178	-0.07017
	0.8532	0.8513	0.5432	0.002	<.0001	0.9619	0.5444		0.1865	0.9847	0.4502
New Cloud	0.17925	-0.19816	0.12714	0.26435	0.06844	0.74325	-0.1291	0.12245	1	-0.05945	0.06105
	0.0521	0.0315	0.1701	0.0038	0.4615	<.0001	0.1635	0.1865		0.5225	0.5114
Firm Size	0.11582	-0.10811	0.12663	-0.26149	-0.01661	0.05488	0.17254	-0.00178	-0.05945	1	0.1564
	0.2117	0.2439	0.1718	0.0042	0.8583	0.555	0.0617	0.9847	0.5225		0.0908
Leverage	0.14023	-0.16968	0.12501	0.07186	-0.10185	0.09157	0.01011	-0.07017	0.06105	0.1564	1
	0.1299	0.0662	0.1774	0.4394	0.2725	0.324	0.9135	0.4502	0.5114	0.0908	

Table 3.7 contains the resulting regression statistics for the predicting variables for systematic risk differences using Equation 3.4

Table 3.7. Statistics Predicting Variables Statistics for Systematic Risk Difference

Heteroscedasticity Consistent Parameter Estimates					
Variable	**DF**	**Parameter Estimate**	**Standard Error**	**t Value**	**Pr > |t|**
Intercept	1	-0.10022	0.5587	-0.18	0.858
BetaPre	1	-1.30282	0.08519	-15.29	<.0001
RETSUM	1	-0.01579	0.12218	-0.13	0.8974
New	1	0.18353	0.08977	2.04	0.0434
BI	1	-0.09767	0.16545	-0.59	0.5562
Cloud	1	0.32258	0.13634	2.37	0.0198
GRC	1	-0.07163	0.10276	-0.7	0.4873
FirmSize	1	0.01695	0.02322	0.73	0.4669
Leverage	1	-0.12812	0.21396	-0.6	0.5506
NewCloud	1	-0.32287	0.16061	-2.01	0.0469
NewBI	1	0.06438	0.18184	0.35	0.724

F Value = 33.19, Pr > F <.0001, Root MSE=.3921, Adj. R2 = .7569

Given the above cited results, H3 is supported, firms with public announcement of new systems exhibited a higher systematic risk change (0.184; Pr > |t|<.05) than those firms that announced updates to already existing systems. H4 is also supported, firms with public announcement of cloud-based enterprise systems exhibited a higher systematic risk change (0.323; Pr > |t|<.05) than those firms that announced traditionally hosted systems. H5 was not supported firms with public announcements of enterprise systems that contained business intelligence modules did not exhibit a significant change in their systematic risk. Finally, H6 was also not supported, firms with public announcements of enterprise

systems that contained government regulatory compliance, did not exhibit a significant change in their systematic risk. Table 3.8 summarizes the findings:

Table 3.8. Summary of Findings

Index	Hypothesized	Findings	Exhibit
H1	Higher Abnormal Returns	Not Supported	None
H2	Lower Systematic Risk	Supported	1.0 Lower post-event beta for all systems
H3	New vs Updates	Supported	0.18 Higher post-event beta for updates
H4	Cloud vs Traditional	Supported	0.323 Higher post-event beta for cloud
H5	Bus. Intelligence vs. Non-BI	Not Supported	None
H6	Govt. Reg. Compliance vs. Non-GRC	Not Supported*	Robust test conflict with these findings and further analysis is required.

3.9 Conclusion

3.9.1 Implications and Future Research

This study addresses the dialogue in the literature surrounding the impact of enterprise system implementations on risk mitigation in addition to this decade's technology and regulatory developments. Specifically, it responds to Otim et al. (2012)'s call to examine the impact of investments in enterprise technology on risk by adopting a methodology designed to improve on previous studies, examining enterprise risk net-effects caused by the changes in the interdependencies in business process and internal controls caused by such implementations.

In terms of hypothesized increase in market value after implementations, the hypothesized abnormal returns are not realized as expected. The findings suggest that implementing enterprise systems in this millennium does not provide higher market value for firms. This suggests that investors may already believe that enterprise system investments will no longer provide competitive advantages over other firms given that the adoption lifecycle has surpassed critical mass and it is no longer considered an innovative tool, but rather a standard necessity. While prior studies have provided evidence that enterprise systems lead to greater firm performance based on financial operations metrics (Becker et al., 2009; Bose et al., 2008; Cotteleer & Bendoly, 2006; Hunton et al., 2003), this study suggests that these firm performance improvements are competed away as the underlying RBV theory suggests. This is consistent

with Nicolaou and Bhattacharya (2006)'s suggestion that implementation timing matters; and it may explain the contrasting results from studies conducted when enterprise systems where considered more innovative in the end of last century, particularly around the time that legacy systems where being replaced due to perceived Y2K issues as exhibited in prior studies (Hayes et al., 2001; Hitt et al., 2002). This study, however, does not assess the timing of the adoption in relation to other competitors in the industry, which would provide more insight if addressed in future research. The findings are also consistent with Dewan and Ren (2007)'s premise that wealth effects may be dissipated away when controlling for risk changes; and this study confirms that such risk profile does indeed change for enterprise system implementers.

The critical finding provided by this study is that firms with public announcement of enterprise systems exhibit a reduction in their systematic risk, averaging a reduction in their risk profile in terms of beta of an average of 1.00. This finding is consistent with the premise that enterprise systems can transform an organization by providing greater controls at the business process and financial management levels, and may also help mitigate regulatory compliance risks (Kallunki et al., 2011; Maurizio et al., 2007; Mundy & Owen, 2013; Sia et al., 2002). This finding is of strong importance, in essence, firms exhibit a reduction of half the systematic risk in relation to the overall market. CAPM theory provides that each asset holds an appropriate required return or discount rate at which future cash flows produced by the asset should be discounted given the asset's relative riskiness. A reduction in the discount rate of an asset means that all future cash flows will have greater return. While investors may not perceive that greater market value may be achieved through such implementations, this study suggests that investors consider enterprise systems to transform an organization's risk profile in a meaningful, positive manner. Such significant reduction in enterprise risk has profound investment consequences in terms of cost and access to capital by a firm and it is consistent with Purser (2004)'s suggestions that return on investment calculations should also include the value of the reduction in risk that result from the investments.

This study also provides some insight in providing systematic risk differences based on software characteristics. Consistent with the literature grounding this study, the results suggests that new projects have less systematic risk reduction than updates. This is also the case for cloud-based systems. Cloud-based systems are perceived to be of higher risk, as such, firms with enterprise system implementation

that are cloud-based did not exhibit as much systematic risk reduction as those firms that implement traditional in-house systems. Firms that announced implementations of enterprise systems containing business intelligence modules did not exhibit any more or less systematic risk reduction than those firms that did not cite such implementations. While the research suggests implementing enterprise systems containing government regulatory compliance (GRC) experience has an effect on a firm's enterprise risk, the small frequency of GRC installations in the sample was not conducive to providing a statistically robust figure to depict an effect size of such difference. Future research may provide more insight on this matter.

This study can assist practitioners by providing evidence of the impact of enterprise system implementations on enterprise risk. This study demonstrates that while enterprise systems may require massive investment considerations, risk mitigation effects should be considered as part of the return on investment in addition to other previously cited firm performance improvements.

3.9.2 Limitations

This study is based on the premise that, as in other event studies, investors are rational and that capital markets are efficient (Fama, 1970) As a result, this study captures the anticipated reaction to an event that theoretically disseminated to investors in an efficient manner. It also focuses on the initial reaction of investors, as time passes, investor perceptions may change or may be reversed. In addition, event size, price stock, trading volumes, confounding and clustering of events may affect the results of the study. While most of these issues were addressed by adopting widely accepted methods, the removal of confounding events from a sample size may be subjective or affected by the lack of historical news.

This sample only consists of publicly traded companies, as such, it cannot be generalized to other types of organizations. While the sample size is sufficient for statistical analysis and comparable to other IS research studies, a larger sample size may have provided more robustness and permitted the inclusion of additional constructs of interest. The findings of the study do not assess the timing of the adoption in relation to other competitors in the industry, which would provide more insight if addressed in future research. The randomization of the sample may also be affected by the availability of historical news as data was collected up to 13 years after such announcements were made.

CHAPTER 4 – IMPACT OF IT GOVERNANCE CERTIFICATIONS ON ENTERPRISE RISK

4.1 Research Background

Businesses all around the globe are increasingly concerned with the cyber risks that exist today given the advent of new technologies that are dependent on an interconnected world wide web. National efforts in the U.S. have aimed to monitor the increasing dependence on information technology through the enactment of legislative initiatives that create a partnerships between the public and private sector to protect enterprises. Among Post 9/11 U.S. government efforts to regulate information security policies, the most impactful legislations include the Federal Information Security Management Act (FISMA), establishing comprehensive information security requirements for the federal government and contractors, the Sarbanes-Oxley Act (SOX) Section 404, which provides a framework of control objectives for information technology, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which implement appropriate policies and procedures to comply with standards, implementation specification to protect patient privacy. As part of FISMA, the National Institute of Standards and Technology was made responsible for developing technology standards and compliance guidelines to safeguard information security. As a result, NIST developed a broad risk-management framework (RMF) that would serve as a vehicle for federal agencies to use in building information security into an organization's infrastructure (Ross, 2007). NIST security standards and guidelines are developed through an open, public vetting process from both public and private stakeholders. While FISMA inducted the creation of key security standards and guidelines (FIPS 199 & 200, NIST publications 800-37, 800-53, 800-53a, 800-59 & 800-60), their efforts have expanded to address organizational issues, governance, and specific information asset protection.

Among such efforts, international standard ISO 17799 is one of the most prominent which established "guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization" (ISO.org, 2013). These authoritative statements aimed to provide best practices on information security, and the procedures necessary to achieve information security in the modern organization. Since then, this norm has been revised to become ISO/IEC 27002:2013, which is intended to provide control objectives to meet the requirements identified

by a risk assessment, setting a common basis and practical guideline for developing organizational security standards and effective security management practices. Such practices are aimed to build confidence in inter-organizational activities, providing assurances to clients, suppliers and other stakeholder assurances of the organizational systemic systems to mitigate risks. Its companion standard, ISO 27001, specifies the requirements for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks" (ISO.org, 2013)". Such standard is suitable to be used by different types of organizations, and can be used by external as an auditing guide that lays out controls that an organization must address in order to obtain a certification of assurance.

Similar to ISO 27001, COBIT 5 (*COBIT 5: Enabling Information*, 2013) is a normative framework for control and governance of information technology that is broader in scope and assess the degree of management direction for controlling the businesses IT processes, overall achievement and organizational goals. While both ISO 27001 and COBIT 5 both encompass the auditing aspects of ISMS, ISO 27001 focuses more on security and caters to mid-management implementations of an ISMS. COBIT 5 on the other hand, targets IT governance at the top-level needs of an enterprise. Additionally, COBIT 5 integrates all functions and processes that establish the governance of enterprise IT into overall enterprise governance.

Other domain-specific assessment are offered and undertaken by certified authorities that create the standards and are licensed to execute the audit. SAS 70 Type II audits, now SSAE 16, by the American Institute of Certified Public Accountants, are designed to assess service auditor examinations, attestation reporting and information systems in a variety of service providers by globally accepted accounting principles (AICPA, 2013) . Companies seeking this external audit are able to demonstrate to partners and customers that their organization's controls are in operation, suitably designed and operating effectively. This external validations is aimed at eliciting trust among partners, customers and stakeholders alike.

4.2 Research Purpose

IT governance, defined as "the process by which organizations seek to ensure that their investment in information technology facilitates strategic and tactical goals" (Debreceny, 2013, p. 129), is considered a subset of a broader corporate governance that is centered around IT'S role in an organization, particularly in the area of having appropriate organizational structures that promote the strategic alignment of organizational goals and IT outcomes, risk management, value and performance measurements (Wilkin & Chenhall, 2010). A new stream of research has emerged investigating the various dimensions of information security governance in connection with third party assurances that aim to build trust with outside stakeholders of an organization. The integration of risk and information security management principles in IT governance that interconnect with other frameworks provides ample ground for research. Yet much is left to examine regarding the role of IT governance and risk management (Debreceny, 2013). Despite the acknowledgements from organizations of the potential value of establishing information security standards such as ISO 27001, organizations may be reluctant to undertake such an enormous endeavor due to the costs associated with the benefits of implementations and the lack of knowledge of its cost/benefit ratio (Fenz, Ekelhart, & Neubauer, 2011). On the other hand, other studies provide evidence that assurances and third party security seals impacts the levels of trust on a company's ability to safeguard data and information (Huang, Shen, Yen, & Chou, 2011). As such, further steps should be taken to evaluate the validity in terms of risk mitigation value of such assurances.

This chapter aims to investigate and validate the impact of third party IT Governance assurances on enterprise risks as perceived by external investors. Although both internal and external methods have been offered by the literature to evaluate the value of technology, studies suggest that the relationship between IT investments and financial performance is "marginally, but significantly, stronger in studies that employ market measures rather than accounting measures of financial performance" (Lim, Dehning, Richardson, & Smith, 2011). Thus, the evaluation of perceived risks by market measures would be a viable measurement of a company's risk status.

The following research questions are explored in this study:

- Does the external assurance of a company's IT Governance result in an increase of market valuation for a publicly traded company?

- Does the external assurance of a company's IT Governance result in a decrease of systematic risk for a publicly traded company?
- What firm characteristics moderate the impact of IT Governance assurances?

The rest of this study is organized as follows: a summary of the literature is presented on the business value and risk of external IT Governance assurances; a theory-based research model is offered; proposed hypotheses are developed; the methodology is detailed; and, results are offered followed by the study's contributions and suggestions for future research.

4.3 Information Security Management Systems Alignment to Enterprise Strategy

The critical importance of the protection of organizational assets and operations is unchallenged and often calculated as the value of avoiding costs associated with security incidents (Tsiakis & Stephanides, 2005). However, researchers suggest that a risk-centric approach that is in alignment with business strategies is necessary to develop core-competencies (Fakhri, Fahimah, Ibrahim, & others, 2015). Business organizations must think in terms of risk-intelligence as a forward looking-tool in determining business survival, success and relevance (Tilman, 2012). As Tilman further describes, a new required business competence that goes beyond simple risk-management, can provide competitive advantages by effectively using "forward-looking risk concepts and tools in making better decisions, alleviating threats, capitalizing on opportunities, and creating lasting value." (p. 1). A risk-intelligent organization aligns its vision, strategic value positions with its enterprise risk mitigation goals in governance structures that encompass the entire organization, including the IS components. Gonzalez, Mahmood, Gemoets and Hall (2009) suggest the existence of risk-centric determinants along with its respective direct and moderating effects on competitive advantage. Caralli (2006) suggests that operational resiliency can only be achieved through the proper alignment of best-practices frameworks such as ISO 27001 and COBIT. Furthermore, Caralli, Allen Stevens, Wilke and Wilson (2004) evidence that misalignment of strategic drivers with security can bring undesirable business volatility. Without the proper alignment of security with corporate strategy, businesses fail to establish information security management systems to not only protect their information assets, but to potentially develop competitive advantages. Consequently, the

establishment of an IT Governance structure does not only help mitigate risk in an organization, but it may be able to provide core-competencies to a business.

Research has evidenced that IT Governance frameworks are difficult to implement due to factors that include human elements and organizational culture challenges (Ashenden, 2008; Vladislav V Fomin, 2008). Given the intensive resources required to address enterprise risk management, it is not surprising that studies exhibiting a majority of U.S. businesses lacking of enterprise risk strategies cite "competing priorities", "insufficient resources" and "lack of value" as the main barriers for establishing risk management initiatives (Beasley, Branson, & Hancock, 2009). In addition to being challenging to implement, the notion that security initiatives may provide low-value to an organization by top executive deprioritizes investments in the area (Lima, Neuman de Souza, Branco, & Ribas, 2013). Indeed, while risk management activities have been evidenced to lead to shareholder value, offsetting costs have to be considered (Fatemi & Luft, 2002). The perceived value of IT governance, however, is not evident in the literature. While there is a plethora of research on the damaging effects of security breaches (e.g. Campbell, Gordon, Loeb, & Zhou, 2003; Cardenas, Coronado, Donald, Parra, & Mahmood, 2012; Cavusoglu, Mishra, & Raghunathan, 2004; Garg, Curtis, & Halper, 2003; Goel & Shawky, 2009), there are few studies that address the value of IT Governance (Debreceny, 2013). Specifically, there is only one study that evaluates the investor reaction of IT Governance certifications (Tejay & Shoraka, 2011) with no positive market valuation effects. However, this study is limited to only ISO 27001 certifications with 5 years of data. In addition, this study did not include the assessment of risk profile changes as a result of IT Governance implementations. As such, this study aims to fulfill a gap in the literature better described by the Journal of Information Systems Senior Editor, Dr. Debreceny (2013) in its special issue editorial for IT Governance:

> *"Other areas of research that are important in the AIS domain and that impact on ITG include IT internal controls, value realization from IT investment, ERP systems, IT audit, continuous monitoring, and business process management to pick just a few…. Indeed, what are the returns from investment in ITG itself? How does ITG maturity correlate with key entity-level metrics?" (pp. 130- 132)*

An emerging debate has risen regarding the right approach to assess the value of security initiatives (Daneva, 2006). Traditional methods such as the Annual Loss Expectancy method (Berinato,

2002) and Cost-Benefit Analysis (Mercuri, 2003) are based on the annualized cost-savings of the probability of occurrence of an event, but are often based on non-empirical analyses. However, other researchers (e.g. Purser, 2004) suggest that the return on investment of security initiatives should also include the value of the reduction in risk associated with such investments. This study aims to examine the value of IT Governance initiatives in a manner consistent with the premise that a firm may be able to lower its risk profile as described next.

4.4 Theoretical Framework and Hypotheses Development

The Resource-Based View (RBV) of the Firm (Barney, 1991; Bharadwaj, 2000) posits that firms derive competitive advantages from resources that are rare and valuable. As exemplified by the literature review, this framework has provided a theoretical basis from which IS capabilities have been examined to explore competitive advantages (D. Q. Chen et al., 2010). Thus, I draw from the RBV to analyze firm performance in terms of risk in comparison to the overall market to conduct this study.

As previously described, financial economics provides a perspective of risk that can be conceptualized in two dimensions: systematic, which represents the risk associated with general market conditions, and unsystematic risk, which is unique and specific to a firm (Dewan & Ren, 2007). Using this perspective, unsystematic risk is perceived to be insignificant given the ability to diversify unsystematic risk away. The capital asset pricing model or CAPM (Treynor, 1962) provides a framework in which risk and return are positively related. The theory contends that all assets have a discount rate at which future cash flows produced by such assets should be discounted given the relative risk of the asset. CAPM makes certain assumptions about the investors (e.g. cost-free transactions, risk-averse investors and unlimited investment capacities), and it asserts that all asset-specific risks can be paired by a beta index relative to the market beta of one. This perspective contends that systematic risk, measured by the sensitivity of the expected asset returns to the expected excess of market returns, cannot be mitigated. Thus, a measure of the success of enterprise risk management initiatives can be assessed by its reduction in its beta (Gordon et al., 2009). CAPM remains fairly popular given its simplicity and utility in a variety of scenarios despite its flaws when compared to more robust methodologies (Fama & French, 2004). Another theoretical basis of this study is the Market Efficiency Hypothesis, in which financial markets are

presumed to be information-efficient. As such, investors cannot consistently achieve returns in excess of average market returns on a risk-adjusted basis, given the information available at the time the investment is made (Fama, 1970). This study presumes that information in the U.S. travels rather efficiently; thus, the potential effect of any public announcements made by publicly traded companies should be reflected in stock market reactions.

Figure 4.1 depicts the proposed model for this study, based on Dewan and Ren's (2007)'s Risk-Adjusted Market Model and expanded as follows:

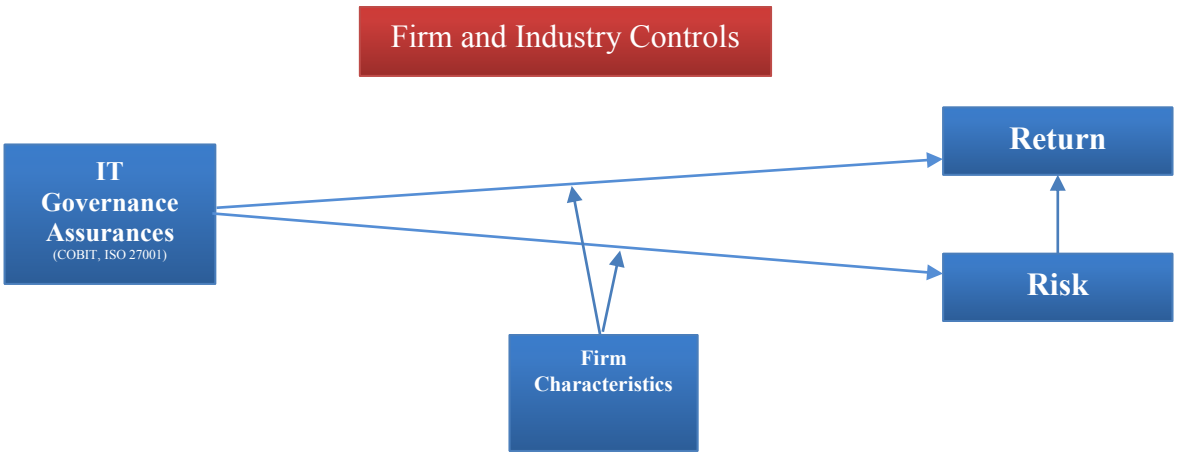

Figure 4.1 Proposed Model.

4.4.1 External IT Governance assurances effects on Market Value and Enterprise Risk

There is an emerging stream of literature that posits that IT security initiatives that align enterprise security with strategic goals can provide competitive advantages that are rare and valuable. If the security breaches have a negative effect on a firm's value breaches (e.g. Campbell et al., 2003; Cardenas et al., 2012; Cavusoglu et al., 2004; Garg et al., 2003; Goel & Shawky, 2009), the prevention of such incidents should theoretically provide an opposite effect. Research also suggests that IT Governance initiatives can add competitive advantages (R. Caralli, 2006; Gonzales et al., 2009). Such competitive advantages

should be perceived by investors in an efficient market place and quantified in a firm's market valuation (Fama, 1970; Fama & French, 2004). As such the following hypothesis is offered:

H1: Firms with public announcements of external IT Governance assurances will exhibit an increase of market valuation as measured by abnormal market returns.

Research suggests that IT Governance initiatives can also change the risk profile of a firm (R. Caralli, 2006). Evidence also exists that lack of IT Governance can result in business volatility (R. A. Caralli et al., 2004); As such, investments in IT Governance initiatives should have the opposite effect as offered by the following hypothesis:

H2: Firms with public announcements of IT Governance assurances will exhibit a decrease in a company's systematic risk.

Research suggests that implementation of IT Governance frameworks is resource-intensive and challenging (Ashenden, 2008; Vladislav V Fomin, 2008). The intensity of implementation of new process and policies to achieve a certification is different than a renewal. The different available types of certifications may also be perceived differently by investors given the issuing authorities that are involved. As such the following hypotheses are offered:

H3: A firm's systematic risk change after a public announcement of an IT Governance assurance certification will be dependent on whether the certification is new or a renewal.

H4: A firm's systematic risk change after a public announcement of an assurance certification will be dependent on the type of certification.

4.5 Methodology

The target sample of this study was U.S. publicly traded companies who announced an IT Governance certification or assurance update on or after the year 2005. To collect this sample, a search was performed on the Lexis/Nexis Academic service and Google News. The search terms "implement", "obtain", "reach", "certified" in junction with the terms "NYSE", "AMEX","NASDAQ", in junction as well with the terms "ISO 27001", "COBIT", "SSAE 16", "SAS 70", "SOC 2", "SOC 3". Subsequently, each press release were inspected to verify that a U.S. publicly traded company was indeed obtaining such IT Governance assurance and for collection of corporation name, trading ticker, date of announcement,

scope, venue, degree of implementation. Announcements within 30 days of each other were consolidated to the 1st occurrence. Consistent with prior studies (Dewan et al., 2007), announcements were eliminated if the Company had less than 120 days of trading history prior and after the events, no data existed at the Center for Research in Security Prices (CRSP) or confounding announcements within a three-day window. After elimination of several announcement due to cited factors, a total of 73 firms with public announcements were rendered valid for analysis.

4.5.1 Risk-Adjusted Market Model Variables and Analysis

In order to jointly examine the effect of risk and return for the events, this study adopts Dewan and Ren's (2007)'s Risk-Adjusted Market Model and expands it as follows:

$$R_{it} = \alpha_i + \alpha'_i D_t + \beta_i R_{mt} + \beta'_i D_t R_{mt} + \beta_i R_{mt} + \varepsilon_{it} \quad (4.1)$$

Under this model, R_{it} represents stock returns on the market portfolio R_{mt}. The dummy variable Dt represents the pre (value 0) and post event (value 1) window, providing an opportunity to measure the parameters α'_i and β_i' to measure the value of alpha and beta respectively. The analysis uses 120 trading days to calculate the pre-event and post-event estimation window to allow the segregation of return and risk effects. The event window is conducted based on t, t±1 trading days. Since both risk and return are considered to be closely correlated, heteroscedasticity may be suspected. As such, an OLS regression with robust standard errors that estimates the asymptomatic covariance matrix of the estimates is a more adequate methodology to address normality, heteroscedasticity and large residual concerns (White, 1980). The model is applied to the data set for each firm in order to obtain parameter estimates. Once the model contained in equation 4.1 was applied to all the firms, the resulting coefficients α_i and $\beta_i R_{mt}$ along with the actual realized return R_{it} were used to calculate the corresponding abnormal returns (AR_{it}), or the deviation of realized returns from the expected returns, for each firm. Equation 4.2 depicts the calculation of abnormal returns:

$$AR_{it} = R_{it} - (\alpha_i + \beta_i R_{mt}) \quad (4.2)$$

For purposes of this study, the cumulative abnormal return (CAR_i) variable for firm i was calculated by summing the abnormal returns for the 3-day event window containing the announcement day plus and minus 1 day (-1,0,1). This variable is subsequently aggregated as an average ($\bar{CAR}$) across all firms or across firms within subgroups (e.g. firms that obtained new certification versus renewals) as depicted in Equation 4.3:

$$\bar{CAR} = \frac{1}{N}\sum_{i=1}^{N} CAR_i \quad (4.3)$$

To provide further insight into the results, a cross sectional analysis relating risk changes to various event and firm characteristics is conducted. This analysis will examine the determinants of total risk as depicted in Equation 4.4:

$$\Delta SysRisk_{it} = \alpha_0 + \alpha_1 PreSysRisk_{it} + \alpha_2 Ret_{it} + \alpha_3 New_{it} + \alpha_4 SOC1_{it} + \alpha_5 SOC2_{it} + \alpha_6 FirmSize_{it} + \varepsilon_{it} \quad (4.4)$$

Where for each company i at time t: "PreSysRisk" represents the systematic risk that existed in the estimation period prior to the event as calculated by equation 3.1. "Ret" represents the average return over the prior 120 days, included given the hypothesis that returns are associated with risk. "New" represents a dummy variable of 1 for a new assurance certification or 0 for an updated one. "SOC1" represents a dummy variable coded with 1 for SOC 1 assurance statements obtained based on SAS 70 or SSAE 16 standards type I or II. Similarly, "SOC2" represents a dummy variable coded with 1 for SOC 2 assurance statements. The reference represents those announcements containing ISO-27001 certifications. Finally, previous literature suggests that certain firm characteristics may influence a company's overall risk (Bharadwaj et al., 1999; K. C. W. Chen & Lee, 1993; Dewan et al., 2007; Otim et

al., 2012); For control variables, FirmSize, operationalized as the logarithm of market value of the firm on the event day.

4.6 Descriptive Statistics

4.6.1 General Descriptive Statistics

Table 4.1 contains a classification summary by industry and enterprise system characteristics contained in the 73 public announcement collected for analysis.

Table 4.1. Classification Summary by Industry and Types of Assurance Statements

	Manufac.	Transport	Retail	Financial	Services	Other	Total
New	10	6	2	4	27	5	***54***
Update	3	4	0	0	12	0	***19***
ISO 27001	9	6	1	2	30	4	***52***
SSAE 16 (SOC 1)	3	2	1	2	5	1	***14***
SSAE 16 (SOC 2)	2	2	0	0	6	0	***10***

4.6.2 Moving Average Variance of Stock Market Returns

Figure 4.2 illustrates the average variance of the difference of stock market returns minus the market returns after announcements of IS Governance certifications. This moving average is based on the average of the prior 120 days before the trading day depicted in the graph, relative to the announcement day. The graph displays a downward departure in total stock variance, normally considered a firm's total risk which encompasses both systematic and unsystematic risk. Figure 4.3 illustrates the average variance of stock market returns after announcements of new assurance certifications versus announcements. The graph displays a difference in average variance, but not a sharp contrast in change as a result of the announcement. Figures 4.4, 4.5 and 4.6 display the average variance of stock returns after announcements of different types of IS Governance assurance statements. While ISO 27001 certifications

do not seem to have a visual difference, absent of appropriate statistical analysis to be conducted in the next section, announcements of SOC 1 and SOC 2 assurance statements by firms display a contrast in the moving average of the stock return variance for the firms contrasted in the graphs.

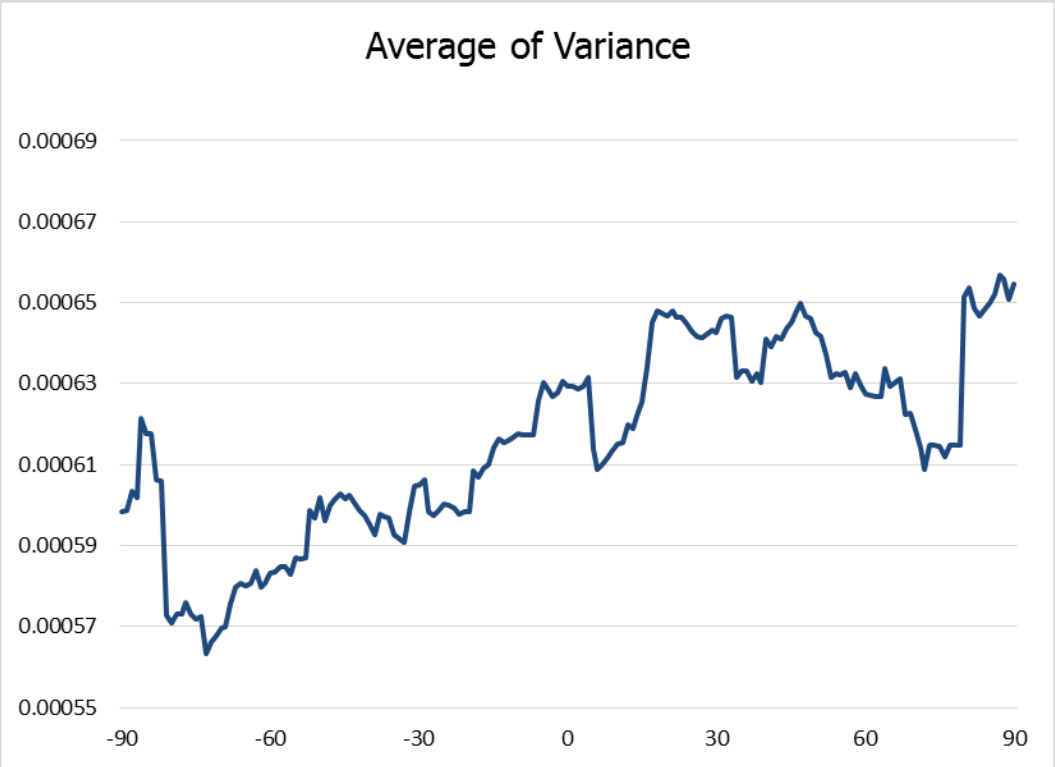

Figure 4.2 Average of Return Variance after IS Governance Announcements

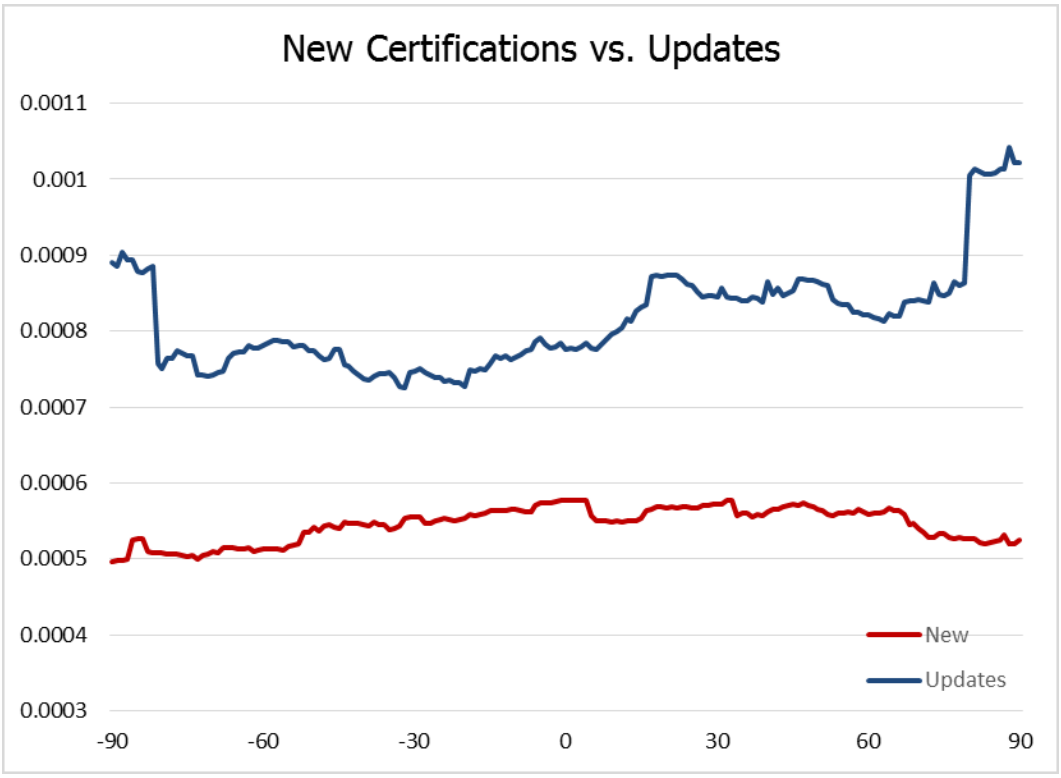

Figure 4.3 Average of Return Variance after IS Governance Announcements-New vs. Updates

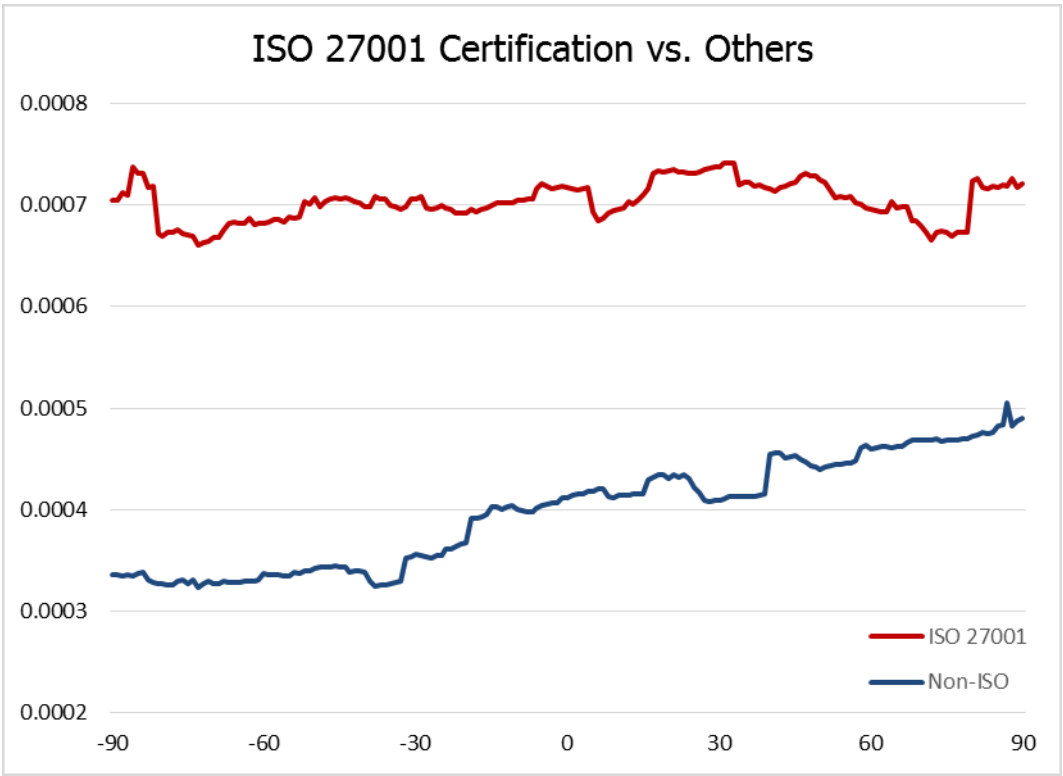

Figure 4.4 Average of Return Variance after IS Governance Announcements-ISO 27001 vs. Others

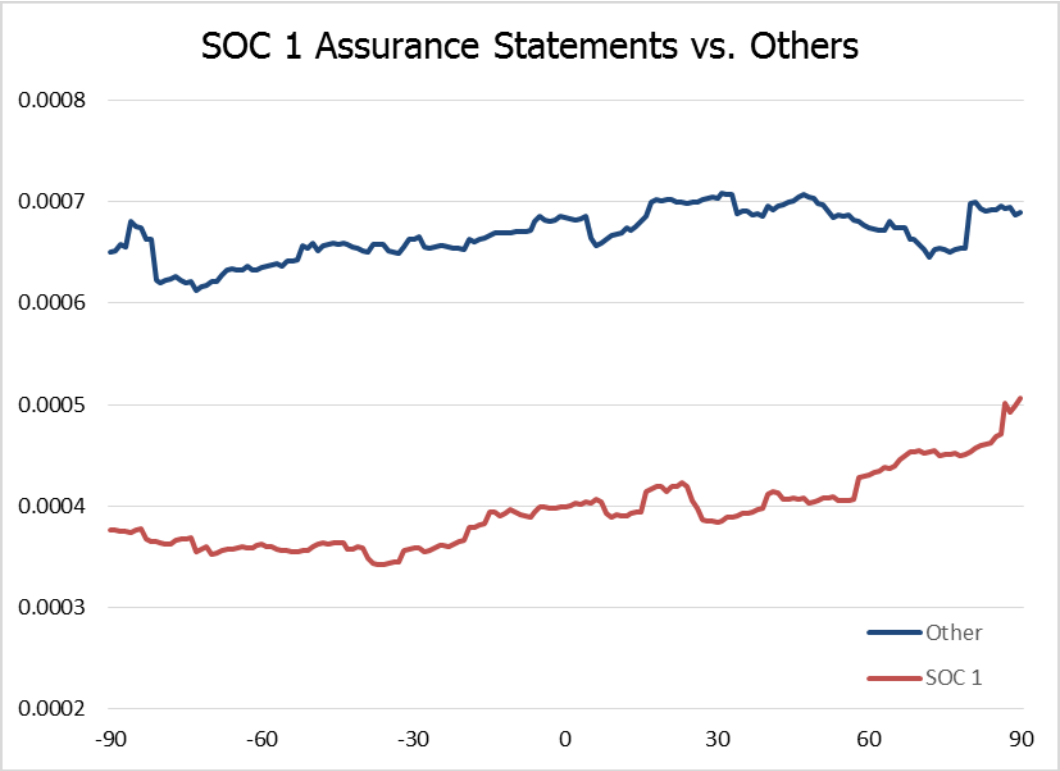

Figure 4.5 Average of Return Variance after IS Governance Announcements-SOC 1 vs. Others

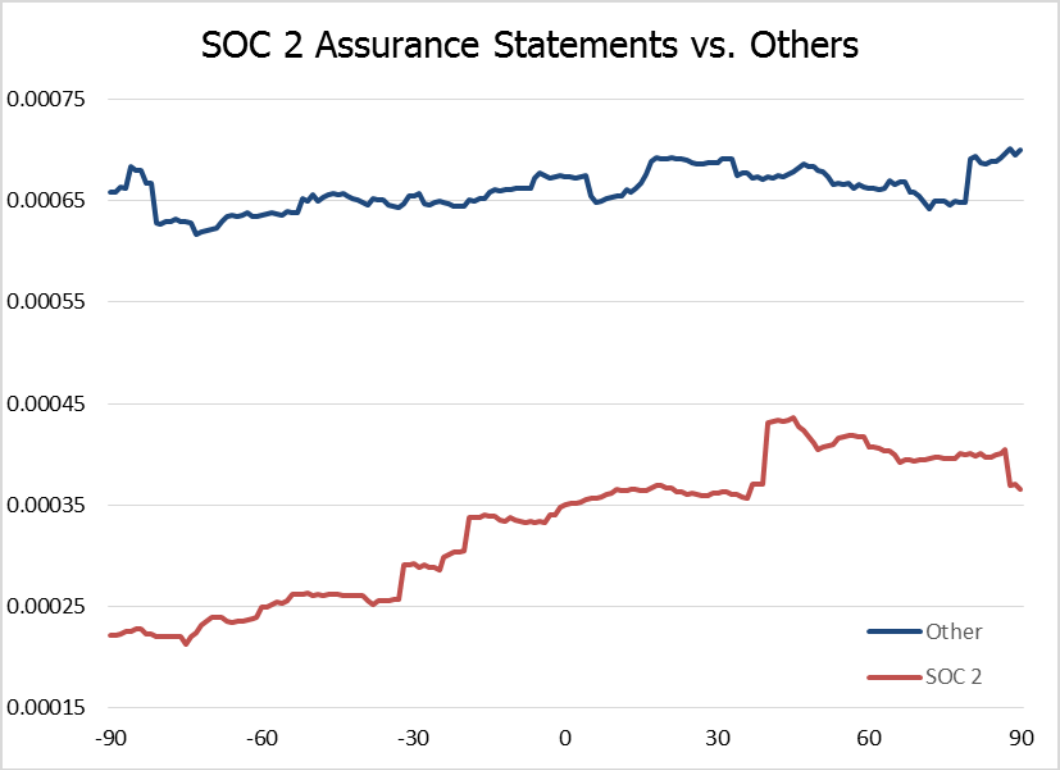

Figure 4.6 Average of Return Variance after IS Governance Announcements-SOC 2 vs. Others

4.6.3 Abnormal Returns and Cumulative Abnormal Returns

The risk-adjusted marked model contained in equation 4.1 was applied to the collected sample in order calculate each firm's parameter estimates. Once the model was applied to the data set for each firm to calculate the corresponding expected returns and the beta coefficients, Equation 4.2 and 4.3 to calculate the corresponding abnormal returns and CĀR for the entire group of firms. In addition, firms were grouped according to types of IS Governance certifications to derive further information. Table 4.2 depicts a summary of the abnormal returns averaged by the different classifications of system characteristics, as well as the trading day relative to the announcement day 0. The table also contains the minimum and maximum abnormal returns observed in the respective classification group. The largest abnormal returns observed for any given announcement are -9.9% on the negative side 10% for the positive side. The corresponding CĀR are -13.7% and 13.2%.

Table 4.2. Summary of Abnormal Returns and CĀR classified by Certification Type

	t= -1			t=0			t=1			CĀR		
	$\bar{x}$	Min	Max	$\bar{x}$	min	max	$\bar{x}$	min	max	$\bar{x}$	min	max
General	-0.003	-0.073	0.100	0.000	-0.071	0.084	-0.002	-0.099	0.069	-0.005	-0.137	0.132
New	-0.002	-0.073	0.076	0.001	-0.071	0.084	0.001	-0.069	0.069	0.000	-0.101	0.132
Update	-0.005	-0.047	0.100	-0.005	-0.060	0.036	0.011	-0.099	0.036	-0.021	-0.137	0.068
ISO 27001	-0.004	-0.073	0.100	0.001	-0.071	0.084	-0.005	-0.099	0.052	-0.008	-0.137	0.132
SOC 1	-0.004	-0.031	0.022	-0.002	-0.023	0.013	0.002	-0.049	0.033	-0.004	-0.101	0.044
SOC 2	0.009	-0.026	0.076	-0.004	-0.052	0.017	0.009	-0.010	0.069	0.014	-0.088	0.091

4.7 Hypothesis Testing and Empirical Results

4.7.1 Effect of IT Governance Assurance on Market Value

In order to test Hypothesis 1 (H1) which posits that firms with public announcements of IT Governance Certifications will exhibit an increase of market valuation as measured by abnormal market returns, a t-Test with 95% confidence interval is conducted on the abnormal returns for days -1, 0 and 1 as well as the cumulative abnormal return for the sample size of 73 companies. In addition, to further explore the reactions based on different types of certifications, the same t-test is applied to eight subgroups that follow the system characteristics classification described before. Table 4.3 provides a summary of the statistical analysis to test H1. The average abnormal return for the sample group was 0, 0 and 0 on days -1, 0 and 1 respectively, all with non-significant p-values (0.31, 0.88, 0..48). The average cumulative abnormal return for the sample is not different than 0, also with non-significant p-value (0.27). Furthermore, for the exception the cumulative abnormal return for the subgroup of updated or renewed certifications which exhibited a 2% lower abnormal return than expected (p-value of 0.05), none of the other treatment tests provide support for H1.

Table 4.3. T-Test Results for Abnormal Returns and CĀR classified by Certification Type

	t= -1			t=0			t=1			CĀR		
	$\bar{x}$	*t*-value	Pr > t	$\bar{x}$	*t*-value	Pr > t	$\bar{x}$	*t*-value	Pr > t	$\bar{x}$	*t*-value	Pr > t
General	0.00	-1.03	0.31	0.00	-0.15	0.88	0.00	-0.71	0.48	-0.01	-1.11	0.27
New	0.00	-0.69	0.49	0.00	0.35	0.73	0.00	0.32	0.75	0.00	0.01	0.99
Update	-0.01	-0.77	0.45	0.00	-0.90	0.38	0.01	-1.67	0.11	-0.02	-2.10	0.05
ISO 27001	0.00	-1.20	0.24	0.00	0.22	0.83	-0.01	-1.37	0.18	-0.01	-1.54	0.13
SOC 1	0.00	-0.91	0.38	0.00	0.85	0.41	0.00	0.33	0.74	0.00	-0.46	0.65
SOC 2	0.01	1.00	0.34	0.00	-0.67	0.52	0.01	1.29	0.23	0.01	0.86	0.41

4.7.2 Effect of IT Governance Assurance on Systematic Risk

Hypothesis 2 (H2) posits that Firms with public announcements of IT Governance assurances will exhibit a decrease in a company's systematic risk. Equation 4.1 was applied to the entire sample group containing 238 trading days (-120 to -2 and 2 to 120) for 73 companies, for the exception of 1 company missing 12 trading days of post-event data. A total of 17,261 observations were used for this equation. The beta coefficients for both $\beta_i R_{mt}$ and $\beta'_i D_t R_{mt}$ were used to compare the pre-event and post-event systematic risk. The analysis of variance for the model was found statistically adequate with an F-Value of 1,564 (Pr > F of <.0001), and an adjusted R^2 of 0.2136. The resulting beta coefficient for the pre-event was found to be significant at a Pr > |t| value of less than 0.0001 with corresponding betas of β_i=1.02581 and the post-event was non-significant $\beta'_i D_t$ = 0.00592, a reduction in systematic risk (β) of 1.00 after the announcement. The non-significance of the post-event beta coefficient indicates there is a clear change in beta as a result of the event in support of the hypothesis. Figure 4.7 displays a graph with the mean agreement points of systematic risk before the announcement and after the announcements.

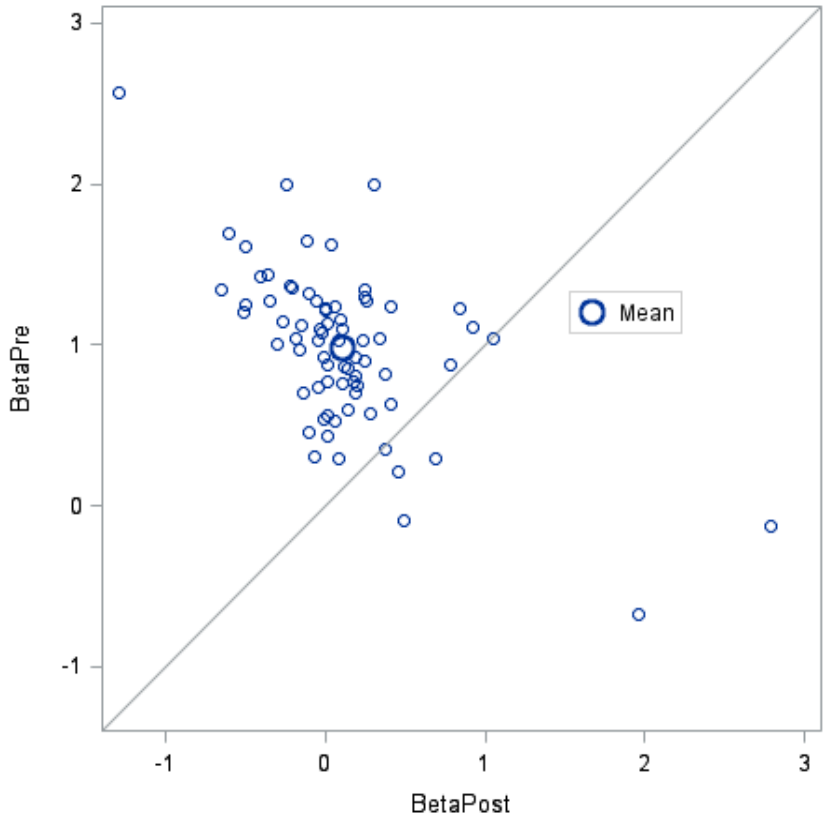

Figure 4.7 Systematic Risk Pre-Event and Post-Event Agreement Graph

To further test this hypothesis, Equation 4.1 was applied to each one of the companies to generate individual firm estimates for pre-event and post-event beta coefficients. A t-test analysis with a 95% lower confidence interval from the mean was conducted to determine the significance of their difference. The results exhibit a reduction in post-event beta of -0.8683 ($Pr < t < .0001$). For robustness purposes, Wilcoxon signed-rank test was also conducted providing supporting results with a median systematic risk reduction (β) of 0.8647 and a mean systematic risk reduction (β) of -0.8683 (Wilcoxon's $W = 185$, $n=73$, $Pr >= |S| <.0001$). As such, H2 is supported, firms with public announcements of IT Governance assurances exhibit a decrease in a company's systematic risk (β).

4.7.3 Effect of IT Governance Assurance Characteristics on Systematic Risk

Hypotheses 3 and 4 posit that a firm's systematic risk reduction exhibited after a public announcement of an IT Governance assurance will be affected by whether the certification is new or updated (H3) and the type of certification (H4). In order to test these hypotheses, Equation 4.4 was applied as described in the methodology section. A correlation analysis was conducted to test for multicollinearity. Table 4.4 illustrates the correlation matrix of the variables contained in the equation. No variables exhibited problematic correlations that may distort the precision of coefficient parameters.

Table 4.4. Correlation Matrix for Predictive Variables for Systematic Risk Difference

Pearson Correlation Coefficients, N = 73 Prob > |r| under H0: Rho=0							
	SysRiskDiff	**BetaPre**	**RETSUM**	**New**	**SOC1**	**SOC2**	**FirmSize**
SysRiskDiff	1	-0.89064	-0.14166	-0.19944	0.01624	-0.08527	-0.1637
		<.0001	0.2319	0.0907	0.8915	0.4732	0.1664
BetaPre	-0.89064	1	0.08995	0.20094	0.02316	0.06369	0.11737
	<.0001		0.4492	0.0883	0.8458	0.5925	0.3227
RETSUM	-0.14166	0.08995	1	0.01709	-0.18703	-0.00934	0.09468
	0.2319	0.4492		0.8859	0.1131	0.9375	0.4256
New	-0.19944	0.20094	0.01709	1	0.13035	0.05473	0.07305
	0.0907	0.0883	0.8859		0.2717	0.6456	0.5391
SOC1	0.01624	0.02316	-0.18703	0.13035	1	-0.09288	0.00896
	0.8915	0.8458	0.1131	0.2717		0.4345	0.9401
SOC2	-0.08527	0.06369	-0.00934	0.05473	-0.09288	1	0.24447
	0.4732	0.5925	0.9375	0.6456	0.4345		0.0371
FirmSize	-0.1637	0.11737	0.09468	0.07305	0.00896	0.24447	1
	0.1664	0.3227	0.4256	0.5391	0.9401	0.0371	

Table 4.5 contains the resulting regression statistics for the predicting variables for systematic risk differences using Equation 4.4

Table 4.5. IT Governance Certification Characteristics Regression Results

Heteroscedasticity Consistent Parameter Estimates					
Variable	**DF**	**Parameter Estimate**	**Standard Error**	**t Value**	**Pr > |t|**
Intercept	1	1.15803	0.51634	2.24	0.0283
BetaPre	1	-1.62664	0.15551	-10.46	<.0001
Retsum	1	-0.15716	0.19017	-0.83	0.4115
New	1	-0.04601	0.1271	-0.36	0.7185
SOC1	1	0.06729	0.10117	0.67	0.5083
SOC2	1	-0.03643	0.09422	-0.39	0.7002
FirmSize	1	-0.01875	0.01891	-0.99	0.3251

F Value = 44.39 Pr > F <.0001, Root MSE=.4317, Adj. R2 = .7859

Given the above cited results, H3 is not supported, firms with public announcement of new assurance certifications do not exhibit a difference in the systematic risk change from those firms that announced updates to already existing certifications. H4 is not supported, a firm's systematic risk change after a public announcement of an assurance certification does not vary on the type of certification. While the intercept representing ISO 27001 shows a significant estimate ($Pr > |t| = .0283$), SOC 1 or SOC 2 certification types do not exhibit a statistically significant change in the risk profiles. Prior systematic risk has the most significant impact in post-event risk reduction.

Table 4.4 summarizes the findings:

Table 4.4. Summary of Findings

Index	Hypothesized	Findings	Exhibit
H1	Higher Abnormal Returns	Not Supported	None
H2	Lower Systematic Risk	Supported	1.0 Lower post-event beta for all systems
H3	New vs Updates	Not Supported	No Significant Changes
H4	Different Types of Certificates	Not Supported	No Significant Changes

4.8 Conclusion

4.8.1 Implications and Future Research

Businesses all around the globe are increasingly concerned with the cyber risks that exist today given the advent of new technologies that are dependent on an interconnected world wide web. National efforts in the U.S. have aimed to monitor the increasing dependence on information technology through the enactment of legislative initiatives that create a partnerships between the public and private sector to protect enterprises. Information Security Management Systems can mitigate the risks businesses experience in today's turbulent cyber environment. This study investigates examined the impact of third party IT Governance assurances on enterprise risks as perceived by external investors. The results exhibit a reduction in enterprise risk at the systematic level for firms that engage in securing third-party validation of the security systems they have in place.

In terms of hypothesized increase in market value after implementations, the hypothesized abnormal returns are not realized as expected. The findings suggest that implementing IT Governance certifications does not provide higher returns for firms in relation to the rest of the market. However, this study does not compare companies in comparison with peer competitors in the industry which may yield different results. This may be addressed in future research studies. In addition, the sample size of this study may limit the robustness of the test which should also be addressed.

The study finds that implementing IT Governance certifications reduces a firm's systematic risk. A firm's reduction of systematic risk has deep implications. As such, ISMS certifications can not only assist firms to foster trust amongst its customer base and mitigate operational hazards, but it can also transform security into a core competency that may translate into higher performance levels. This finding is of strong importance, in essence, firms exhibit a reduction of half the systematic risk in relation to the overall market. CAPM theory provides that each asset holds an appropriate required return or discount rate at which future cash flows produced by the asset should be discounted given the asset's relative riskiness. A reduction in the discount rate of an asset means that all future cash flows will have greater return. While investors may not perceive that greater market value may be achieved through such implementations, this study suggests that investors consider IT Governance certifications highly transformative for an organization's risk profile in a meaningful, positive manner. Such significant reduction in enterprise risk has profound investment consequences in terms of cost and access to capital by a firm and it is consistent with Purser (2004)'s suggestions that return on investment calculations should also include the value of the reduction in risk that result from the investments.

The study also suggests that there is no difference in the type of certification that is implemented by a firm. However, the sample size and high correlation between SOC 2 and SOC 3 assurance statements prevented a more statistically robust analysis of this phenomenon. Future studies should address this issue by including other type of certifications as well as other firm performance metrics, such us return on investment and return on sales.

The study's finding that a higher market valuation in terms of abnormal returns was not exhibited may imply that investors expect such security initiatives to be the norm at this point of time. Not having an ISMS system in place is penalized by higher systematic levels that, in turn, set different expectations on investment returns for individual companies.

4.8.2 Limitations

This study is based on the premise that, as in other event studies, investors are rational and that capital markets are efficient (Fama, 1970) As a result, this study captures the anticipated reaction to an event that theoretically disseminated to investors in an efficient manner. It also focuses on the initial reaction of investors, as time passes, investor perceptions may change or may be reversed. In addition, event size, price stock, trading volumes, confounding and clustering of events may affect the results of the study. While most of these issues were addressed by adopting widely accepted methods, the removal of confounding events from a sample size may be subjective or affected by the lack of historical news.

This sample only consists of publicly traded companies, as such, it cannot be generalized to other types of organizations. While the sample size is sufficient for statistical analysis and comparable to other IS research studies, a larger sample size may have provided more robustness and permitted the inclusion of additional constructs of interest. The findings of the study do not assess the timing of the adoption in relation to other competitors in the industry, which would provide more insight if addressed in future research. The randomization of the sample may also be affected by the availability of historical news as data was collected up to 9 years after such announcements were made.

REFERENCES

AICPA. (2012). *Statement on Standards for Attestation Engagements 16*. New York.

AICPA. (2013). *Statement on Standards for Attestation Engagements No. 16*. AICPA. Retrieved from http://ssae16.com/

Alchian, A., & Demsetz, H. (1996). Production, information costs, and economic organization. *The Economic Nature of the Firm: A Reader*, 193–216.

Aloini, D., Dulmin, R., & Mininno, V. (2007). Risk management in ERP project introduction: Review of the literature. *Information & Management*, *44*(6), 547–567. http://doi.org/10.1016/j.im.2007.05.004

Ashbaugh-Skaife, H., Collins, D. W., Kinney Jr, W. R., & Lafond, R. (2009). The Effect of SOX Internal Control Deficiencies on Firm Risk and Cost of Equity. *Journal of Accounting Research*, *47*(1), 1–43. http://doi.org/10.1111/j.1475-679X.2008.00315.x

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99.

Baskerville, R., Pawlowski, S., & McLean, E. (2000). Enterprise resource planning and organizational knowledge: patterns of convergence and divergence. In *Proceedings of the twenty first international conference on Information systems* (pp. 396–406). Atlanta, GA, USA: Association for Information Systems. Retrieved from http://dl.acm.org/citation.cfm?id=359640.359767

Beasley, M. S., Branson, B. C., & Hancock, B. V. (2009). ERM: Opportunities for Improvement Take your risk management system to the next level. *Journal of Accountancy*, *208*(3), 28.

Becker, J. U., Greve, G., & Albers, S. (2009). The impact of technological and organizational implementation of CRM on customer acquisition, maintenance, and retention. *International Journal of Research in Marketing*, *26*(3), 207–215. http://doi.org/10.1016/j.ijresmar.2009.03.006

Bell, D. E., & LaPadula, L. J. (1973). *Secure computer systems: Mathematical foundations*. DTIC Document. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=AD0770768

Berinato, S. (2002). Calculated risk. *CSO Magazine*.

Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, *24*(1), 169–196. http://doi.org/10.2307/3250983

Bharadwaj, A. S., Bharadwaj, S. C., & Konsynski, B. R. (1999). Information Technology Effects on Firm Performance as Measured by Tobin's q. *Management Science*, *45*(7), 1008–1024.

Biba, K. J. (1977). *Integrity considerations for secure computer systems*. DTIC Document. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA039324

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, *51*(4), 64–68.

Borgatti, S. P., Everett, M. G., & Freeman, L. C. (2002). *Ucinet for Windows: Software for Social Network Analysis*. Harvard, MA: Analytic Technologies.

Bose, I., Pal, R., & Ye, A. (2008). ERP and SCM systems integration: The case of a valve manufacturer in China. *Information & Management*, *45*(4), 233–241. http://doi.org/10.1016/j.im.2008.02.006

Brazel, J. F., & Dang, L. (2008). The Effect of ERP System Implementations on the Management of Earnings and Earnings Release Dates. *Journal of Information Systems*, *22*(2), 1–21.

Brynjolfsson, E., & Hitt, L. M. (2003). Computing Productivity: Firm-Level Evidence. *Review of Economics and Statistics*, *85*(4), 793–808. http://doi.org/10.1162/003465303772815736

Bumiller, E., & Shanker, T. (2012, October 11). Panetta Warns of Dire Threat of Cyberattack on U.S. *The New York Times*. Retrieved from http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448.

Cao, J., Nicolaou, A. I., & Bhattacharya, S. (2010). A Longitudinal Study of Market and Firm-Level Factors Influencing ERP Systems Adoption and Post-Implementation System Enhancement Options. In *7th International Conference on Enterprise Systems, Accounting, and Logistics (ICESAL)*. Citeseer. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.365.7629&rep=rep1&type=pdf

Caralli, R. (2006). Sustaining Operational Resiliency: A Process Improvement Approach to Security Management. Retrieved from http://repository.cmu.edu/sei/402/

Caralli, R. A., Allen, J. H., Stevens, J. F., Willke, B. J., & Wilson, W. R. (2004). *Managing for enterprise security*. DTIC Document. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA430839

Cardenas, J., Coronado, A., Donald, A., Parra, F., & Mahmood, M. (2012). The Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation. *AMCIS 2012 Proceedings*. Retrieved from http://aisel.aisnet.org/amcis2012/proceedings/StrategicUseIT/7

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Retrieved from https://www.fas.org/sgp/crs/misc/RL32331.pdf

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104.

Chand, D., Hachey, G., Hunton, J., Owhoso, V., & Vasudevan, S. (2005). A balanced scorecard based framework for assessing the strategic impacts of ERP systems. *Computers in Industry*, *56*(6), 558–572. http://doi.org/10.1016/j.compind.2005.02.011

Chang, M.-K., Cheung, W., Cheng, C.-H., & Yeung, J. H. Y. (2008). Understanding ERP system adoption from the user's perspective. *International Journal of Production Economics*, *113*(2), 928–942. http://doi.org/10.1016/j.ijpe.2007.08.011

Chang, S.-I., Wu, C.-C., & Chang, I.-C. (2008). The Development of a Computer Auditing System Sufficient for Sarbanes-Oxley Section 404— A Study on the Purchasing and Expenditure Cycle of the ERP System. *Information Systems Management*, *25*(3), 211–229. http://doi.org/10.1080/10580530802151145

Chapman, C. S., & Kihn, L.-A. (2009). Information system integration, enabling control and performance. *Accounting, Organizations and Society*, *34*(2), 151–169. http://doi.org/10.1016/j.aos.2008.07.003

Chen, C. C. (2011). *Empirical Examination of Sales Research: Meta-Analysis, Social Network and Nomological Network Analyses*. Doctoral Dissertation, University of Texas at Arlington.

Chen, D. Q., Mocker, M., Preston, D. S., & Teubner, A. (2010). Information Systems Strategy: Reconceptualization, Measurement, and Implications. *MIS Quarterly*, *34*(2), 233–A8.

Chen, K. C. W., & Lee, C.-W. J. (1993). Financial Ratios and Corporate Endurance: A Case of the Oil and Gas Industry. *Contemporary Accounting Research*, *9*(2), 667–694.

Coase, R. H. (1937). The Nature of the Firm. *Economica*, *4*(16), 386–405. http://doi.org/10.1111/j.1468-0335.1937.tb00002.x

COBIT 5: Enabling Information. (2013). Rolling Meadows, IL: ISACA.

Compeau, D. R., & Higgins, C. A. (1995). Application of social cognitive theory to training for computer skills. *Information Systems Research*, *6*(2), 118–143.

Cotteleer, M. J., & Bendoly, E. (2006). Order Lead-Time Improvement following Enterprise Information Technology Implementation: An Empirical Study. *MIS Quarterly*, *30*(3), 643–660.

Cronbach, L. J., & Meehl, P. E. (1955). Construct validity in psychological tests. *Psychological Bulletin*, *52*(4), 281–302. http://doi.org/10.1037/h0040957

Daneva, M. (2006). *Applying Real Options Thinking to Information Security in Networked Organizations* (info:eu-repo/semantics/report No. TR-CTI). Enschede: Centre for Telematics and Information Technology, University of Twente. Retrieved from http://doc.utwente.nl/66175/

Debreceny, R. S. (2013). Research on IT Governance, Risk, and Value: Challenges and Opportunities. *Journal of Information Systems*, *27*(1), 129–135. http://doi.org/10.2308/isys-10339

Dehning, B., Richardson, V. J., & Zmud, R. W. (2007). The financial performance effects of IT-based supply chain management systems in manufacturing firms. *Journal of Operations Management*, *25*(4), 806–824. http://doi.org/10.1016/j.jom.2006.09.001

Denning, D. E., & Denning, P. J. (1977). Certification of programs for secure information flow. *Communications of the ACM*, *20*(7), 504–513.

Dewan, S., & Ren, F. (2007). Risk and Return of Information Technology Initiatives: Evidence from Electronic Commerce Announcements. *Information Systems Research*, *18*(4), 370–394.

Dewan, S., Shi, C., & Gurbaxani, V. (2007). Investigating the Risk--Return Relationship of Information Technology Investment: Firm-Level Empirical Analysis. *Management Science*, *53*(12), 1829–1842.

Dorantes, C.-A., Li, C., Peters, G. F., & Richardson, V. J. (2013). The Effect of Enterprise Systems Implementation on the Firm Information Environment. *Contemporary Accounting Research*, *30*(4), 1427–1461. http://doi.org/10.1111/1911-3846.12001

Dos Santos, B. L., Peffers, K., & Mauer, D. C. (1993). The Impact of Information Technology Investment Announcements on the Market Value of the Firm. *Information Systems Research*, *4*(1), 1–23.

Drazin, R., & Ven, A. H. V. de. (1985). Alternative Forms of Fit in Contingency Theory. *Administrative Science Quarterly*, *30*(4), 514–539. http://doi.org/10.2307/2392695

Elmes, M. B., Strong, D. M., & Volkoff, O. (2005). Panoptic empowerment and reflective conformity in enterprise systems-enabled organizations. *Information and Organization*, *15*(1), 1–37. http://doi.org/10.1016/j.infoandorg.2004.12.001

Fakhri, B., Fahimah, N., Ibrahim, J., & others. (2015). Information Security Aligned To Enterprise Management. *Middle East Journal of Business*, *10*(1). Retrieved from http://www.mejb.com/upgrade_flash/Jan2015/Infosecurity.pdf

Fama, E. F. (1970). Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance*, *25*(2), 383–417. http://doi.org/10.2307/2325486

Fama, E. F., & French, K. R. (2004). The Capital Asset Pricing Model: Theory and Evidence. *The Journal of Economic Perspectives*, *18*(3), 25–46.

Fatemi, A., & Luft, C. (2002). Corporate risk management: Costs and benefits. *Global Finance Journal*, *13*(1), 29–38. http://doi.org/10.1016/S1044-0283(02)00037-6

Feldman, R., & Dagan, I. (1995). Knowledge Discovery in Textual Databases (KDT). In *KDD* (Vol. 95, pp. 112–117). Retrieved from http://www.aaai.org/Papers/KDD/1995/KDD95-012.pdf

Feng, M., Li, C., & McVay, S. (2009). Internal control and management guidance. *Journal of Accounting and Economics*, *48*(2–3), 190–209. http://doi.org/10.1016/j.jacceco.2009.09.004

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information Security Risk Management: In Which Security Solutions Is It Worth Investing? *Communications of the Association for Information Systems*, *28*(1), 22.

Field, A. P., & Gillett, R. (2010). How to do a meta-analysis. *British Journal of Mathematical and Statistical Psychology*, *63*(3), 665–694. http://doi.org/10.1348/000711010X502733

Fisher, R. A. (1935). The design of experiments. Retrieved from http://psycnet.apa.org/psycinfo/1939-04964-000

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. *Social Networks*, *1*(3), 215–239. http://doi.org/10.1016/0378-8733(78)90021-7

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT Security Breaches: what do investors think? *Information Systems Security*, *12*(1), 22–33.

Gefen, D., Arik. (2005). A Multi-Level Approach to Measuring the Benefits of an Erp System in Manufacturing Firms. *Information Systems Management*, *22*(1), 18–25.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404–410.

Gonzales, M., Mahmood, A., Gemoets, L., & Hall, L. (2009). Risk and IT factors that Contribute to Competitive Advantage and Corporate Performance. *AMCIS 2009 Proceedings*. Retrieved from http://aisel.aisnet.org/amcis2009/711

González-Pereira, B., Guerrero-Bote, V. P., & Moya-Anegón, F. (2010). A new approach to the metric of journals' scientific prestige: The SJR indicator. *Journal of Informetrics*, *4*(3), 379–391. http://doi.org/10.1016/j.joi.2010.03.002

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, *28*(4), 301–327. http://doi.org/10.1016/j.jaccpubpol.2009.06.006

Grabski, S. V., Leech, S. A., & Schmidt, P. J. (2011). A Review of ERP Research: A Future Agenda for Accounting Information Systems. *Journal of Information Systems*, *25*(1), 37–78. http://doi.org/10.2308/jis.2011.25.1.37

Granlund, M. (2009). *On the interface between accounting and modern information technology*. Turku School of Economics. Retrieved from http://info.tse.fi/julkaisut/vk/Ae13_2009.pdf

Granlund, M., & Malmi, T. (2002). Moderate impact of ERPS on management accounting: a lag or permanent outcome? *Management Accounting Research*, *13*(3), 299–321.

Guest, G., MacQueen, K. M., & Namey, E. E. (2011). *Applied thematic analysis*. Sage. Retrieved from http://books.google.com/books?hl=en&lr=&id=VuWrexznC7sC&oi=fnd&pg=PR13&dq=%22Applied+Thematic+Analysis%22&ots=YaG-D1wf1M&sig=PjKIJPh5sxY-3vJc0iaBiZchU3E

Häkkinen, L., & Hilmola, O.-P. (2008). Life after ERP implementation: Long-term development of user perceptions of system success in an after-sales environment. *Journal of Enterprise Information Management*, *21*(3), 285–310.

Hayes, D. C., Hunton, J. E., & Reck, J. L. (2001). Market Reactions to ERP Implementation Announcements. *Journal of Information Systems*, *15*(1), 3–18.

Hendricks, K. B., Singhal, V. R., & Stratman, J. K. (2007). The impact of enterprise systems on corporate performance: A study of ERP, SCM, and CRM system implementations. *Journal of Operations Management*, *25*(1), 65–82. http://doi.org/10.1016/j.jom.2006.02.002

Hitt, L. M., Wu, D. J., & Xiaoge Zhou. (2002). Investment in Enterprise Resource Planning: Business Impact and Productivity Measures. *Journal of Management Information Systems*, *19*(1), 71–98.

Holsti, O. R. (1969). Content analysis for the social sciences and humanities. Retrieved from http://library.wur.nl/WebQuery/clc/410414

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, *14*(2), 104–115.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), 99–110.

Hoyt, R. E., & Liebenberg, A. P. (2011). The Value of Enterprise Risk Management. *Journal of Risk & Insurance*, *78*(4), 795–822. http://doi.org/10.1111/j.1539-6975.2011.01413.x

Huang, S.-M., Shen, W.-C., Yen, D. C., & Chou, L.-Y. (2011). IT governance: Objectives and assurances in internet banking. *Advances in Accounting*, *27*(2), 406–414. http://doi.org/10.1016/j.adiac.2011.08.001

Hunter, J. E., & Schmidt, F. L. (2000). Fixed Effects vs. Random Effects Meta-Analysis Models: Implications for Cumulative Research Knowledge. *International Journal of Selection and Assessment*, *8*(4), 275–292.

Hunton, J. E., Lippincott, B., & Reck, J. L. (2003). Enterprise resource planning systems: comparing firm performance of adopters and nonadopters. *International Journal of Accounting Information Systems*, *4*(3), 165–184. http://doi.org/10.1016/S1467-0895(03)00008-3

Hunton, J. E., Wright, A. M., & Wright, S. (2004). Are Financial Auditors Overconfident in Their Ability to Assess Risks Associated with Enterprise Resource Planning Systems? *Journal of Information Systems*, *18*(2), 7–28.

ISO/IEC. (2005). *ISO/IEC 17799 Information technology - Security techniques - Code of practice for information security management"*. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO/IEC. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Jaquith, A. (2007). *Security metrics*. Pearson Education. Retrieved from http://books.google.com/books?hl=en&lr=&id=Af8F00gTRN4C&oi=fnd&pg=PP3&dq=%22Security+Metrics%22+Jaquith&ots=NnpWot2KtJ&sig=RWai7RNiYGC5FHWfOrUxtoE89B0

Kallunki, J.-P., Laitinen, E. K., & Silvola, H. (2011). Impact of enterprise resource planning systems on management control systems and firm performance. *International Journal of Accounting Information Systems*, *12*(1), 20–39. http://doi.org/10.1016/j.accinf.2010.02.001

Kelley, K., & Preacher, K. J. (2012). On effect size. *Psychological Methods*, *17*(2), 137–152. http://doi.org/10.1037/a0028086

Kenny, D. A., Kashy, D. A., & Cook, W. L. (2006). Methodology in the Social Sciences. In *Dyadic Data Analysis*. Guilford Press.

Kohli, R., & Devaraj, S. (2003). Measuring Information Technology Payoff: A Meta-Analysis of Structural Variables in Firm-Level Empirical Research. *Information Systems Research*, *14*(2), 127–145. http://doi.org/http://dx.doi.org/10.1287/isre.14.2.127.16019

Ko Hsu, Sylvestre, J., & Sayed, E. N. (2006). Avoiding ERP pitfalls. *Journal of Corporate Accounting & Finance (Wiley)*, *17*(4), 67–74. http://doi.org/10.1002/jcaf.20217

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. http://doi.org/10.2308/jis.2010.24.1.91

Le, H., Schmidt, F. L., Harter, J. K., & Lauver, K. J. (2010). The problem of empirical redundancy of constructs in organizational research: An empirical investigation. *Organizational Behavior and Human Decision Processes*, *112*(2), 112–125. http://doi.org/10.1016/j.obhdp.2010.02.003

Lent, B., Agrawal, R., & Srikant, R. (1997). Discovering Trends in Text Databases. In *KDD* (Vol. 97, pp. 227–230). Retrieved from http://www.aaai.org/Papers/KDD/1997/KDD97-046.pdf

Lima, A. s., Neuman de Souza, J., Branco, E. C., Jr., & Ribas, M. (2013). Towards value-based information security management monitoring. Presented at the Proceedings of the 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), IEEE.

Madapusi, A., & D'Souza, D. (2012). The influence of ERP system implementation on the operational performance of an organization. *International Journal of Information Management*, *32*(1), 24–34. http://doi.org/10.1016/j.ijinfomgt.2011.06.004

Mathrani, S., & Mathrani, A. (2013). Utilizing enterprise systems for managing enterprise risks. *Computers in Industry*, *64*(4), 476–483. http://doi.org/10.1016/j.compind.2013.02.002

Maurizio, A., Girolami, L., & Jones, P. (2007). EAI and SOA: factors and methods influencing the integration of multiple ERP systems (in an SAP environment) to comply with the Sarbanes-Oxley Act. *Journal of Enterprise Information Management*, *20*(1), 14–31. http://doi.org/10.1108/17410390710717110

McCollum, T., Lightle, S. S., & Vallario, C. W. (2003). Segregation of Duties in ERP. *Internal Auditor*, *60*(5), 27–31.

Mercuri, R. T. (2003). Analyzing security costs. *Communications of the ACM*, *46*(6), 15. http://doi.org/10.1145/777313.777327

Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. (2011). When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination. *Info. Sys. Research*, *22*(3), 606–623. http://doi.org/10.1287/isre.1100.0341

Morris, J. J. (2011). The Impact of Enterprise Resource Planning (ERP) Systems on the Effectiveness of Internal Controls over Financial Reporting. *Journal of Information Systems*, *25*(1), 129–157. http://doi.org/10.2308/jis.2011.25.1.129

Morris, J. J., & Laksmana, I. (2010). Measuring the Impact of Enterprise Resource Planning (ERP) Systems on Earnings Management. *Journal of Emerging Technologies in Accounting*, *7*(1), 47–71. http://doi.org/10.2308/jeta.2010.7.1.47

Mundy, J., & Owen, C. A. (2013). The Use of an ERP System to Facilitate Regulatory Compliance. *Information Systems Management*, *30*(3), 182–197. http://doi.org/10.1080/10580530.2013.794601

Ngai, E. W. T., Law, C. C. H., & Wat, F. K. T. (2008). Examining the critical success factors in the adoption of enterprise resource planning. *Computers in Industry*, *59*(6), 548–564. http://doi.org/10.1016/j.compind.2007.12.001

Nicolaou, A. I. (2004). Firm Performance Effects in Relation to the Implementation and Use of Enterprise Resource Planning Systems. *Journal of Information Systems*, *18*(2), 79–105.

Nicolaou, A. I., & Bhattacharya, S. (2006). Organizational performance effects of ERP systems usage: The impact of post-implementation changes. *International Journal of Accounting Information Systems*, *7*(1), 18–35. http://doi.org/10.1016/j.accinf.2005.12.002

Nocco, B. W., & Stulz, R. M. (2006). Enterprise Risk Management: Theory and Practice. *Journal of Applied Corporate Finance*, *18*(4), 8–20. http://doi.org/10.1111/j.1745-6622.2006.00106.x

O'Leary, D. E. (2000). *Enterprise resource planning systems: Systems, life cycle, electronic commerce, and risk*. Cambridge; New York and Melbourne:

Otim, S., Dow, K. E., Grover, V., & Wong, J. A. (2012). The Impact of Information Technology Investments on Downside Risk of the Firm: Alternative Measurement of the Business Value of IT. *Journal of Management Information Systems*, *29*(1), 159–194.

Parent, M., & Reich, B. H. (2009). Governing Information Technology Risk. *California Management Review*, *51*(3), 134–152.

Parra, F., Han, T., Peters, A., & Vidyarthi, P. (2012). A Thematic Trend Analysis of Relationships Among Organizational Behavior Constructs. Presented at the Academy of Management and Business Conference, Boston.

Parra, F., Kirs, P., & Udo, G. (2012). A Trend Analysis of Information Systems Sourcing. Presented at the Decision Science Institute 43rd Annual Meeting, San Francisco, CA.

Poston, R., & Grabski, S. (2001). Financial impacts of enterprise resource planning implementations. *International Journal of Accounting Information Systems*, *2*(4), 271–294. http://doi.org/10.1016/S1467-0895(01)00024-0

PrivacyRights.org. (2013). *Chronology of Data Breaches*. Retrieved from www.privacyrights.org/data-breach

Purser, S. A. (2004). Improving the ROI of the security management process. *Computers & Security*, *23*(7), 542–546.

Robey, D., Ross, J. W., & Boudreau, M.-C. (2002). Learning to Implement Enterprise Systems: An Exploratory Study of the Dialectics of Change. *Journal of Management Information Systems*, *19*(1), 17–46.

Ross, R. (2007). Managing enterprise security risk with NIST standards. *Computer*, *40*(8), 88–91.

Roztocki, N., & Weistroffer, H. R. (2009). The impact of enterprise application integration on stock prices. *Journal of Enterprise Information Management*, *22*(6), 709–721. http://doi.org/10.1108/17410390910999594

Rubin, E., & Rubin, A. (2013). The impact of Business Intelligence systems on stock return volatility. *Information & Management*, *50*(2–3), 67–75. http://doi.org/10.1016/j.im.2013.01.002

Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *Information Management Journal*, *39*(4), 60–66.

Scapens, R. W., & Jazayeri, M. (2003). ERP systems and management accounting change: opportunities or impacts? A research note. *European Accounting Review*, *12*(1), 201–233.

Schneberger, S., Wade, M., Allen, G., Vance, A., & Eargle, D. (Eds.). (2013). Theories Used in IS Research Wiki. Retrieved from http://istheory.byu.edu

Selznick, P. (1948). Foundations of the Theory of Organization. *American Sociological Review*, *13*(1), 25–35. http://doi.org/10.2307/2086752

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise Security Architecture: A Business-Driven Approach*. Backbeat Books.

Short, J. C., Broberg, J. C., Cogliser, C. C., & Brigham, K. H. (2010). Construct Validation Using Computer-Aided Text Analysis (CATA) An Illustration Using Entrepreneurial Orientation. *Organizational Research Methods*, *13*(2), 320–347. http://doi.org/10.1177/1094428109335949

Sia, S. K., Tang, M., Soh, C., & Boh, W. F. (2002). Enterprise Resource Planning (ERP) Systems As a Technology of Power: Empowerment or Panoptic Control? *SIGMIS Database*, *33*(1), 23–37. http://doi.org/10.1145/504350.504356

Simon, H. A. (1959). Theories of decision-making in economics and behavioral science. *The American Economic Review*, *49*(3), 253–283.

Snow, G. M. Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, § Senate Judiciary Committee, Subcommittee on Crime and Terrorism (2011). Washington, D.C. Retrieved from http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism

Somers, T. m., Nelson, K., & Sprague, R. h. (2001). The impact of critical success factors across the stages of enterprise resource planning implementations. In R. h. Sprague (Ed.), . Presented at the Proceedings of the 34th Annual Hawaii International Conference on System Sciences, IEEE Comput. Soc. Univ. Hawaii College of Bus. Adm Univ. Hawaii College of Bus. Adm.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2013). Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions. *Journal of Information Systems*, 130710125151003. http://doi.org/10.2308/isys-50510

Stoneburner, G. (2001). *SP 800-33. Underlying Technical Models for Information Technology Security*. Gaithersburg, MD, United States: National Institute of Standards & Technology.

Stratopoulos, T. C., Vance, T. W., & Zou, X. (2013). Incentive effects of enterprise systems on the magnitude and detectability of reporting manipulations. *International Journal of Accounting Information Systems*, *14*(1), 39–57. http://doi.org/10.1016/j.accinf.2012.08.001

Sumner, M. (2000). Risk factors in enterprise-wide/ERP projects. *Journal of Information Technology*, *15*(4), 317–327. http://doi.org/10.1080/02683960010009079

Su, Y., & Yang, C. (2010). Why are enterprise resource planning systems indispensable to supply chain management? *European Journal of Operational Research*, *203*(1), 81–94. http://doi.org/10.1016/j.ejor.2009.07.003

Tanriverdi, H., & Ruefli, T. W. (2004). The Role of Information Technology in Risk/Return Relations of Firms. *Journal of the Association for Information Systems*, *5*(11/12), 421–447.

Tejay, G. P. S., & Shoraka, B. (2011). Reducing cyber harassment through *de jure* standards: a study on the lack of the information security management standard adoption in the USA. *International Journal of Management and Decision Making*, *11*(5), 324–343. http://doi.org/10.1504/IJMDM.2011.043407

Tilman, L. M. (2012). Risk Intelligence A Bedrock of Dynamism and Lasting Value Creation. *The European Financial Review*.

Treynor, J. L. (1962). *Toward a Theory of Market Value of Risky Assets*. Unpublished manuscript.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & Security*, *24*(2), 105–108. http://doi.org/10.1016/j.cose.2005.02.001

Vladislav V Fomin, H. J. D. V. (2008). ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption.

Weber, R. A. (1998). *Information Systems Control and Audit* (1st ed.). Pearson Education.

White, H. (1980). A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity. *Econometrica*, *48*(4), 817–838.

Wier, B., Hunton, J., & HassabElnaby, H. R. (2007). Enterprise resource planning systems and non-financial performance incentives: The joint impact on corporate performance. *International Journal of Accounting Information Systems*, *8*(3), 165–190. http://doi.org/10.1016/j.accinf.2007.05.001

Wilkin, C. L., & Chenhall, R. H. (2010). A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems*, *24*(2), 107–146.

Wright, M. (1999). Third generation risk management practices. *Computer Fraud & Security*, *1999*(2), 9–12. http://doi.org/10.1016/S1361-3723(99)80005-0

Wright, S., & Wright, A. M. (2002). Information System Assurance for Enterprise Resource Planning Systems: Unique Risk Considerations. *Journal of Information Systems*, *16*(1), 99–113.

VITA

Fernando Parra is a business information systems expert who obtained his Ph.D. in International Business and Information Systems from the University of Texas at El Paso (UTEP). He has served in different capacities both in the private and public sectors, including The World Trade Center El Paso/Juarez and Walt Disney World. He has played a key role in supporting small to medium-sized businesses with software solutions including ecommerce, HIPAA compliant records management, CRM and ERP in the medical, retail and legal industries. Fernando has served in several honorary boards, including the Association of Information Technology Professionals (Assistant Advisor 2011-Present), Information Systems Doctoral Student Association (President, Vice President and Secretary 2012-Present), El Paso County Civil Service Commission (Commissioner 2006-2008), City of El Paso's IT Advisory Board (Member 2003-2006).

Fernando's research interests include IT Governance, Information Systems Management, Information Systems Audit, Systems Strategy, Security Management, Adoption, Social Media and Organizational Behavior. Fernando has presented peer-reviewed manuscripts in both national and international forums including the Hawaii International Conference on system Sciences (HICSS), American Conference on Information Systems (AMCIS), Decision Science Institute (DSI), Academy of Management (AOM), International Academy of Management and Business (IAMB), and the American Political Science Association (APSA). He is the recipient of the Best Student Paper Award from the International Academy of Management and Business (IAMB) for the San Francisco 2011 conference manuscript titled "On a Firm's Core Competency through Information Systems: A Meta-Analysis".

Fernando strongly believes that as instructors, we have the responsibility to influence tomorrow's business leaders in a transformational way; aligning our educational strategies with those of the institution we serve, fostering the advancement of education, creativeness, artistic production and the promotion of knowledge. He is fully committed to providing service-oriented instruction that is demonstrated by the students' ability to remain engaged in their assignments, their collective comprehension of the subject matter and their ability to apply the absorbed knowledge in real life business scenarios. Fernando was awarded the 2013 "Excellence in Undergraduate Instruction Award" for Information and Decision Sciences by the College of Business Administration at the University of Texas at El Paso.

Fernando Parra also holds a Masters of Information Technology and a Bachelors of Business Administration in Computer Information Systems, both from UTEP.

Permanent address: 919B Agua Caliente Dr.
El Paso, TX 79912

This thesis/dissertation was typed by Fernando Parra Reyes.