2017

Relationship between Corporate Governance and Information Security Governance Effectiveness in United States Corporations

Robert Elliot Davis
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Robert Davis

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Alexandre Lazo, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Jamie Klein, Committee Member, Doctor of Business Administration Faculty

Dr. Reginald Taylor, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Relationship Between Corporate Governance and Information Security Governance Effectiveness in United States Corporations

by

Robert E. Davis

MBA, West Chester University, 1985

BBA, Temple University, 1977

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

September 2017

Abstract

Cyber attackers targeting large corporations achieved a high perimeter penetration success rate during 2013, resulting in many corporations incurring financial losses. Corporate information technology leaders have a fiduciary responsibility to implement information security domain processes that effectually address the challenges for preventing and deterring information security breaches. Grounded in corporate governance theory, the purpose of this correlational study was to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and information security governance (ISG) effectiveness in United States-based corporations. Surveys were used to collect data from 95 strategic and tactical leaders of the 500 largest for-profit United States headquartered corporations. The results of the multiple linear regression indicated the model was able to significantly predict ISG effectiveness, $F(5, 89) = 3.08$, $p = 0.01$, $R^2 = 0.15$. Strategic alignment was the only statistically significant ($t = 2.401$, $p <= 0.018$) predictor. The implications for positive social change include the potential to constructively understand the correlates of ISG effectiveness, thus increasing the propensity for consumer trust and reducing consumers' costs.

Relationship Between Corporate Governance and Information Security Governance Effectiveness in United States Corporations

by

Robert E. Davis

MBA, West Chester University, 1985

BBA, Temple University, 1977

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

September 2017

Dedication

This doctoral study research is dedicated to my family, who has unconditionally supported my aspirations that in turn inspired me to continue my educational journey. To my beloved mother, who values education and through whose encouragement I was able to overcome doctoral program challenges: Thank you. To my pragmatic father, who enjoys reading and through whose gifted books I was able to acquire an appreciation for objectivity when addressing my chosen doctoral research topic: Thank you. To my loved significant other, your home environment oversight ensured completing my doctoral studies with minimal external interference: Thank you. Last, but not least, to my brothers and sons, thank you for sharing your higher education experiences.

Acknowledgments

First and foremost, I thank God for preparing me for this educational journey. I am also grateful for having such a distinguished and supportive doctoral study committee. The committee chair, Dr. Alexandre Lazo, the second committee member, Dr. Jaime Klein, and the University Research Reviewer, Dr. Reginald Taylor, provided the needed advice and guidance in meeting my prospectus, proposal, and final documentation requirements. Dr. Alexandre Lazo, thank you for your patience and support as I completed this paper. Dr. Jaime Klein, thank you for your suggested improvements for enhancing this paper. Dr. Reginald Taylor, thank you for your dedication to achieving high standards and quality for quantitative doctoral study research.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

Given the global business environment, information technology (IT) deployments are indispensable for enabling information reliability, processing efficiency, and communication expediency to acquire and maintain a competitive advantage (Masa'deh, 2013). Because information has measurable value (Hughes, Bon, & Rapp, 2013; Mishra & Mohanty, 2014), data collection, processing, storage, and transmission by organizational employees need appropriate safeguarding (Ahmad, Maynard, & Park, 2014). Safeguarding information mandates addressing information assets protection (IAP) to ensure managerial due care and due diligence (Mohare & Lanjewar, 2012; R. Davis, 2008).

Stemming from fiduciary responsibilities, an IT leader's information systems related due care is what drives appropriate information security due diligence activities (Boyson, 2014; R. Davis, 2008; Whitman & Mattord, 2012). Instituting and sustaining information safeguarding requires a comprehensive organizational program to address cyber threats that can thwart organizational mission achievement (Ahmad et al., 2014; Kushwaha, 2016; Mohare & Lanjewar, 2012). Though information security breaches can emanate from external or internal actions (Crossler et al., 2013; Silic & Back, 2014), enterprise IT leaders should ensure ethical behavior by every individual interacting with the organization's information systems through effectual information security governance (ISG; Boyson, 2014). However, several significant information security breaches have decreased corporate value appropriation (Clark & Harrell, 2013; Silic & Back, 2014).

Problem Statement

With cyber attackers targeting large corporations achieving a 93% success rate during 2013 (Brewer, 2014), IT leaders needed to improve ISG practices (Silic & Back, 2014). Near the end of 2013, the average annualized cybercrime cost of globally surveyed industry sectors was $7.22 million per organization (Brewer, 2014). The general business problem is that many corporations are incurring financial losses due to information security breaches. The specific business problem is that some IT leaders do not know the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations.

Purpose Statement

The purpose of this quantitative correlational study was to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. The targeted population consisted of strategic and tactical leaders of the 500 largest for-profit United States headquartered corporations. The predictor variables were strategic alignment, resource management, risk management, value delivery, and performance measurement implementations. ISG effectiveness was the criterion variable. The implications for positive social change include the potential to understand the correlates of ISG effectiveness better, thus increasing the propensity for consumer trust and reducing consumers' costs.

Nature of the Study

I used a quantitative method for this study. Researchers use the quantitative method to compare group differences or examine the relationship between variables (Frels & Onwuegbuzie, 2013; Ross & Onwuegbuzie, 2014; Welford, Murphy, & Casey, 2012). The quantitative method was more appropriate than qualitative or mixed methods because the focus of the study was to analyze numerical data and infer the results to a larger population. A researcher's qualitative or mixed methods analysis involves considering words to understand the meaning of human actions (Masa'deh, Maqableh, & Karajeh, 2014; Parylo, 2012; Turner, Balmer, & Coverdale, 2013; Welford et al., 2012).

I used a correlational research design. Correlational research enables clarifying or discovering the relationships between variables (Turner et al., 2013). My intention was to identify and examine factors potentially predicting effective ISG, by assessing the ISG implementation extents within five IT Governance Institute (ITGI; 2008) ISG focus areas. Experimental designs (true experiment and quasiexperiment approaches) were inappropriate because I was not collecting data from more than one group, not performing group comparisons among variables, and not seeking a cause-and-effect relationship between variables.

Research Question

What is the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations?

Hypotheses

Null Hypothesis (H_0): There is no significant relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations.

Alternative Hypothesis (H_1): There is a significant relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations.

Theoretical Framework

To implement ISG focus areas effectively, practices for large organizations should reflect corporate governance theoretical principles (De Haes, Grembergen, & Debreceny, 2013; Kearney & Kruger, 2013). Corporate governance by definition is the objectives, strategies, policies, and processes for controlling and directing an enterprise (Kearney & Kruger, 2013; Whitman & Mattord, 2012; Yaokumah, 2013). Corporate governance can constitute a set of rules (Yaokumah & Brown, 2014) or voluntary as well as mandatory actions (Stagliano & Sillup, 2014) governing the relationships between management and stakeholders. Essential constructs underlying the theory are (a) strategic alignment, (b) resource management, (c) risk management, (d) value delivery, and (e) performance measurement (Yaokumah, 2013; Yaokumah & Brown, 2014). As applied to this study, the corporate governance theory holds that I would expect the predictor variables (corporate governance constructs) measured by the Yaokumah (2013) survey

instruments to forecast ISG effectiveness because ISG is a functional subset of corporate governance.

As shown in Figure 1, corporate governance theory is relevant in defining the constructs that help evaluate ISG because corporate governance theory offers a lens for understanding the organizational practices concerning the phenomenon (Yaokumah, 2013). Corporate governance theory application by manager-leaders can affect ISG practices because management concepts address accountability, roles, interactions, activities, and resource use of agents (Yaokumah, 2013). Scholars and practitioners apply corporate governance theory to understand variations in policies, setting priorities among goals, technological and social changes, and managerial hierarchies (Starbuck, 2014). A contextual discussion will take place in the following literature review subsections concerning ISG practices that support corporate governance theory and how corporate governance theory relates to ISG effectiveness.

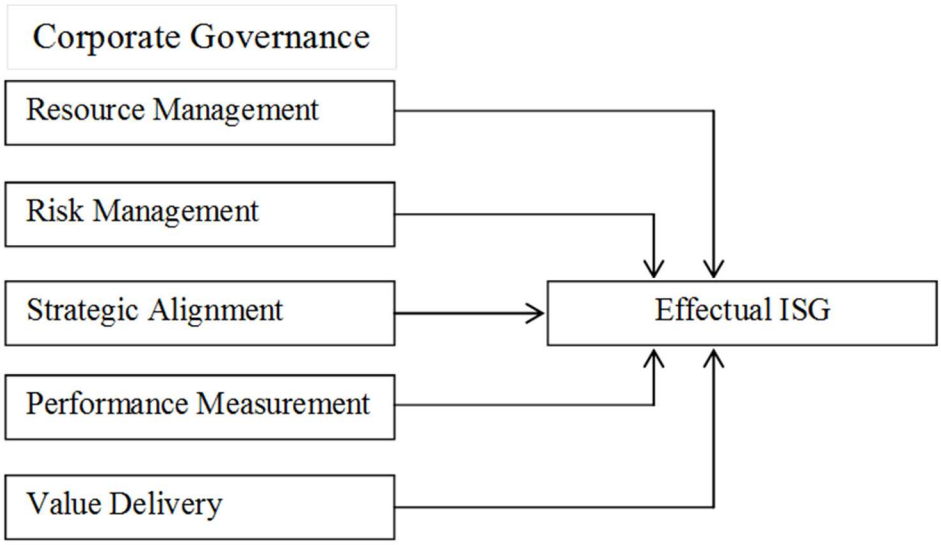

Figure 1. The ISG research theoretical lens. A graphical model of corporate governance theory constructs as it applies to examining effectual ISG.

Operational Definitions

Corporate governance: Corporate governance is a system enabling firms to strategically direct, integratively manage, and holistically control in an entrepreneurial and ethical manner appropriate for each particular context (Hilb, 2012).

Effectual information security governance (effectual ISG): Effectual ISG is the extent to which enterprise leaders ensure information security strategic alignment, value delivery, risk management, performance measurement, and resource management to meet stakeholder expectations (Yaokumah, 2014).

Information assets: Information assets are items of value that contain data (R. Davis, 2012).

Information security: Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (Da Veiga & Martins, 2015; R. Davis, 2012).

Information security governance (ISG): ISG is "a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security [program]" (ITGI, 2008, p. 18).

Performance measurement: Performance measurement involves quantifying, monitoring, and reporting the performance of information security systems, processes, and related activities to ensure achievement of organizational objectives (ITGI, 2008).

Resource management: Resource management represents the intention for optimal investment in and the proper administration of information security resources by manager-leaders (Mohare & Lanjewar, 2012; R. Davis, 2008; Yaokumah, 2013).

Risk management: Risk management reflects principles, approaches, and processes using systematic application (Rasheed, ChangFeng, & Yaqub, 2015).

Strategic alignment: Strategic alignment centers on ensuring enterprise, IT, and information security plan linkage; defining, maintaining, and validating the information security value proposition; and information security operational congruence with business and IT operations (R. Davis, 2008).

Value delivery: Value delivery represents executing the information security value proposition throughout the delivery cycle and ensuring information security delivers asseverated benefits against adopted enterprise strategies (R. Davis, 2008).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions represent unverified values, time, or space perceptions (Bhattacherjee, 2012; Roy & Pacuit, 2013). Scholars and practitioners have abstracted that information security is no longer primarily a technical issue requiring handling solely by operational IT personnel but rather more of a governance concern (Julisch, 2013a; Mohare & Lanjewar, 2012; Whitman & Mattord, 2012). Yaokumah (2013) recommended addressing IAP at the governance level to mitigate organizational technology risks. I accepted this assumption to be true and attempted to omit operational-level management from data collection and analysis while investigating effectual ISG at the strategic and tactical management levels.

Information security strategic planning involves some planning aspects common to the entire organization (Whitman & Mattord, 2012). In particular, the information security planning process should include ensuring the establishment of a mission, vision, and values statement. Upon long-term goals and objectives creation and subsequent strategic plans translation into tactical and operational plans, operationalization occurs (Whitman & Mattord, 2012). Regarding strategic planning, I assumed management's business environment risk assessments would determine information security implementation criticality in the United States.

Data collection occurred through the Internet for this doctoral study. Internet-based survey use enables study participants to complete posed questions through computer network access (Chang & Vowles, 2013). Internet-based survey use should

only prevail if the proposed study participants have access and understand the employed data collection technologies (Yaokumah, 2013). I assumed the intended participants had access to and familiarity with Internet.

Limitations

Limitations reflect potential study weaknesses (Bhattacherjee, 2012; Brutus, Aguinis, & Wassmer, 2013; S. Singh, 2015). My survey response rate was extremely low as a result of the sensitive nature of the ISG study. Previous survey-based research evidence suggested that when collecting data of a sensitive nature, the researcher should expect a very low response rate (Flores, Antonsen, & Ekstedt, 2014; Yaokumah, 2013). The sample selection for the ISG study comprised broad population subcategories (United States business sector types). As such, my research findings might be generalizable to the target population IT leaders.

Delimitations

Delimitations are ambit restrictions in theory application (Bhattacherjee, 2012; Denscombe, 2013). My study ambit was ISG deployments in the United States to assist large corporation strategic- and tactical-level leaders in the enhancement of new and existing information security programs. I focused the study on examining the level to which IT leaders implement strategic alignment, resource management, risk management, value delivery, and performance measurement in generating effectual ISG that prevents and deters information security breaches.

I excluded for-profit small and medium enterprises (SMEs). However, for-profit SMEs proportionately confront information security issues (Cholez & Girard, 2014;

Harris & Patten, 2014). Because most for-profit SMEs do not have the human and financial resources to deploy ISG practices (Cholez & Girard, 2014; Harris & Patten, 2014), I did not include SMEs in the study. Nonetheless, for-profit SME managers who plan to install or have implemented an ISG program may use my study findings for understanding the correlates of ISG effectiveness and associated guidelines.

I excluded not-for-profit organizations. Because for-profit corporate organizational formations occur to generate tangible and intangible wealth for stakeholders while not-for-profit organizations occur to satisfy perceived societal needs (R. Davis, 2008), nonprofit enterprises were not included in the study. Despite the organizational formation difference, nonprofit manager-leaders who are planning deployment or who have deployed an ISG program may use my study findings for understanding the correlates of ISG effectiveness and associated guidelines.

I excluded operational-level management. Operational-level management oversees the day-to-day information security related tasks in most organizations, and their inclusion in the study might have brought some significant perspectives on the ISG research findings (Yaokumah, 2013). However, operational-level management exclusion from the study reflected an assumption that effectual ISG is a strategic and tactical concern more than an operational issue (Yaokumah, 2013). As such, my random participant sample only included strategic- and tactical-level managers.

Significance of the Study

Contribution to Business Practice

The contributions to business practice were an improvement in ISG practice areas to protect information assets more effectively with a concomitant reduction in recovery costs. Effectual ISG counteracts security threats through the deployment of controls enabling ethical and legal managerial responsibilities fulfillment for IAP (R. Davis, 2008; Tarafdar, D'Arcy, Turel, & Gupta, 2015). Scholars have specifically examined ISG implementation maturity in developing countries (Yaokumah, 2014; Yaokumah & Brown, 2014). However, the degree of ISG realization in developed countries has remained an open question (Flores et al., 2014). The results of this study might help IT leaders improve ISG practice areas to protect information assets more effectively with a concomitant reduction in recovery costs.

Implications for Social Change

The implications for positive social change include potential increased trust and reduced costs from electronic commerce (e-commerce) use. Information security breaches can have a detrimental effect on stakeholder satisfaction when an incident result in financial fraud, information tampering, or access denial (Arief, Adzmi, & Gross, 2015). Corporate IT leaders can improve trust for stakeholders in technology containing personally identifiable information through effectual ISG (R. Davis, 2008). More secure IT operations can benefit communities through enhanced governance quality that consequently would increase trust and reduce costs from e-commerce use (Bahmanziari & Odom, 2015; Ludin & Cheng, 2014; Starbuck, 2014; Yaokumah, 2014).

A Review of the Professional and Academic Literature

Similar to any other group formations, corporations reflect personal aims, values, expectations, and sentiments that transform into a culture (Hu, Dinev, Hart, & Cooke, 2012). An enterprise's environment represents all conditions surrounding and affecting organizational endeavors (R. Davis, 2008). Most corporations operate in an environment influenced by perceived stakeholder values as well as the firm's mission, vision, and values (Hu et al., 2012; R. Davis, 2008). Community and organizational ethics and culture, applicable laws, regulations, and policies, as well as industry practices, affect corporate personnel (Hu et al., 2012; R. Davis, 2008).

Managers who interact with the environment endeavor to maintain the corporate culture while attempting to control external and internal forces affecting activities committed to enterprise mission achievement (R. Davis, 2008; Steiger, Hammou, & Galib, 2014). Management typically needs a governance framework that enables organizational alignment, judicious resource allotment, adaptive risk assessments, acceptable value delivery, and accurate performance measurements to address business environment security issues (Mohare & Lanjewar, 2012; R. Davis, 2008). The purpose of this quantitative correlational study was to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement, and ISG effectiveness in United States-based corporations. Considering the above discussion led to the following central hypotheses:

H_0: There is no significant relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations.

H_1: There is a significant relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations.

Literature Review Synopsis

Corporate governance theory was an appropriate theoretical foundation to study ISG (Hu et al., 2012; Whitman & Mattord, 2012; Yaokumah & Brown, 2014). The method used for this research included the foundational governance theory capabilities in providing holistic corporate ISG practices. The chosen theory was relevant in defining the constructs that help evaluate ISG because corporate governance propositions furnish an organizational view and understanding of the phenomenon (Yaokumah, 2013). Deriving constructs from a previously established and proven theory also aids in measures selection as well as furnishes a valid and comprehensive phenomenon understanding (Yaokumah, 2013; Yaokumah & Brown, 2014).

Corporate governance scholars examined management practices, structures, processes, and effectiveness from distinct theoretical perspectives (Yaokumah & Brown, 2014). Various combinations supporting organizational theories best describe effective corporate governance (Htay, Salman, & Meera, 2013; Yaokumah, 2013). Scholars have simultaneously employed institutional, resource-based, social network, and stakeholder theories (e.g., Varsei, Soosay, Fahimnia, & Sarkis, 2014), as well as agency and

stewardship theories (e.g., Turel & Bart, 2014), to explain governance implications. Thus, selected supporting conceptualizations have relevance in determining constructs that help evaluate ISG effectiveness due to delineated organizational lens and phenomenon cognitions (Yaokumah, 2013).

Scholarly researchers have referred to security program management as the ISG focal point (Silic & Back, 2014). ISG studies typically investigate organizational programs from any of four abstractions: strategy and information security policy, governance structure, frameworks and standards, or information security advisory (Silic & Back, 2014). Strategy and information security policy research has focused on determining how organizations implement security design to protect their information systems (Ahmad et al., 2014). Governance structure studies have centered on designed tasks and deployed technology. Information security advisory studies offered suggestions about the best course of action. Frameworks and standards addressed defining and providing insights contextually related to security governance (Silic & Back, 2014). These studies revealed abstractions considered by academia as relevant to realizing effectual ISG.

Literature Review Sources

Researchers applied quantitative, qualitative, and mixed methods to explore, describe, or explain information security related theories and practices (Silic & Back, 2014). I have included commentary from multiple sources, including journal articles, throughout the literature review by comparing viewpoints while focusing on the purpose of the study. Through scholarly bibliographic coupling (Pautasso, 2013), no more than

15% of the cited material was older than 5 years from the anticipated study completion date. Therefore, considering the doctoral study completion date, the presented information was recent, relevant, and credible. Table 1 summarizes the sources used in this literature review.

Table 1

Summary of Research Sources in Literature Review

Reference type	Total	Less than 5 years	Total percentage
Peer-reviewed journal articles	194	170	88
Doctoral dissertations/studies	6	5	83
Contemporary books	4	1	25
Total	204	176	86

Literature Review Organization and Strategy

A researcher gains insight into a selected topic when performing an initial academic literature review several ways (Jaffe & Cowell, 2014). Nonetheless, the academic literature search process is a primary study quality determinant (Jaffe & Cowell, 2014). When writing a literature review, the goal is to reconstruct the relevant accumulated knowledge in a particular subject domain (Schryen, 2013). A literature search represents the first fundamental step in building the accumulated knowledge and principally defines reconstruction in the subsequent literature analysis (Jaffe & Cowell, 2014; Wahl & Bull, 2013). My academic research for this doctoral study focused on articles published in peer-reviewed journals, dissertations, and related doctoral studies as

well as subject-related books. The literature search strategy to obtain the best possible periodical outcome used procedures suggested by Silic and Back (2014).

I applied a systematic literature review approach for online periodical interrogation that consisted of a four-step process: journal, database, keywords, and citation chaining (backward as well as forward) searches. My exploration of academic journals included the leading periodicals in the field of information security dating back to the early 2000s. My exploration of databases encompassed the leading digital libraries providing access to the preeminent journals. As for keyword searches, my queries commenced with the previously identified databases. My backward search entailed reviewing article references generated from the keyword queries and a forward search required examining additional sources that had cited the articles.

My literature review search for corporate ISG within the United States of America encompassed defining various combinations of keywords. Given the topic, selected descriptors in developing keywords included *information systems (IS)*, *information technology (IT),* as well as *information and communication technology (ICT)* acronyms based on commonality of use. Thus, concerning defining keywords, my study search list included *IS security*, *IT security,* and *ICT security*. Additionally, my selected search phrases were *corporate governance*, *information security governance*, *information security*, *cybersecurity governance*, *cybersecurity*, and *information technology governance*.

As shown in Figure 2, I presented separate discussions on corporate governance and ISG theories as well as practices within the doctoral study literature review.

Considering research performed by Yaokumah (2013, 2014) as well as Yaokumah and Brown (2014), my literature review included relevant studies related to the relationship between strategic alignment, value delivery, risk management, performance measurement, resource management, and effectual ISG. Based on Yaokumah's (2013) and Yaokumah and Brown's (2014) research, I also covered stakeholder theories, agency theories, and resource-based theories explaining corporate governance in the literature review. Moreover, subjects I referred to in this literature review included information theories and decision theories linked to ISG.

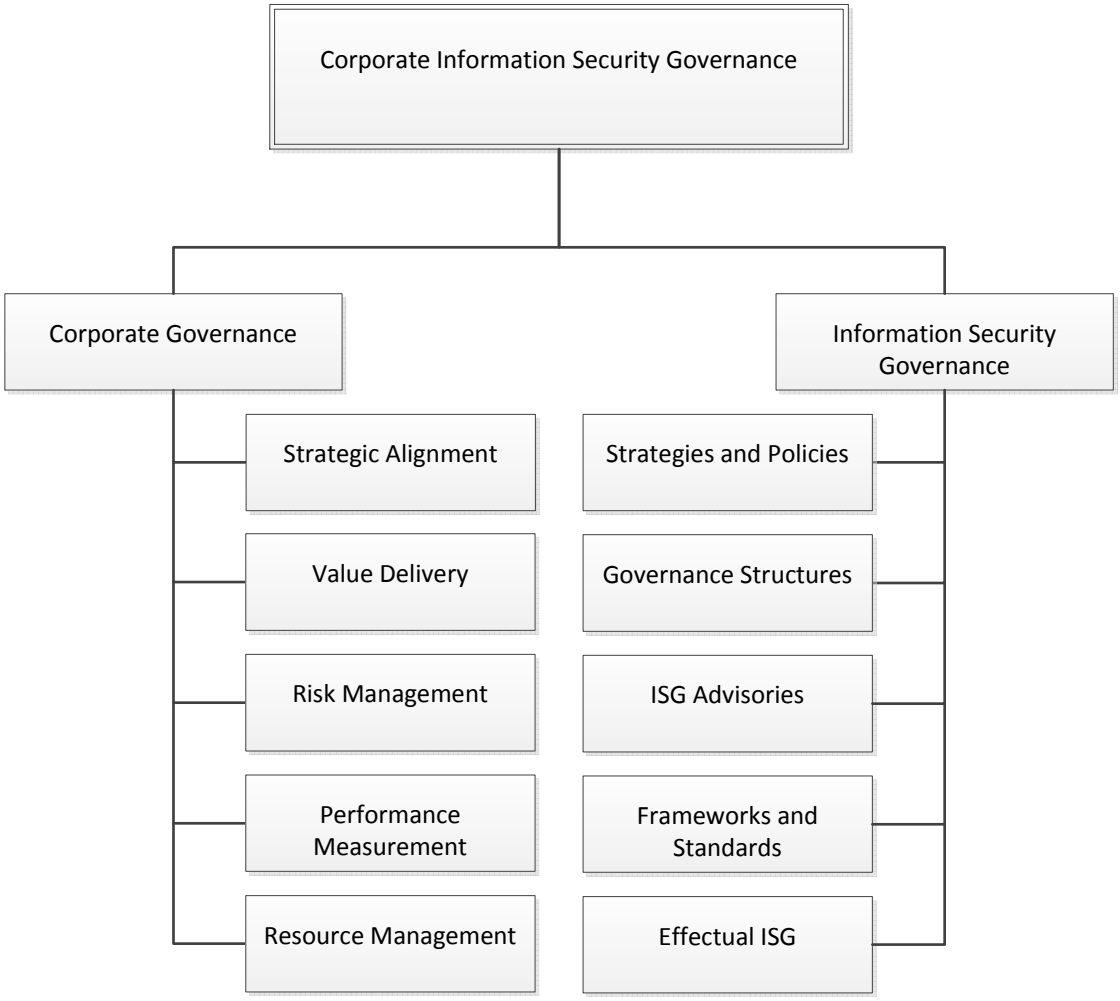

Figure 2. Corporate ISG literature review organization.

Corporate Governance

Corporate governance is a significant factor influencing firm performance (Al-Azzam, Al-Qura'an, & Al-Mohameed, 2015; Alnaser, Shaban, & Al-Zubi, 2014; Tseng, Wu, & Lin, 2013) that consequently leads to firm valuation (Mishra & Mohanty, 2014). Corporate governance also lacks a singularly accepted theoretical foundation (Htay et al., 2013; L'Huillier, 2014; Pande & Ansari, 2014; Sachdeva, 2014). However, most

scholarly researchers supported studies by following prominent theories to explain corporate governance determinants (L'Huillier, 2014; Yaokumah & Brown, 2014).

Corporate governance savants examined governance structures, processes, practices, and effectiveness using various theoretical lenses (Yaokumah & Brown, 2014). These theoretical perspectives include stakeholder theory (e.g., Abraham, 2012; J. Harrison & Wicks, 2013), agency theory (e.g., Heracleous & Lan, 2012; Raelin & Bondy, 2013), and resource-based theory (e.g., Turel & Bart, 2014). Notwithstanding other theories are applicable in deriving constructs for an ISG study, the stakeholder, agency, and resource-based theories have a significant potential influence on achieving effectual ISG practices (Yaokumah & Brown, 2014).

Researchers presented stakeholder theory as recognizing constituencies other than shareholders with legitimate concerns and claims regarding corporations (Heracleous & Lan, 2012). Corporate governance theoretically furnishes internal and external control mechanisms to protect stakeholders (Sachdeva, 2014). Miles (2012) explored whether the lack of stakeholder theory consensus was conceptual confusion, or the stakeholder concept was foundationally contestable. For this, Miles obtained research data through a literature review. Miles uncovered significant evidence to classify the stakeholder concept as both inherently contestable and essentially contested. Correspondingly, the research benefits included demonstrating the stakeholder concept is a complex construct (Miles, 2012).

Modern corporate governance has emphasized financial aspects of increasing shareholder value and an integrated approach that considers the rights and interests of all

stakeholders (Hilb, 2012). Leadership, stewardship, ethics, security, vision, direction, influence, and values are prominent corporate governance components enabling the flow of stakeholder expectations (Flores et al., 2014; R. Davis, 2008). The integrated corporate governance perspective focuses on stakeholder value protection as well as shareholder value creation and enhancement (Heracleous & Lan, 2012; Hilb, 2012). Corporate governance conceptualizations should reflect a dynamic and integrated approach addressing financial, social, environmental, and economic concerns of all stakeholders (Hilb, 2012). For-profit public corporation manager-leaders typically seek to optimize stakeholder satisfaction to ensure continuity (J. Harrison & Wicks, 2013; Tashman & Raelin, 2013). Nonetheless, scholars aligned strategic stakeholder theory with various approaches, considering the theoretical objective and research design (Miles, 2012).

Governance helps satisfy stakeholder expectations concerning managerial responsibilities (R. Davis, 2008). Implicit in expectations for effective governance are the fiduciary relationship between stakeholders and executive management's adherence to stated values (R. Davis, 2008). Stakeholder identification (Gil-Lafuente & Paula, 2013) and value analysis (J. Harrison & Wicks, 2013) help assess enterprise-level strategy and organizational culture alignment. Derivatively, stakeholder and organizational values alignment depend on the firm's ability to pursue the defined mission effectively and efficiently while strictly adhering to espoused organizational values. Alignment exists and is maintainable considering the presented stakeholder values as long as an organization can furnish products and services in a manner supporting acceptable value creation (Chou, 2015; Di Gregorio, 2013) and value appropriation (Di Gregorio, 2013).

Deviation from the values alignment construct could result in stakeholder dissatisfaction generating perceptions that competitors offer a stronger value proposition.

Agency theory can reflect a foundational shareholder primacy premise that owners (principals) establish a relationship with manager-leaders (agents) through responsibilities delegation (Heracleous & Lan, 2012; R. Davis, 2008; Yaokumah & Brown, 2014). A tenet of this theoretical perspective is corporation shareholders are the principals who hire the agents to perform activities (Heracleous & Lan, 2012; Tashman & Raelin, 2013; Yaokumah & Brown, 2014). In other words, the shareholder primacy is a structure with emphasis on shareholder ownership with manager-leaders viewed as stewards of shareholders (Abraham, 2012). From this theoretical perspective, agents are expected to make decisions and act in the best interest of principals (Heracleous & Lan, 2012; R. Davis, 2008; Yaokumah & Brown, 2014). Under agency theory, boards of directors are a means to address agency problems between managers and shareholders (Boshkoska, 2015; Feldman & Montgomery, 2015).

The board of directors can play a vital role as a corporate governance mechanism (L. Guo, Smallman, & Radford, 2013; Misangyi & Acharya, 2014; Sachdeva, 2014). Under the director primacy model, manager-leaders are subject to the expectations and pressures of stakeholder constituents such as employees, suppliers, customers, and government regulators as well as shareholders (Heracleous & Lan, 2012). The director primacy model aligns with stewardship theory and stakeholder theory (Heracleous & Lan, 2012). Thus, manager-leaders assume the responsibilities of an organizational fiduciary with a fiduciary duty (Heracleous & Lan, 2012; L'Huillier, 2014). Stewardship

theory assumes agents are trustworthy, with intrinsic motivation and oriented to serving the collective rather than themselves (Glinkowska & Kaczmarek, 2015; Heracleous & Lan, 2012; Pande & Ansari, 2014). Consequently, manager-leaders must often deal with issues that relate to organizational potency and viability while simultaneously balancing the needs of various stakeholders (Heracleous & Lan, 2012). Accordingly, manager-leaders acquire enhanced utility when they develop a collaborative approach rather than when they behave in a selfish and opportunistic manner (Pande & Ansari, 2014).

Researchers found not all agents adhere to making decisions in the best interest of principals--the principal-agent agency problem (Boshkoska, 2015; Hilt, 2014; Tseng et al., 2013). Perceptions exist that the principal-agent agency problem is a managerial incentive issue arising when ownership is highly diffuse (Boshkoska, 2015; Heracleous & Lan, 2012; Hilt, 2014). Other potential issues associated with corporate governance include the principal-principal agency problem and the power of the state problem (Hilt, 2014). The principal-principal agency problem is the issue of controlling majority shareholders from taking actions benefitting themselves at the expense of minority or outside investors (Hilt, 2014; Mishra & Mohanty, 2014). The power of the state problem arises from controlling the creation of corporations or expropriating existing enterprises (Hilt, 2014; R. Davis, 2008).

Politics has been important in the evolution of corporations in the United States; yet corporate governance evolution was nonlinear (Hilt, 2014). Deficits in the existing corporate governance structures have contributed to the nonlinear corporate governance evolution (Abraham, 2012). Lack of effective and efficient corporate governance can

create a business crisis (Kasum & Etudaiye-Muthar, 2014). The United States has experienced significant episodes of corporate governance crises and governance ineptness (Hilt, 2014). Governance crises have shown that there are serious issues with the principal-agent relationship in particular industry sectors (Kasum & Etudaiye-Muthar, 2014). Numerous corporate governance failures have resulted from ethical commitment lapses by manager-leaders in the form of fraud (Abraham, 2012).

Scholarly research has viewed corporate governance as a solution to agency conflicts between management and shareholders (Kapooria, Sharma, & Kaul, 2014; Pande & Ansari, 2014; Renders & Gaeremynck, 2012; Sachdeva, 2014; Siagian, Siregar, & Rahadian, 2013). C. Chen, Lu, and Sougiannis (2012) revealed robust corporate governance mitigates the positive association between the agency problem and the degree of selling, general, and administrative cost asymmetry. In addressing the issues found in corporate governance, United States legislators have responded by writing codes (Hilt, 2014; Mishra & Mohanty, 2014) affecting the organizational control environment (R. Davis, 2008). The regulatory control environment has an influence on both fraudulent workplace behaviors and counterproductive workplace behaviors (C. Chen et al., 2012). Workplace behavioral standards and values communication typically are broadcast to a corporation's personnel through exemplary actions, policy statements, as well as conduct codes (R. Davis, 2008).

The principal-principal agency problem affects corporate governance quality and effectiveness (Renders & Gaeremynck, 2012). Renders and Gaeremynck (2012) examined the effect of the principal-principal agency problem on the quality and

effectiveness of corporate governance structures. The authors' sampled 1,064 observations in 14 European Union countries listed on the FTSEurofirst 300 index from 1999 to 2003 (Renders & Gaeremynck, 2012). Renders and Gaeremynck found the constructed conflict index affects corporate governance quality and effectiveness. The research benefits included applying a theoretical organizational governance framework to a setting where the primary agency problem arises between majority and minority shareholders (Renders & Gaeremynck, 2012).

Corporate governance reflects managerial power to exercise stewardship of the firm's total resource portfolio with the objective of sustaining and enhancing shareholder value and other stakeholders' satisfaction while considering the corporate mission (Al-Azzam et al., 2015). Corporate business models address optimal resource deployments (Bertels, Koen, & Elsum, 2015). Effectual corporate governance mechanisms ensure preferable resource allocations and management (Mishra & Mohanty, 2014). Scholars have employed resource-based theory to explain governance implications (e.g., Varsei et al., 2014). The resource-based view of the enterprise and the resultant resource-based theory furnish a valuable framework for explaining and predicting a corporation's foundational performance and competitive advantage (Kozlenkova, Samaha, & Palmatier, 2014). Resource-based theory suggests how valuable, rare and unique resources can become for generating an organizational competitive advantage (Cui & Pan, 2015; Varsei et al., 2014; Yaokumah & Brown, 2014).

Under the resource-based theory, resources refer to enterprise-controlled assets, capabilities, competencies, processes and knowledge enabling deployment strategies, and

enhanced competitiveness (Tabares, Alvarez, & Urbano, 2015; Varsei et al., 2014). Yaokumah and Brown (2014) suggested the resource-based view of organizational resource-based theory focuses on the role of the board of directors in furnishing access to resources needed by the enterprise. Whereas, Feldman and Montgomery (2015) advanced the resource-based view focuses on the skills and expertise of directors as resources for the enterprise.

Figure 3 depicts how corporate governance theories influence ISG domains (Yaokumah & Brown, 2014). Contextually, three previously discussed corporate governance theories map indirectly to ISG practice domains (Yaokumah & Brown, 2014). Specifically, the stakeholder theory maps to strategic alignment and value delivery, the agency theory maps to risk management and performance measurement while the resource-based theory maps to resource management (Yaokumah & Brown, 2014). After which, there is a one-to-one mapping correspondence between corporate governance strategic alignment, value delivery, risk management, performance measurement, resource management, and ISG practices.

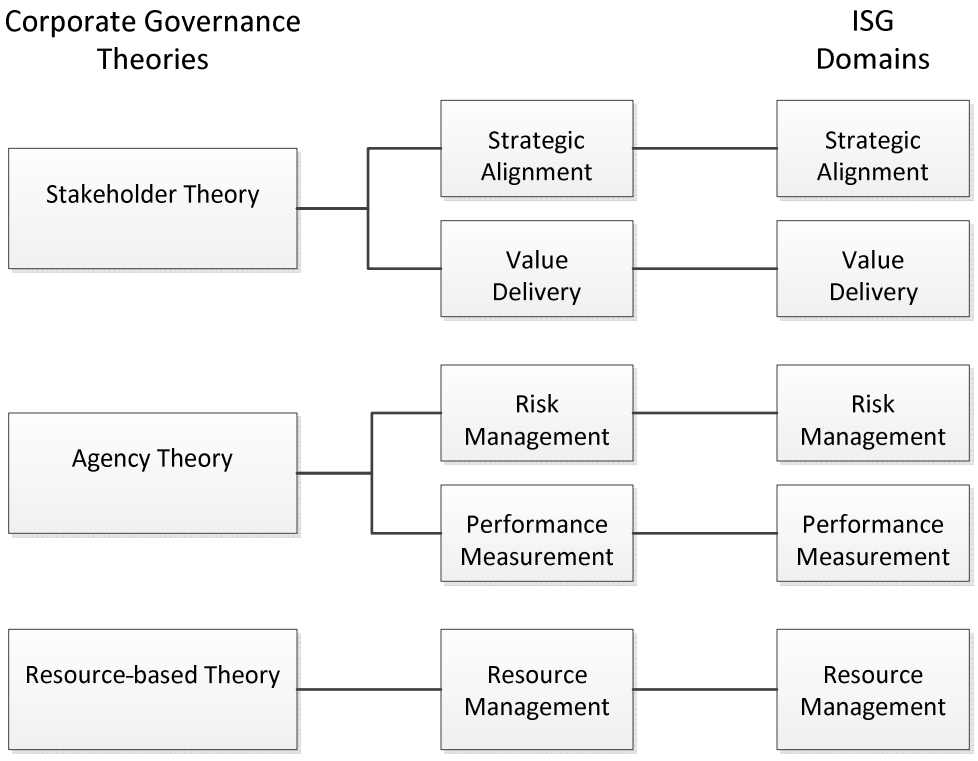

Figure 3. Mapping of corporate governance theories to ISG domains. Adapted from "An Empirical Examination of the Relationship Between Information Security/Business Strategic Alignment and Information Security Governance Domain Areas," by W. Yaokumah and S. Brown, 2014, *Journal of Business Systems, Governance & Ethics, 9*(2), p. 52. Copyright 2014 by Winfred Yaokumah and Steven Brown. Adapted with permission (see Appendix A).

Strategic alignment. A manager-leader's selected tactics misaligned with the adopted corporate focal strategy can prevent performance objective realization (Hardcopf, Goncalves, Linderman, & Bendoly, 2016). As part of corporate governance, ISG is the most suitable path to gain control of security processes and guarantee alignment with business strategies (Rebollo, Mellado, Fernández-Medina, & Mouratidis, 2015). ISG strategic alignment between corporate and information security functions and strategies establishment occurs in an enterprise when strategic management ensures information security strategies are congruent with organizational strategies (Yaokumah &

Brown, 2014). For effective strategic alignment, the corporate strategies should encompass critical information security capabilities, future security requirements, people, and information assets that are deployable to meet business needs (Yaokumah & Brown, 2014). Thus, effective strategic alignment must exhibit flexibility, commitment, and adaptability attributes to meet changing business and security environments to avoid organizational discontinuity (Yaokumah & Brown, 2014).

There are three strategy levels manager-leaders typically consider within an organization related to alignment: corporate, business, and functional (Alsudiri, Al-Karaghouli, & Eldabi, 2013). The relationship between corporate governance, IT governance (ITG), and ISG vary in academic literature (Williams, Hardy, & Holgate, 2013). Figure 4 depicts corporate, IT and information security functional strategic alignment. A corporation's information security and IT functions should align with the organizational vision, mission, values, objectives and strategies for effective practices (Alsudiri et al., 2013; R. Davis, 2011).

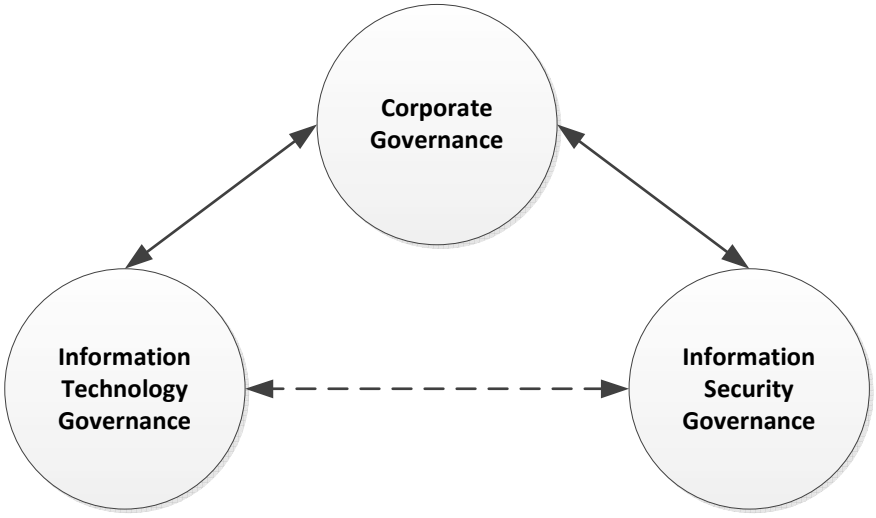

Figure 4. Functional corporate governance, ITG, and ISG strategic alignments. Adapted from *IT Auditing: Assuring Information Assets Protection* (p. 54) by R. E. Davis, 2008, Mission Viejo, CA: Pleier. Copyright 2008 by Robert E. Davis. Adapted with permission (see Appendix A).

Nodal organizational connectivity imposes ISG alignment with enterprise-level governance requirements (R. Davis, 2008; Yaokumah, 2013). Hierarchical node connectivity establishment often transpires when standard attributes sharing occurs in parent-child data relationships (Kearney & Kruger, 2013; R. Davis, 2011). In contrast, vertical node equality defines similar data sharing perceptions (R. Davis, 2011). Corporate executives provide the foundation for creating a legitimate governance structure (Abraham, 2012) that permits sharing relationships. Information security nodal connectivity enables developing and sustaining information systems strategically aligned with the corporation's goals and objectives (R. Davis, 2008). ISG strategic alignment with ITG activities is also necessary for maintaining information security congruency with corporate governance (Fenz, Heurix, Neubauer, & Pechstein, 2014; R. Davis, 2008).

ISG should reflect good corporate governance (Yaokumah & Brown, 2014). By which, information security processes should portray good ISG. Inversely, where consistently applied, ISG can improve corporate governance (R. Davis, 2011). Monitoring and reporting enable information security alignment with business processes and requirements that consequently strengthen the governance bidirectional enterprise information security relationship (Kwon, Ulmer, & Wang, 2013; R. Davis, 2011). Corporate IT leaders ensure strategic alignment when appropriate control deployments occur under an effective ISG program (Mohare & Lanjewar, 2012; R. Davis, 2011).

Previous quantitative ISG survey research furnished the importance of information security risk management, performance measurement, resource management, and value delivery practices as organizational strategic alignment predictor variables (Yaokumah, 2013; Yaokumah & Brown, 2014). Yaokumah (2013) as well as Yaokumah and Brown (2014) surveyed 360 individuals within 112 Ghanaian organizations for evaluating whether the integration of the domains generated ISG success. The Yaokumah and Brown ISG research conferred effectual ISG realization can occur through sound corporate governance theories while the Yaokumah ISG research presented ITG structures, processes, and relational mechanisms applicable to generating effective ISG. The ISG researchers' demonstrated that organizational risk management, resource management, performance measurement, and business value delivery practices positively correlate to effective ISG strategic alignment (Yaokumah, 2013; Yaokumah & Brown, 2014).

Effectual ISG strategic alignment substantially enhances organizational risk management, resource management, performance measurement, and value delivery (Mohare & Lanjewar, 2012; Yaokumah & Brown, 2014). A cross-organizational committee should exist to develop, implement, and monitor the corporate and ISG strategic plans for objectives and goals synchronization (R. Davis, 2011). Once approval of strategic plans occurs, manager-leaders must ensure direction transformation into the right information security service and support deployments (Mohare & Lanjewar, 2012; R. Davis, 2011). Activity alignment orientation and adaptability orientation are complementary in strategy operationalization (Hodgkinson, Ravishankar, & Aitken-Fischer, 2014). Where optimal value to customers is the adopted strategic objective, information security realization can create a service advantage (R. Davis, 2011). Though, achieving the customer value objective through information security realization is not riskless (Hashizume, Rosado, Fernández-Medina, & Fernandez, 2013; R. Davis, 2011; Rebollo et al., 2015).

An ISG researcher qualitatively investigated how organizational information systems personnel perceive the information security strategy issue. Ahmad et al. (2014) primarily collected research data through a literature review and two focus groups (with five participants per group) held in Korea. Ahmad et al. obtained considerable evidence that showed security strategy is driven bottom-up rather than top-down by all study participants representing organizations.

Stakeholder identification and salience theories assist in determining general classes relevant to strategy development (Tashman & Raelin, 2013). However, Ahmad et

al. (2014) suggested there is a lack of knowledge and an ad-hoc approach to security strategy development. As a potential explanation, Mohare and Lanjewar (2012) found no ready organizational strategic roles and responsibilities framework or discussion after conducting a literature review.

When ISG misalignment to corporate governance and ITG occurs; financial, legal, reputational, and operational risks can escalate beyond demarcated tolerance levels (R. Davis, 2008; Yaokumah, 2014). In fact, a functional corporation's very existence might depend on how well IT leaders safeguard information assets used in achieving the adopted organizational mission (Bahl & Wali, 2014; D'Arcy, Herath, & Shoss, 2014; R. Davis, 2008). ISG development and deployment represents how an enterprise's designated information security management team intends to accomplish the organizational safeguarding mission (R. Davis, 2008; Whitman & Mattord, 2012).

Value delivery. The stakeholder perspective promotes a value-laden approach to corporate governance as opposed to other views that are unilateral (Abraham, 2012). Stakeholder value is derived from the relevance and quality of products as well as services (J. Harrison & Wicks, 2013). Ascertaining the degree that manager-leaders should give priority to competing stakeholder claims can occur through organizational- and societal-level stakeholder power, legitimacy, and urgency assessments (Tashman & Raelin, 2013). Given the identification of stakeholders and perceived salience, strategic correlation occurs through satisfying what stakeholders' value and determining valued outcomes. Management practices ensure efficient and effective stakeholder value delivery through good governance (Mishra & Mohanty, 2014). Investors prefer to deal

with corporations that have credible and good governance practices (Mishra & Mohanty, 2014).

Stakeholders and societies assert organizations have a responsibility to support environmental and social sustainability efforts in a manner that is financially responsible (Glavas & Mish, 2015). Managerial conceptual congruence nourished acceptance of the triple bottom line (TBL; Glavas & Mish, 2015). Managers frequently used the TBL approach to describe corporate social responsibility activities (Nalband & Kelabi, 2014). The TBL approach places value on financial returns, human resources, and physical environment considering fair business practices benefiting labor, the community, and the greater common good (Sharma & Khanna, 2014).

Program management can reflect enterprise value creation that extends beyond project portfolio performance (Rijke et al, 2014). Value creation and subsequent value appropriation occur through efficient and effective value management. Creating value for sustainable solutions is a means of increasing the organization's value propositions and remediating unsustainable business practices affecting social and ecological systems. The stakeholder model aligns with sustainable development (Miles, 2012). However, heterogeneity in defining stakeholders has created confusion and inadvertent failures to address stakeholder expectations appropriately and providing optimal value delivery (Gil-Lafuente & Paula, 2013).

Creating optimized value for stakeholders is a responsibility of manager-leaders (Tashman & Raelin, 2013). As commonly stated program success factors, effective value delivery practices must engage all stakeholders and assign accountability for delivery of

expected capabilities as well as benefits realization (R. Davis, 2011; Rijke et al, 2014; Yaokumah & Brown, 2014). ISG value delivery is a strategic alignment function of information security strategies and business objectives (Mohare & Lanjewar, 2012; Yaokumah & Brown, 2014). The general strategic alignment model explains the value generated from alignment within a corporation (Flores et al., 2014). Efficient value delivery defines and monitors key metrics and responds quickly to any changes or deviations as well as provides continuous monitoring, evaluation, and improvement (R. Davis, 2011; Rijke et al, 2014).

Primary information security value occurs if deployed information security assists in meeting stated objectives of information systems (Pérez-Méndez & Machado-Cabezas, 2015; R. Davis, 2011). At the subcategory level, effective information security service can create value (Liang-Chuan & Liang-Hong, 2015) that assists in overall ISG value delivery. For most corporations, information security's value is generated when requested information is delivered within the expected timeframe and budget while satisfying functionality requirements (R. Davis, 2011). Communicating identified data transparently within a timeframe enabling personnel to carry out their duties is considered information security value realization (R. Davis, 2011). However, nonfinancial barometers can determine delivery value--such as information presentation usefulness (Hughes et al., 2013).

Key management practices ensure effectual value delivery (R. Davis, 2011; Yaokumah & Brown, 2014). As with links in a metal chain hoisting precious cargo, manager-leaders must provide appropriate ISG tensile strength for the organizational

environment to achieve corporate objectives (R. Davis, 2011). Considering that acquiring and maintaining ISG resources have costs, IAP must produce benefits from implementation until retirement to justify expenditures (R. Davis, 2011). Unfortunately, without adequate governance, too much tended to be promised by the organization and contracted third party providers; while the IT end-user community assumed too much (R. Davis, 2011). Where the expectation circumstance existed, there was the potential for bilateral misunderstandings, resources mismanagement, poor performance, or outcomes misalignment that invariably reduced ISG value delivery (R. Davis, 2011).

Enterprise-level business models reflect interrelated activity sets enabling value creation, value delivery, and value appropriation (Lambert & Davidson, 2013). Business operations rely on successful supply chain management to assist in satisfying product and service demands (Saber, Bahraami, & Haery, 2014). Cyber security issues need appropriate responses to achieve an acceptable cyber-resilience level for supply chains (Boyes, 2015). Sindhuja (2014) explored the effect of information security initiatives on supply chain performance. Resultantly, Sindhuja indicated information security initiatives positively associated with supply chain operations that, in turn, positively influenced supply chain performance. More recently, Boyes (2015) presented a model for securing information across the supply chain. Using an alternative theoretical lens, Boyes explored supply chain cyber-resilience issues considering the nature of threats and vulnerabilities as well as the attributes of cyber security.

Arguably; IT systems, processes, activities, and tasks represent the key support structure for effective information and communication configurations (R. Davis, 2011;

Sun & Bhattacherjee, 2014). Almost every corporate manager aspires to use technology for integrating information, achieving process efficiencies, and transforming service delivery into an effectiveness paragon (R. Davis, 2011). However, most corporate managers have come to realize that emphasizing technologies and enterprise-centric solutions will not produce the desired results; and a holistic approach is required (De Haes et al., 2013; R. Davis, 2011). Effectual ISG value delivery practices recognize different categories of investments that must be evaluated and managed asymmetrically (Yaokumah & Brown, 2014).

Risk management. Extensive risk exposure can lead to failure in attaining management's established objectives for a corporation (Badara & Saidin, 2014). Risk management integrates a systematic approach to identifying risk and defining the effect on an enterprise's ability to provide goods or services (Mohare & Lanjewar, 2012; R. Davis, 2008). A corporation's business risk management framework should be a strategic axial enabled to accept diverse strategy spokes (R. Davis, 2011; Williams et al., 2013). Business risk management should represent the proactive process by which a corporation methodically addresses risks attached to activities with the objective of achieving sustained benefit within each action and across the organizational portfolio (R. Davis, 2011).

An enterprise's strategic mission as well as risk management system consideration is necessary for achieving proper corporate performance and conformance equilibrium (R. Davis, 2011). Corporations must establish a single control definition that serves all organizational units to empower performance and conformance through

enterprise-centric risk management (R. Davis, 2011). Corporate risk management must also provide standards against which organizational units can assess their control systems and determine what improvements are necessary (Flores et al., 2014; R. Davis, 2011). Cascading from these requirements, enterprises that execute a strong balance between performance and conformance through appropriate value delivery risk management have the best long-term prospects for thriving in their particular regulatory environment (R. Davis, 2011).

Risk management is not a platitude used to demonstrate effective leadership (Boyson, 2014, R. Davis, 2008). Those responsible for governance within an enterprise must provide guidance dedicated to appropriately handling risks their corporation encounters (Boyson, 2014, R. Davis, 2008). In particular, the risks associated with information and related technology necessitates comprehensive management based on a carefully executed impact and likelihood assessment regarding projected adverse event occurrences (Boyson, 2014, R. Davis, 2008). Determining information asset risk magnitudes to ensure appropriate resource allocations addressing threats, opportunities, and vulnerabilities impacting the organization is necessary for realizing effectual ISG (R. Davis, 2008).

Business risk management necessitates information security risk awareness by manager-leaders (Clark & Harrell, 2013; Mohare & Lanjewar, 2012; R. Davis, 2008). Correspondingly, there is a need for a clear understanding of the corporation's appetite for information security risks and information security compliance requirements (Clark & Harrell, 2013; Mohare & Lanjewar, 2012; R. Davis, 2008). There is also a need for

transparency regarding significant organizational information security risks and embedding management responsibilities (Clark & Harrell, 2013; Mohare & Lanjewar, 2012; R. Davis, 2008, 2011). However, Stewart and Lacey (2012) found a lack of formal methodologies in information security awareness for systematically identifying audience communication requirements.

Common information system security controls reduce risk to information systems and enterprises when correctly implemented (Barton, Tejay, Lane, & Terrell, 2016). Deployed managerial business processes and IT risk assessments can assist in determining IAP control intensity (Flores et al., 2014; R. Davis, 2008; Rubino & Vitolla, 2014). Based on the threats, opportunities, and vulnerabilities assessment reports; an enterprise may require IAP remediation to ensure the adequacy of the IT security control system (R. Davis, 2008; Yaokumah & Brown, 2014). Unfortunately, it usually is prohibitively expensive to reduce IAP risks to a tolerable level for all potential IAP failures simultaneously (Nazareth & Choi, 2015; R. Davis, 2008). In addressing this accepted limitation, a risk grading system assists in information asset evaluation and prioritization (Nazareth & Choi, 2015; R. Davis, 2008; Rubino & Vitolla, 2014).

Strategic alignment practices are an organizational risk management predictor (Yaokumah & Brown, 2014). With organizational risk management alignment, ISG can furnish a framework for evaluating investments in information safeguarding, adequate resource coverage, as well as enable objectives achievement (R. Davis, 2008). Information asset managerial due care dictates consistent information security resources administration considering a corporation's ability to deliver business results or value at an

affordable cost--within an acceptable risk level (R. Davis, 2008; Yaokumah & Brown, 2014). Ascertaining an appropriate resource risk level prerequisites organizational risk analyses addressing foreseeable threats, opportunities, and vulnerabilities (Mohare & Lanjewar, 2012; R. Davis, 2008). Contextually, risk management principles and practices are critical drivers for ISG safeguarding activities (R. Davis, 2008).

Responsibility for appropriate safeguarding activities should span the corporation's total tangible and intangible resources (Magdaraog-Jr, 2014; R. Davis, 2008). Risk management should be a continuous effort addressing threats, opportunities, and vulnerabilities (Mohare & Lanjewar, 2012; R. Davis, 2008). Employing software integrity as the research foundation, Boyson (2014) found sampled supply chain initiatives had apparent risk management effort clustering around internally oriented system development and core supplier-oriented sourcing. In contrast, Ahmad et al. (2014) revealed security managers largely ignored business security risks while Magdaraog-Jr (2014) uncovered that most enterprise manager-leaders neglect resource security significance of some information assets.

Scholars concluded a list of significant barriers that perceivably obstruct risk management implementation or impede risk management proficiency in programs (Rasheed et al., 2015). Monetary constraints, schedule requirements, unstable organizational environment, lack of executive commitment towards risk, and a deficit of risk-aware culture are the primary barriers impeding risk management deployment in large-scale Pakistan Telecom programs (Rasheed et al., 2015). Regarding unstable organizational environments, supply chain risk variability and uncertainty make

predicting disruptions challenging (Chopra & Sodhi, 2014; Kumar, Himes, & Kritzer, 2014).

Concerning contextual constraints, researchers also uncovered the considered risk management approaches do not explicitly provide mechanisms to support decision makers in choosing an appropriate risk versus cost trade-off (Deursen, Buchanan, & Duff, 2013; Fenz et al., 2014). However, earlier research by A. Kim, Lee, and Lee (2012) found Hacking, Incident Protection Countermeasures; IT Planning and Operating; and IT Internal Control usable as risk management measures regarding security countermeasures. Information security efforts should reflect coordination through assessed risks, relevant controls development and deployment, and implemented controls effectiveness monitoring (Flores et al., 2014).

Internal and external control systems are governance requirement projections that may have misconceived control elements; because control construction is dependent on the architectural frame of reference (Magdaraog-Jr, 2014; R. Davis, 2008). Internal control systems are also enterprise-centric and may embrace mistaken assumptions regarding required control assurance levels to satisfy stakeholders (R. Davis, 2008). Stemming from managerialism, configured control mechanisms may only minutely affect market inefficiencies and resulting corporate governance issues (Raelin & Bondy, 2013). Thus, employing risk management based controls may do little to enhance stakeholder fiduciary confidence in the corporation's personnel because manager-leaders typically have the ability to override deployed controls (R. Davis, 2008).

Performance measurement. Strategic alignment occurs when proper deployment monitoring ensures success under an adopted vision (R. Davis, 2011). The essence of a monitoring system is feedback information on the results of actions by employees (R. Davis, 2011; Rebollo et al., 2015). Performance feedback information regularly addresses measurement, matching, and regulation of designed processes (R. Davis, 2011, Stewart & Lacey, 2012). The controls can be good or bad; precise or imprecise, and formal or informal (R. Davis, 2011). Nonetheless, control has two key aspects: performance measurement against a standard and performance remediation (if necessary) considering the measure (R. Davis, 2011). A successful control system is one that institutes corrections before process deviations become acute (R. Davis, 2011).

Governance control requires effective performance management (Atoum, Otoom, & Ali, 2014). Controls are the activities increasing certainty that organizational plans are achieving the desired objective (R. Davis, 2011). Controls can facilitate information security implementation efficacy through influencing employee behaviors (Atoum et al., 2014). The dispersed nature of IT limits the effectiveness of many traditional controls (R. Davis, 2011). Nonetheless, a corporation's products and services performance can usually be measured quantitatively or qualitatively (R. Davis, 2011). However, selecting the appropriate measure of the monitored performance activity is crucial for effective performance management (Flores et al., 2014; R. Davis, 2011).

Performance management control techniques include Management by Exception, Management by Objectives, Assurance Reporting, Network Analysis, Balanced Scorecard Analysis (De Haes et al., 2013; R. Davis, 2011), and Budget Analysis (R.

Davis, 2011; Shaaban & Conrad, 2013). Individuals measuring performance may or may not participate in the monitored activity (R. Davis, 2011). Nonetheless, behavioral considerations are important in selecting who performs the measurement (Crossler et al., 2013; Flores et al., 2014; R. Davis, 2011). Furthermore, behavioral factors are important in what is measured, and the standards utilized for comparative analysis (Crossler et al., 2013; Flores et al., 2014; R. Davis, 2011). Measurements should reflect the corporation's strategy as well as provide critical data and information about key processes, systems, and programs (Deursen et al., 2013; R. Davis, 2011). Through analysis of data generated by deployed tracking processes, adopted measures or indicators may be adaptively evaluated and changed to improve managerial goals support (Flores et al., 2014; R. Davis, 2011).

Practice and research necessitate understanding the manager-leaders' strategic organizational intent as an essential prerequisite for deploying an appropriate and efficient monitoring and evaluation system (Yaokumah & Brown, 2014) ensuring effective change management. Utilizing a maturity model can aid management in identifying risk issues (Boyson, 2014). Procedurally, a maturity model provides a standard means to document and evaluate the state of controls (De Haes et al., 2013; Looy, De Backer, Poels, & Snoeck, 2013). Collectively, corporate managers can contribute to identifying risk issues as well as rate controls through a maturity model (De Haes et al., 2013). Some information security manager-leaders suggested that if the system is correctly configured and appropriately monitored by trained individuals, then breach risk minimization will prevail (Lopez, 2012).

Computer technology deployments continue to advance toward a tiered decentralized world of distributed platforms for entering, processing, and retrieving information (R. Davis, 2008). Given the increasing complexity of IT systems and networks, there is a mounting information security challenge for providers and users (Bahl & Wali, 2014; R. Davis, 2008). Where a stringent mandatory security requirement causes a shift to outsourcing, the greater the number of clients a selected managed security service provider has generates a corresponding increase in system interdependency risk (Sen & Borle, 2015). For an organization's outsourced processes, monitoring can detect contractual risk (R. Davis, 2011). For outsourced activities, management should have processes to govern the relationship with and the performance of third party providers (Boyson, 2014; R. Davis, 2011).

Resource management. Business organizations face constant pressure to achieve and maintain a competitive advantage in the marketplace (Cegielski, Bourrie, & Hazen, 2013). The resource-based theory indicates that corporations should center on deployment and combinations of particular inputs rather than avoidance of opportunities (Chou, 2015). Of particular importance is dynamic capabilities viewed as strategic options that give a firm a choice to pursue new directions when opportunities arise (Cegielski et al., 2013). Practitioners, as well as researchers, hold the opinion that a competitive advantage derived from using IT is often temporary (Cegielski et al., 2013). Information systems scholars have also questioned how deployed and used IT can build a competitive advantage (Bharadwaj, El Sawy, Pavlou, & Venkatraman, 2013; Drnevich & Croson, 2013; Seddon, 2014).

Information systems are task configurations that perform data collection, processing, and organization for conveyance to perceived users or storage. Information systems deployments represent the entire organization, infrastructure, elements, and people that collect, process, store, transmit, display, disseminate, and disposition information (Schryen, 2013). The information systems resource-based perspective focuses on understanding what resources are most likely to contribute a competitive advantage (Pan, Pan, & Lim, 2015). Resource Orchestration enables integrating notions of resource management and asset orchestration (Cui & Pan, 2015; N. Wang, Liang, Zhong, Xue, & Xiao, 2012). Resource Orchestration provides a more precise understanding of the manager-leaders' role in structuring a resource portfolio, bundling resources into capabilities and leveraging the capabilities to create value for customers (Cui & Pan, 2015; N. Wang et al., 2012). Researchers have shown that managerial IT oversight enhances value when using a resource-based lens (Turel & Bart, 2014).

The IT architecture refers to technology priorities, and choices allowing applications, software, networks, hardware, and data management integration into a cohesive platform (Masa'deh, 2013). Markus and Loebbecke (2013) argued that the digital business strategies of orchestrators have consequences beyond the boundaries of their ecosystems when ecosystems overlap. Commonly, a disruptive IT produces a response from the industries serving the same market (Carlo, Gaskin, Lyytinen, & Rose, 2014; Catinean & Cândea, 2013; Cui & Pan, 2015). Cross-boundary industry disruptions may, in turn, change value networks to multisided markets (Pagani, 2013). With the increased global competitiveness, development of platforms for IT disruptive advantage

for organizational differentiation and sustainability is a top strategic issue for business leaders (Berman & Marshall, 2014). Disruptive changes in IT platforms have resulted in radical and pervasive innovations in software development organizations across three innovation types: adopted base technologies, produced services, and selected processes (Carlo et al., 2014).

There are four classifications of ISG resources: people, information, processes, and infrastructure (De Haes et al., 2013; R. Davis, 2011). Organizational resources use should occur judiciously and productively to achieve management's business objectives while simultaneously executing control objectives (De Haes et al., 2013; R. Davis, 2011). Control techniques for resource management include relational mechanisms, structures, and processes (Schobel & Denford, 2013). Where applied; the best path to right-sizing ISG controls is provisioning diligent subordinates with justified resources needed to achieve their specific ISG IAP goals (De Haes et al., 2013; R. Davis, 2011). However, regardless of the control techniques and automated capabilities available, the best possible means of control is selecting high-quality employees (R. Davis, 2011).

Hiring and retaining high-quality ISG personnel is critical to sustaining IT departmental effectiveness and efficiency (Cavusoglu, Cavusoglu, Son, & Benbasa, 2013; R. Davis, 2011). Without competent individuals to manage or manipulate IT resources, even a superbly designed architecture can become ineffective and inefficient (Hashizume et al., 2013; R. Davis, 2011) in preventing or deterring an information security breach. Corporate human resource practices can assist in ISG resource quality assurance through legal screening processes applied to assess ISG talent competency and

ethics (K. Guo & Yuan 2012; Price, 2014; R. Davis, 2011). For instance, ethics screening is necessary because cloud administrators typically have unrestricted access to the cloud data (Hashizume et al., 2013). As for deployed personnel, ISG manager-leaders can enhance service quality by ensuring superior education and training (A. Singh, Picot, Kranz, Gupta, & Ojha, 2013; Hashizume et al., 2013; R. Davis, 2011).

Behaviorally, information security responsibility delegation must and should occur (Posey, Roberts, Lowry, & Hightower, 2014; R. Davis, 2008). Deterministically, the appropriate amount of authority must also transfer responsibility (R. Davis, 2008). However, a higher direct reporting position within the corporation cannot evade ultimate accountability for delegated responsibility and authority (R. Davis, 2008). Authority without accountability can promote corrupt practices (Pitesa & Thau, 2013). Employee accountability affects responsibility for meeting standards (R. Davis, 2008). Responsibility for a standard should directly correlate to an activity responsibility because standards become ineffective measurement tools when accountability is lacking (R. Davis, 2008). Therefore; accountability is necessary to ensure appropriately administered authority within the assigned responsibilities context (R. Davis, 2008).

Accountability for decision-making procedures offers a way to contain the self-serving outcomes of power (Pitesa & Thau, 2013). As revealed by researchers, organizational power stems from meanings, resources, process, and systems (Kolkowska & Dhillon, 2013). Power granting to employees can occur through managerial authority, information access, qualifications, competence, seniority, experience, reputation, or respect (R. Davis, 2008). If information reliability is in question so is employee integrity

and corresponding controls (R. Davis, 2008). Making agents accountable for their decision-making procedure is an effective self-serving decision restrictor under moral hazard (Pitesa & Thau, 2013). Ultimate responsibility for conveying expectations rests with the corporation's manager-leaders (R. Davis, 2008). Conclusively, it is imperative that the deployed ISG program ensure ethical employee behavior.

Information Security Governance

Just as corporate governance has been driven by the imperative to manage organizational operations to meet stakeholder expectations for strategic alignment, value delivery, risk management, performance measurement, and resource management, so have ISG scholars focused on achieving similar information security accountabilities (Yaokumah & Brown, 2014). Theories aid in conceptualizing objects and structures that shape activities (Imenda, 2014; Scharff, 2013; Zachariadis, Scott, & Barrett, 2013). Developed theoretical models can be generalizable and can explain cause-and-effect relationships that enable predicting outcomes (K. Davis, 2016). Through metaanalytic research, Silic and Back (2014) identified 164 different theories used in 684 publications addressing information security. Silic and Back depict ISG as frameworks, standards, and policy definitions; where appropriate strategy and security policy require contextual deployment to protect effectually against potential risks.

Information and decision theories have convergence points when conjoined with the binodal processes depicting organizational governance relationships (R. Davis, 2008). Information theory practice domains include data processing systems design, organization analysis, and advertising effectiveness; whereas decision theory practice

areas encompass organization, learning, cybernetics, and suboptimization disciplines (R. Davis, 2008). At the application level, information theory techniques enable classification determination, impact assessments, and technological evaluations (Hughes et al., 2013). Application-level decision theory techniques can provide objectives determination, interaction assessments, performance estimates, and organizational analysis (R. Davis, 2008).

Strategies and policies. ISG research encompasses strategy and policy subthemes (Silic & Back, 2014). ISG planning allows forecasting future organizational direction and relevant influences as well as deriving a better strategy for accomplishing objectives (R. Davis, 2008). An extensive grasp of the corporation's business environment, processes, and organizational objectives enables effective information security strategies development (Flores et al., 2014). Similar to enterprise strategic planning, the ISG planning process translates strategy into measurable tactical and operational plans as well as retranslating operational plans into policies, procedures, directives, standards, and rules (R. Davis, 2008; Edwards, 2013). Ahmad et al. (2014) investigated how organizations implemented security strategies to protect their information systems, and subsequently found a significant proportion of the participating organizations used preventive strategies to maintain the availability of technology services. As a preventive strategy, though policies are necessary means to communicate expected behavior, determining the effectiveness of adopted information security objectives is even more critical.

Typically, safeguarding information assets translates into management ensuring that resource acquisition, use, and disposal occurs (Boyson, 2014) through protection mechanisms and separation-of-duties (R. Davis, 2008). These safeguarding activities must follow policies and procedures as well as approvals because even small asset misappropriations could cause significant losses to organizations (X. Zhao, Xue, & Whinston, 2013). Safa et al. (2015) found a firm's information security policy has a positive effect on subjective norms towards performing the information security conscious care behavior.

The effect of reward on information security policy compliance appears inconclusive. On the one hand; Y. Chen, Ramamurthy, and Wen (2012) showed reward plays an important part in influencing employee compliance intention. On the other hand; Siponen, Mahmood, and Pahnila (2014) found reward does not have a significant influence on employee compliance intention. Depending on a corporation's technological advancement, employer expectations transmission and reception can occur through auditory, visual, as well as sensation activities enabling current or future processing for a decisional application (R. Davis, 2008; Y. Chen, Ramamurthy, & Wen, 2012). The communicated expectations list extends to acceptable business behaviors, financing sources, as well as organizational structures (R. Davis, 2008).

Acceptable business behaviors. Governance policies are particular courses or methods of action selected by management from alternatives to guide as well as determine present and future decisions (R. Davis, 2008). By which, counterproductive work behavior is an ISG policy subcategory. Categorically, counterproductive work

behavior is intentional conduct contrary to legitimate organizational interests (Chernyak-Hai & Tziner, 2014; Claycomb, Huth, Flynn, McIntire, & Lewellen, 2012; H. Zhao, Peng, & Sheard, 2013). Multilevel sanctions are designed and implemented to prevent information security policy violations in the workplace (K. Guo & Yuan, 2012). Regardless, scholarly information security authors have approached counterproductive work behavior inquiry from different perspectives.

On the one hand, K. Guo and Yuan (2012) performed a quantitative study that surveyed 2,793 Canadian organizational computer users to test a proposed mediation model using four scenario-based questions. The scenarios used in the K. Guo and Yuan study reflected security issues related to user authentication and access control, hardware, software, and computer networking. The authors found personal self-sanctions and workgroup sanctions influenced the effect of organizational sanctions regarding employee security policy violation (K. Guo & Yuan, 2012). The researchers' results also revealed both personal self-sanctions and workgroup sanctions had significant negative impact on employee intentions to violate security policies (K. Guo & Yuan, 2012). However, organizational sanctions were nonsignificant when the personal self-sanctions and workgroup sanctions were inclusive (K. Guo & Yuan, 2012).

On the other one hand; Claycomb, Huth, Flynn, McIntire, and Lewellen (2012) presented data extracted from a large database of actual insider activity. The authors obtained 15 actual cases of insider IT sabotage chosen from over 130 previously collected cases of insider activity, covering the crimes of fraud, intellectual property theft, and sabotage (Claycomb et al., 2012). The authors found seven of the insider cases

studied apparently became disgruntled more than 28 days before attacking (Claycomb et al., 2012). However, nine carried out malicious act events less than a day before attacking (Claycomb et al., 2012). The authors also found of 15 attacks, eight ended within a day (Claycomb et al., 2012). Moreover, the authors found 12 detections occurred within a week, and in 10 cases action was taken on the organization insider within a month (Claycomb et al., 2012).

There are social, economic, and technological factors associated with the wrongful use of IT (Chatterjee, Sarker, & Valacich, 2015). Comparatively, K. Guo and Yuan's (2012) derived assertions from a postpositivist perspective, whereas Claycomb et al. (2012) extrapolated assertions from a social constructionist perspective. The studies have well-presented data, yet alternative data views. In studying counterproductive work behavior, K. Guo and Yuan's suggested time is an important consumer behavior determinant while Claycomb et al. considered discounting as a research affect factor. Nonetheless, both datasets are linkable to technical, behavioral, and sociotechnical counterproductive work behavior factors. K. Guo and Yuan communicated the practice implications while Claycomb et al. conveyed the practice and research implications.

Financing sources. A cyber attack commonly denotes illegal activities conducted using the Internet (Julisch, 2013a). Researchers have furnished insights concerning stock market response to a publicly announced cyber attack on a publicly traded firm (Spanos & Angelis, 2016). Das, Mukhopadhyay, and Anand (2012) examined the stock market reactions to publicly declared cyber attacks on listed enterprises. For which, Das et al. obtained data from newspaper and Internet declarations of 101 information security

breaches on firms listed in the United States or India stock exchanges. Resultantly, Das et al. found the firm type, firm size, and attack damage potency was factors that individually affected cumulative abnormal returns. The authors further found Denial of Service attacks on e-commerce generated significantly negative cumulative abnormal returns (Das, Mukhopadhyay, & Anand, 2012). Last, the authors' research revealed information theft attacks on financial institutions produced significantly negative cumulative abnormal returns (Das et al., 2012).

Publicly held company manager-leaders should ensure compliance with all regulatory disclosure requirements and guidance. However, United States Securities and Exchange Commission (USSEC) registrants are prone to ignore or disregard the guidance for additional information security disclosures in their regulatory filings (Stagliano & Sillup, 2014). T. Wang, Kannan, and Ulmer (2013a) investigated how the nature of security risk factors disclosure associated with future breach announcements. Wherefore; T. Wang et al. (2013a) obtained data from financial reports and text-mining media content containing a security breach announcement. Resultantly, the authors showed disclosed security risk factors with action-oriented terms and phrases are less likely to relate to future incidents (T. Wang et al., 2013a). The authors additionally found the market reaction following the security breach announcement is different depending on the nature of the disclosure (T. Wang et al., 2013a). Nonetheless, little had changed concerning cybercrime risks disclosure over the 5 years before the published study by Stagliano and Sillup (2014).

T. Wang, Ulmer, and Kannan (2013b) also investigated the relationship between the textual contents of information security breach reports and the stock price. T. Wang et al. (2013b) examined the trading volume reactions of the affected firm(s) around the breach announcement day. For which, T. Wang et al. (2013b) obtained data from online and offline newspaper article declarations of 89 information security breaches publicly traded companies. Resultantly, the authors found general investors could estimate the price and volume reactions to breach announcements based on the textual contents of the reports (T. Wang et al., 2013b).

Organizational structures. Organizational structures are operational segmentations, managerial layers, and constructed processes that determine how employees accomplish work (Julisch, 2013b). Interior and exterior environmental factors influence organizational structures (Hodgkinson et al., 2014; R. Davis, 2008; Sila, 2013). Traditional organizational structures represent inherited, established, or conventional business architectures (Steiger et al., 2014). Traditional organizations typically utilize the Simple, Bureaucratic, Professional (Functional), or Divisional organizational structures (Steiger et al., 2014). In contrast, where complexity, bureaucracy, and centralization are excessively confining, the Adhocracy (Matrix) organizational structure supports the need to innovate and operate situationally to overcome environmental circumstances (Steiger et al., 2014). Less traditional corporations rely on informal organizational structures through alliance building and boundary spanning management techniques (Foss & Dobrajska, 2015; Steiger et al., 2014).

IT has influenced organizational formation structures (Guadalupe, Li, & Wulf, 2014). A corporation's IT may support a myriad of users and can consist of a multitude of individual elements connected to networks (Garba, Armarego, Murray, & Kenworthy, 2015; R. Davis, 2008). Programs or systems may perform a single task or multiple tasks for a departmental process or the entire corporation in a centralized, decentralized, or hybrid IT environment (R. Davis, 2008; Yaokumah, 2013). Researchers indicated relevant knowledge and activities are the most salient factors for information systems security in organizations (S. Kim, Yang, & Park, 2014). Within this context, knowledge sharing and knowledge application are beneficial to employees (Findikli, Yozgat, & Rofcanin, 2015). However, the effect of organizational structure has a slightly weaker effect on the establishment of security knowledge sharing in organizations (Flores et al., 2014).

Effective knowledge management supporting innovation management has become an organizational necessity (Tseng et al., 2013). IT integration can facilitate knowledge management using advanced IT applications to support interorganizational communication and information processing for acquiring and sustaining a competitive advantage (Liu, Ke, Wei, & Hua, 2013; Masa'deh, 2013). Processes to coordinate implemented security knowledge sharing mechanisms have a significant direct influence on the deployment of security knowledge sharing in organizations (Flores et al., 2014). From a corporate governance lens, Kearney and Kruger (2013) showed how a security incident could create opportunities for organizational learning. Ahmad, Maynard, and

Shank (2015) proposed a new double-loop model for incident learning to address potential systemic corrective actions.

The knowledge barrier prevents efficient communication between information security manager-leaders and business manager-leaders. Information security manager-leaders discerned that there is a knowledge impediment preventing efficient communication between the two identified cohorts (Lopez, 2012). The business manager-leaders internalize the words, yet have no real understanding because of the lack of technical information security knowledge (Lopez, 2012). Flores et al. (2014) found business-based information security management had no significant direct effect on security knowledge sharing. As a remedy to this knowledge sharing challenge, corporate manager-leaders can apply Beer's organizational cybernetics framework to ensure a viable governance structure (Arif, 2016) for efficient communication between information security manager-leaders and business manager-leaders.

Governance structure. Cybernetics control theory emphasizes the role of organizational structure in information governance (Boyson, 2014). Information has been considered a quasiphysical concept related to the degree of organization in a system (Boyson, 2014). From a system perspective, there is a presumption that governance structures are a process outcome (Misangyi & Acharya, 2014). Structures deployed by an organizational governance system allocate rights and responsibilities within the structures, and necessitates assurance that manager-leaders are operating effectively and expectantly within the defined structures (A. Singh et al., 2013; Too & Weaver, 2014). The role of manager-leaders is to administrate within the defined governance system

framework (Too & Weaver, 2014). Thus, ISG reflects the system through which an organization directs and controls information security activities (Kushwaha, 2016; Williams et al., 2013).

Although corporations exist for various reasons, the broadcasting of information security breaches across industries is increasing public and private demands to institutionalize ISG with program oversight (Srivastava & Kumar, 2015). Organizational information and communication have employee responsibility and reporting structures (Mohare & Lanjewar, 2012). Formal organizational structures often reflect constructs associated with laws, regulations, policies, directives, procedures, standards, and rules (Flores et al., 2014; Kearney & Kruger, 2013; R. Davis, 2008). Informal organizational structures mirror the interlocking social makeup governing how people work together in practice (Flores et al., 2014). Guadalupe, Li, and Wulf (2014) suggested executive team structure is a pivotal organizational design choice.

Information security manager-leaders should have the opportunity to learn and discuss practical ITG implementations, effective risk identification strategies, and integration of accepted frameworks to ensure appropriately aligned IT and business processes. Regardless, at the corporate environment detail level, organizational structures are impacted by designed tasks and deployed technology (Guadalupe et al., 2014). Thus, information security is both structural and technical (Boyson, 2014).

IT permits collecting and processing large data volumes as well as inspires innovation (Soava, 2014). IT that links information systems have made intra-organizational communication almost seamless depending on product-specificity

(Guadalupe et al., 2014). Within a corporation's organizational structure, providing acceptable service delivery necessitates the installation of an effective support system (Boyes, 2015; Cegielski et al., 2013). Employed dynamic capabilities enable maintaining competitiveness (Cui & Pan, 2015) through combining, enhancing, protecting, and reconfiguring the corporation's resources and abilities (Pan et al., 2015). Within the deployed IT support system, information security service delivery and support may range from operational protection deployment to crisis response training (R. Davis, 2008). Concurrently, innovations may manifest in different forms that require managerial attention (Cegielski et al., 2013).

Technological innovation adoption can raise security threats (Chou, 2015) and presents challenges to manager-leaders that demand a shift in mindset, culture, or operational procedures (Catinean & Cândea, 2013). As technological innovations extend social impact, correspondingly ethical issues expand for corporate employees (Stahl, Eden, Jirotka, & Coeckelbergh, 2014). In response, a managerial moral assessment concerning what is sound and unsound about new devices (or methods that may emerge; Stahl et al., 2014), and what is appropriate and inappropriate IT options use become imperative (Stahl, Timmermans, & Flick, 2016).

Required information protection changes and maintenance can also occur through various problems encountered by users (Safa, Solms, & Furnell, 2016) or deliberate attacks on the established information security architecture (Safa et al., 2015). Assessing changes in and maintenance of existing systems are critical information security service elements contributing to value delivery (R. Davis, 2008). When assessing IT security

risks, sustained employee, as well as consumer integrity and ethics, define technology safety (R. Davis, 2008). An essential value delivery practice for minimizing projection versus perception risks is service-level management appropriateness (R. Davis, 2011). For example, Ludin and Cheng (2014) surveyed 200 Malaysian young adults for online shopping and found only electronic service quality affected customer satisfaction.

Designing and maintaining appropriate risk management requires comparative assessments of implemented general and application IT controls (Herath & Herath, 2014; R. Davis, 2008). As general and application security categories, significant risks to an organization implementing and using IT are deficient logical access controls (A. Kim, Lee, & Lee, 2012) and weak network infrastructure security (Cowley, Greitzer, & Woods, 2015). Inappropriate environmental controls, misaligned risk responses, and inadequate physical access controls are also significant risks to an organization implementing and using IT (A. Kim et al., 2012). Last, inadequate confidential information lifecycle protection is a major risk to an organization implementing and using IT (Da Veiga & Martins, 2015; Fenz et al., 2014).

Stakeholders are a critical factor in the success or failure of computer software (Babar, Ghazali, Jawawi, & Zaheer, 2015). Bahl and Wali (2014) investigated the effect of ISG on information security service quality delivered to customers. The researchers also examined the perceptions of software services provider employees regarding ISG (Bahl & Wali, 2014). Bahl and Wali assumed that ISG as part of corporate governance drove information security service quality. In this quantitative study, the authors found ISG in an IT outsourcing firm providing software services has a highly significant and

predictable effect on information security service quality (Bahl & Wali, 2014). The authors further concluded there is a positive relationship collectively between ISG and elements of information security service quality (Bahl & Wali, 2014).

ISG frequently includes resilient security regarding the corporate IT infrastructure and information systems supporting critical functions or business processes (Ahmad et al., 2014). An ISG program should manage IT safeguarding (R. Davis, 2008). Information security programs are a significant risk management element that presents the means for preserving information assets (R. Davis, 2008). Programmatically, ISG should control risks as an anticipated deployment advantage. With corporate risk management alignment, ISG can provide a structure for assessing investments in data safeguarding, adequate resource coverage, as well as allow objectives achievement (Nazareth & Choi, 2015). IT risks can affect tangible and intangible assets, including a firm's: image, reputation, financial instruments, consumer confidence, proprietary information, and competitive advantage (R. Davis, 2008; Tabares et al., 2015). Corporations can lower risks to information through effective information systems security (Barlow, Warkentin, Ormond, & Dennis, 2013; Barton et al., 2016).

Logical access controls are the manual and electronic policies, procedures, and organizational structures deployed to safeguard symbolic objects (R. Davis, 2008). Operationally adopted logical controls can ensure that only designated users with approved authorization have access to intangible assets (R. Davis, 2008). Authorization controls provide the ability to verify credentials granted permission to access resources (Baltatzis, Ilioudis, & Pangalos, 2012; R. Davis, 2008). Thus, derivatively, IT

authorization empowers designation and subsequently allowed actions administration for a given information asset (Baltatzis et al., 2012; R. Davis, 2008).

Network infrastructure facilities are the areas where IT hardware and software reside and require access controls (R. Davis, 2008). Consistent with logical access controls, users of the corporation's information processing facilities should receive authentication and authorization through a formal policy and method (R. Davis, 2008). Physical security involves reducing technological vulnerabilities, usually by limiting access to the buildings and rooms housing information assets, or by installing mechanical locks on devices (R. Davis, 2008).

Organizational manager-leaders recognize the criticality of ISG as an integrative program for achieving ITG and corporate governance success (Yaokumah, 2014). Crucial to successful ISG program structures and processes is communication amongst all parties based on constructive relationships, common language utilization and the shared commitment to resolving information security related issues (R. Davis, 2008). Reflective of characteristic organizational requirements; ISG information and communication dissemination usually occurs at different organizational strata (Ahmad, Maynard, & Shank, 2015; R. Davis, 2008; Williams et al., 2013). Resulting procedures are operationally tailored, with processes linking to systems, and systems interfacing with various programs receiving objectives from the firm's oversight committee through established reporting lines (R. Davis, 2008). As a corporate oversight committee subcommittee, Audit Committee members should ensure relevant and quality cyber

security information receipt, and diffusion for devising appropriate IT risk management strategies (Lanz, 2014).

ISG advisories. Research and practice-oriented literature offer considerable information security advice (Ahmad et al., 2014). ISG conformance and performance objectives were found institutionally contingent by scholars (Williams et al., 2013). Consequently, deployed information security programs can be enterprise-centric as well as comprehensive (Edwards, 2013; Mohare & Lanjewar, 2012; R. Davis, 2008). Corporate manager-leaders should enhance strategic alignment attributes to achieve effectual ISG (Yaokumah & Brown, 2014).

IT leaders usually plan, coordinate and recommend organizational information assets deployments (R. Davis, 2008). Correspondingly, responsibility for planning IT protection against unauthorized use and abuse should reside with the corporation's chief information security officer (Mohare & Lanjewar, 2012; R. Davis, 2008). This responsibility may include designing methods for preventing system attacks by external as well as internal hackers and crackers that activate or exploit undesirable security events (R. Davis, 2008). IT security manager-leader duties also typically include establishing departmental policies, procedures, and standards for information assets; based on the organizational structure (R. Davis, 2008).

IT opportunities, as well as threats, need evaluation, organization, and management to reduce potential enterprise risks using available resources (Barrett, 2016; Fenz et al., 2014; R. Davis, 2008). Effectual IAP technologies are valuable defense mechanisms for combating inappropriate and malicious behavior (Claycomb et al., 2012).

Therefore, chief information security officers should assign responsibility for identifying and evaluating deployed configuration management tools to ensure the corporate network infrastructure maintains data integrity and availability (Boyes, 2015).

Stakeholders derive value from organizational justice cognitions, affiliation utility, and opportunity cost perceptions (J. Harrison & Wicks, 2013). Extending agency theory to diverse settings using a deductive approach is achievable through formally recognizing and incorporating the institutional context encompassing the principal-agent relations into agency-based models (Wiseman, Cuevas-Rodríguez, & Gomez-Mejia, 2012). Combined, Stakeholder-Agency Theory explains why manager-leaders might overlook or ignore stakeholder interests (Tashman & Raelin, 2013). As a particular, Stakeholder-Agency Theory scholars have argued that market frictions can cause fragmentary contracting that can misalign managerial abstractions of whom and what is significant to a corporation (Tashman & Raelin, 2013). For instance, top management team may commit financial resources to deploy an enterprise-wide ISG program that will ensure appropriate IAP, yet abstains from using safeguards or other ISG program aspects (Garba et al., 2015; Kushwaha, 2016).

Deeply embedded in employment social and physical context are security issues (Carlson, 2014; R. Davis, 2008). Motives for information systems security counterproductive work behavior can reflect employee organizational justice perceptions (Willison & Warkentin, 2013). For which, organizations should focus on information systems security awareness and moral beliefs (Vance & Siponen, 2012). Security awareness is a process that interacts with the organizational context and with other

security management processes and elements (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2012). Monitoring of policies, user activities, network accesses, and information security protocols can furnish opportunities to enrich training (Price, 2014). Moreover, training improvements may occur through securing an emotional connection or making the content especially pertinent (Price, 2014). Combined, adequate conduct codes and training are beneficial in influencing employee conceptions of appropriate behaviors (Vance & Siponen, 2012).

Organizational information security policies have a positive effect on subjective norms towards information security conscious care behavior performance (Safa et al., 2015). Nonetheless, it would serve corporations well to examine how much of their employees' time is spent on organizational tasks (Posey et al., 2014). High user workloads create a conflict between assigned organizational tasks and information security responsibilities (Posey et al., 2014). Employees who feel overburdened are more likely to have lapses in information security vigilance (Posey et al., 2014).

According to decision theories under uncertainty, people choose an alternative that brings the highest utility or prospect (Lee & Lee, 2012). Choice utility or prospect consists of possible choice consequences, where each consequence has a weighted subjective probability and utility (or value) for the decision maker (Lee & Lee, 2012). As subcategorical decision theories, subjective expected utility theory and prospect theory build on the same basic structure of possible outcomes and probabilities as well as provision similar platforms (Lee & Lee, 2012).

On the other hand, subjective expected utility theory and prospect theory differ from each other in model formulation and assumptions at the detail level (Lee & Lee, 2012). Subjective expected utility theory is a canonical decision theory that suggests a normative decision model based on perfect rationality (Lee & Lee, 2012). The prospect theory is a descriptive attempt to explain seemingly nonrational decisions that diverge from canonical model predictions (Lee & Lee, 2012). Vance and Siponen (2012) found perceived benefits had a substantial influence on employee noncompliance with information system policies. Moreover, Ifinedo (2014) showed how social-organizational and psychological factors might encourage or accentuate employee compliance with information system security policies.

Employee decisions are essential to the achieving ISG goals (R. Davis, 2008). Goal congruence influences the decision quality (R. Davis, 2008). If decision quality is essential and if subordinates do not share the same ISG goals, manager-leaders face losing control over expected activities (R. Davis, 2008) that may have detrimental organizational effects. Hence, employee goal incongruence potentially suboptimizes ISG decision quality (R. Davis, 2008). Therefore, manager-leaders must ensure employees accept and comply with ISG goals (R. Davis, 2008). For which, manager-leaders should acquire an in-depth understanding of the corporation's business environment, processes, and organizational objectives to enable provisioning information security services congruent with organizational needs (Flores et al., 2014). Deep knowledge acquisition by manager-leaders also permits effective coordination of information security activities (Flores et al., 2014).

Manager-leaders should place considerable attention on risk management (Magdaraog-Jr, 2014). Hierarchically, an organization's control environment is an important factor affecting IAP risk management (Mohare & Lanjewar, 2012; R. Davis, 2008). Risk management practitioners are aware of control system limitations in an unethical control environment (R. Davis, 2008). Therefore, after completing the control evaluation process, IAP control risk, as well as inherent risk, should be distinctively delineated from residual risk to assist ethical manager-leaders in understanding quantitative and qualitative control limitations (Nazareth & Choi, 2015; R. Davis, 2008). Additionally, Kwon, Ulmer, and Wang (2013) indicated organizations need to assign proper political influence concerning information security risks.

Stakeholders have placed pressure on corporate manager-leaders to engage in risk management activities in supply chains (Cantor, Blackhurst, Pan, & Crum, 2014). In response, supply chain managers should examine the technologies involved in network configurations to assess vulnerabilities (Boyes, 2015). Organizational managers should also refrain from performing or authorizing knowledge sharing across the supply chain unless they are confident about protection mechanisms (Manzouri, Rahman, Nasimi, & Arshad, 2013). Manzouri, Rahman, Nasimi, and Arshad (2013) presented a model for securing information across the supply chain. Data collection occurred through a literature review, investigating recent IT and conducting focus group interviews with supply chain management and IT professionals (Manzouri et al., 2013). Resultantly, the authors proposed Active Directory Federation Service as the best method to secure information across the supply chain partners (Manzouri et al., 2013).

Internet-based technologies have brought organizational and customer advantages (Safa et al., 2016). With an ever-increasing number of organizations and individuals Internet-reliant for exchanging confidential and sensitive information, appropriate message security is a technological management concern (Chatterjee et al., 2015; R. Davis, 2008; Wlosinski, 2016). Researchers found security was significant for e-commerce system quality (Homsud & Chaveesuk, 2014). Serviceable standard e-commerce models include business-to-business (B2B) and business-to-consumer (B2C) architectures (R. Davis, 2008; Z. Wang, Huang, & Tan, 2013). Delineated, B2B is e-commerce between discernibly distinct organizations (R. Davis, 2008) and reflect open standards (Sila, 2013). B2B links enable the exchange of products, services, or messages between organizations (R. Davis, 2008; Sila, 2013). However, B2B e-commerce is more vulnerable to security breaches when compared to legacy systems (Sila, 2013).

Electronic data interchange (EDI) methodologies are the forerunners and pillars of Internet integrated B2B relationships (R. Davis, 2008). An analysis of business wholesalers suggested that B2B e-commerce still relies on proprietary EDI systems (Sila, 2013). Depending on activity frequency and application, EDI control risk can become material (R. Davis, 2008). Lack of direction, reliance on third parties, and system dependencies potentially expose a corporation to additional legal, security, and operational risks with an EDI system (R. Davis, 2008).

Customer loyalty determines B2C long-term success (Homsud & Chaveesuk, 2014). Regarding B2C models, Lee and Lee (2012) examined the responses of online customers to a publicized information security incident. Lee and Lee developed and

tested a model of retreative behaviors triggered by a publicized information security incident. The authors found an information security incident can cause a measurable negative influence on customer behaviors although the effect seems mainly limited to that particular website (Lee & Lee, 2012). The authors further found perceived damage, and availability of alternative shopping sources can significantly increase retreative behaviors of victimized customers (Lee & Lee, 2012). Last, the authors' research revealed perceived relative usefulness and ease-of-use of the website show limited effects in reducing such behaviors (Lee & Lee, 2012).

Information security addresses safeguarding activities throughout information life cycles as well as asset use within the established protection perimeter (R. Davis, 2008). The primary objective of setting a security perimeter is provisioning an ambit for enterprise-centric policies and protection (Konieczny, Trias, & Taylor, 2015). Management typically designates an IAP perimeter to manage network IT security risks programmatically (Konieczny et al., 2015). For IT-based networking, the main improvements in protection mechanisms were e-mail user identity authentication and e-mail confidentiality as well as privacy transforming (Babrahem, Alharbi, Alshiky, Alqurashi, & Kar, 2015). However, with the advent of linked information enclaves, erecting layered protective barriers preserving IT configurations can introduce a tactical security quagmire (Konieczny et al., 2015; H. Zhao et al., 2013). To reduce network confounding, researchers have suggested employing usability heuristics (Jaferian, Hawkey, Sotirakopoulos, & Velez-Rojas, 2014) and changing the IT architecture model (Konieczny et al., 2015).

Corporate manager-leaders have a cogent incentive to identify and redress any gaps that exist between their firm's current access control and legal obligations. Accessing information assets without permission is a criminally prosecutable offense (R. Davis, 2008; Sen & Borle, 2015) as well as civilly litigable in the United States (Romanosky, Hoffman, & Acquisti, 2014). Nonetheless, a high access control level can decrease security flexibility (Thomson, 2012) and network performance (Hayajneh, Mohd, Itradat, & Quttoum, 2013). To prevent, detect, or correct potential security gaps, corporate IT leaders should voluntarily introduce formal IT related control self-assessment procedures that assure adherence to legal obligations and organizational edicts (R. Davis, 2008).

Executives are leading the drive for bring your own device (Thomson, 2012), and bring your own technology adoption in enterprises to achieve a competitive advantage. Bring your own device and technology (BYODT) to the workplace trend has resulted in security challenges (Olalere, Abdullah, Mahmod, & Abdullah, 2015). Governance is critical to successful BYODT practices (Thomson, 2012). Governance includes furnishing policy controls for BYODT management (Priyadarshi, 2013; Tokuyoshi, 2013). Manager-leaders are typically pursuing BYODT related policies for three reasons: better and more costs savings, intuitive tool knowledge, and productivity gains (Priyadarshi, 2013). However, there are security dangers that should give pause to adopting BYODT work policies (Li & Clark, 2013; Priyadarshi, 2013; Tokuyoshi, 2013). Specifically, resizing and integrating all organizational security requirements into a

personal device to protect work related information may present configuration challenges (Li & Clark, 2013; Meng, Liu, Zhang, Pokluda, & Boutaba, 2015; Tokuyoshi, 2013).

Security performance measurement also becomes challenging in the cloud computing environments (Avram, 2014; Herath & Herath, 2014; Kalloniatis, Mouratidis, & Islam, 2013). A performance evaluation decision model allows organizations to choose whether conducting an IT security audit is worthwhile (Herath & Herath, 2014). If deemed beneficial, a question arises as to what additional factors need consideration when engaging third-party assurance reporting (Herath & Herath, 2014) such as data leakage during and after an audit as well as audit efficacy. Considering confidentiality, C. Wang, Chow, Wang, Ren, and Lou (2013) conducted security and performance analytics using experiment outcomes to demonstrate the proposed schemes furnish verifiable protection and are highly efficient in a cloud computing environment. Resultantly, the authors' authenticator and random masking experiments generated evidence that a third party auditor (TPA) would not obtain any stored data content knowledge on a cloud server (C. Wang, Chow, Wang, Ren, & Lou, 2013). Additionally, regarding efficacy, the experiments produced data that the TPA can perform various auditing tasks in a batch manner for better efficiency (C. Wang et al., 2013).

Scholars suggested storage, virtualization, and networks are the biggest security concerns in Cloud Computing (Hashizume et al., 2013). Complementary to the scholars' assessment, Rai, Sahoo, and Mehfuz (2015) revealed through performing a systematic literature review that a technical challenge when adopting Cloud Computing includes the security architecture. As a potential technological remedy, Pfaff and Ries (2014)

emphasized using standards-based Web Single Sign-on protocols that provision authentication requests with expressiveness and token security versatility. Subsequently, Samanthula, Elmehdwi, Howser, and Madria (2015) suggested homomorphic encryption and proxy re-encryption schemes can prevent the leakage of unauthorized data when a revoked user rejoins the system. Consequently, IT leaders should deploy a comprehensive risk assessment framework for information security to assist in the design of appropriate employee IAP policies, procedures, standards, and rules.

Frameworks and standards. Frameworks can capture skewed model distributions (Pagani, 2013). Frameworks can also serve as a tool for IT leaders to build effective ISG programs (R. Davis, 2008). IT controls immersion should be transparent throughout a corporation's adopted ISG framework (R. Davis, 2008). As a prosecution avoidance mechanism, deploying an exceptional ISG framework addressing every IT resource can significantly reduce legal risks (R. Davis, 2008). ISG studies of standards, as well as frameworks, address defining and providing contextual insights (Silic & Back, 2014).

Frameworks. Several researchers have introduced platform security frameworks. Khalil, Khreishah, and Azeem (2014) proposed a cloud security framework that presented the various defense lines and identified the dependency levels among them. Samanthula et al. (2015) proposed a scheme to achieve fine-grained data sharing and access control over the enterprise's outsourced data in the cloud. Watfa, Khan, and Radmehr (2014) developed and tested a proposed strategy framework for cloud single sign-on solutions considering IT, business, and organizational domains.

Security related situations ensnaring deployed information systems have additionally recast the way corporate employees conduct business with consumers as well as other stakeholders (Srivastava & Kumar, 2015). Sindhuja (2014) developed and tested an integrated information security framework that considers intra-organizational and interorganizational activities as well as processes to strengthen the supply chain. Similarly, Boyson (2014) developed and tested a Cyber Supply Chain Framework that assists in determining risk governance, system integration, and operations initiative coverage.

Properly framed, ISG supports stakeholder expectations regarding management's fiduciary responsibilities (R. Davis, 2008). IT application and user access multiplicity increase the possibility of unauthorized events occurring during authorized IT sessions (R. Davis, 2008). Information security manager-leaders can deploy a variety of techniques to protect organizational information. Protection mechanisms are an essential element to appropriate security (Sen & Borle, 2015). Baltatzis, Ilioudis, and Pangalos (2012) developed and tested a proposed access control framework using a role engineering method for collaborating organizations. Meng, Liu, Zhang, Pokluda, and Boutaba (2015) also developed and tested a proposed collaborative framework that enables node coordination for performing specific actions to enhance system or network security.

Information security manager-leaders do not have the same degree of experience with organizational information security breaches. Some information security manager-leaders have not experienced any information security breach. Other information security

manager-leaders have experienced several information security breaches. Corporate IT leaders should establish an appropriate environment for information security knowledge sharing (Safa & Solms, 2016). Researchers introduced frameworks that permit security-incident managers with different trusted domains to share alarms and countermeasures (Aguirre & Alonso, 2012). Tsohou et al. (2012) introduced a framework that enables security awareness activities and interactions analysis with various organizational processes and events. Similarly, Aguirre and Alonso (2012) developed and tested a framed approach for improving the usability of security information and event managers.

There is a perception that lack of focus and support causes information security breaches. Organizations need a balanced approach to various technical, human and organizational information security management challenges (A. Singh et al., 2013). Primary punishment severity, reward significance, and control certainty effects are all serious managerial actions with information security framework deployment (Kolkowska & Dhillon, 2013; Y. Chen et al., 2012). Atoum et al. (2014) proposed a holistic cyber security implementation framework to implement cyber security strategies. Williams et al. (2013) presented a more multifaceted information protection view incorporating a tiered technical and social features set that form and are established by governance adaptations. Kushwaha (2016) proposed a framework for development and deployment of an information security management system aligned with defined good governance practices.

Organizational culture influences attitudes toward, and implementation of, information security (D'Arcy & Greene, 2014; Edwards, 2013). The discernment of

information security manager-leaders is that organizational cultures are negative because the information security culture is unacceptable as an operational element (Lopez, 2012). Information security manager-leaders recognize that there is a need to improve organizational information security. Information security manager-leaders saw the necessity for improvement regarding how information security affects operations (Lopez, 2012). AlHogail (2015) devised a framework enabling effective information security culture development for protecting organizational information assets.

As a cultural dimension, information security manager-leaders recognize that there are some issues making communication with business manager-leaders difficult (Lopez, 2012). Information security manager-leaders and business manager-leaders have divergent views and goals making communication more demanding. There is a need for information security manager-leaders and business manager-leaders to work together to accomplish information security goals (Lopez, 2012). Davis (2008) constructed a practice framework that abstracted managerial aspects permitting governance information and communication alignment.

Standards. Ratiocinative information security standards must be designed and implemented (Järveläinen, 2012). Evaluating the current information security state requires comparison to accepted standards for performance measurement (R. Davis, 2008). Standards can reflect specific goals or objectives for comparison against performance (R. Davis, 2011). IT leaders need to consider the importance of compliance with standards for achieving effectual ISG (Lopez, 2012; Price, 2014). Effectiveness evaluation requires measurement against established information security standards, yet

audits and standards play different roles in interorganizational IT relationships (Järveläinen, 2012). Performance measurement point selection is critical to an effective standard deployment (R. Davis, 2011). IT leaders should establish standards as baselines for measuring quantity, weight, extent, value, or quality (R. Davis, 2011).

The ISO/IEC 27000 series empower information security managers with a method for classifying and base-lining security, compliant with internationally accepted standards (R. Davis, 2008; Sheikhpour & Modiri, 2012). Contextually, ISO/IEC 27001 provides development and operation normative requirements regarding deployable and deployed information security management systems (Sheikhpour & Modiri, 2012). Clauses structure requirements for management systems that include objectives targeted by information security controls (Sheikhpour & Modiri, 2012). The ISO/IEC 27001: 2015 version focuses on measuring and evaluating the organization's information security management system activities and performance. Therefore, ISO/IEC 27001 reflects a security best practices set that permits benchmarking processes that enable governing a corporation's information security environment.

Effectual ISG. Information is data interpretation presented in a form that furnishes value to a recipient (Da Veiga & Martins, 2015). Global telecommunications services revenue was predicted to grow from $2.1 trillion USD in 2012 to $2.7 trillion USD in 2017 at a combined average growth rate of 5.3% (Atoum et al., 2014). Cyber-attack proliferation threatens the confidentiality, integrity, and availability of IT networks and e-commerce (Chatterjee et al., 2015). Corporate manager-leaders worldwide are devoting significant financial resources to ensure enterprise information security (Flores

et al., 2014). For organizations in the United States, the 2014 average total estimated cost per data breach was $5.9 million (Sen & Borle, 2015). Given cyber attackers targeting large corporations achieved a 93% success rate during 2013 (Brewer, 2014), effectual security solutions are imperative to achieve trust relationships with stakeholders.

Previous quantitative survey research benchmarked interindustry sector ISG implementations and identified areas that might require improvement in developing countries (Yaokumah, 2014). Yaokumah (2014) surveyed 360 individuals within 112 Ghanaian organizations for evaluating the ISG deployment status. The researcher found, as a whole, the surveyed industry classifications have partially implemented ISG. The Yaokumah ISG research revealed all surveyed Ghanaian industry sectors made marginal efforts in aligning information security to business strategy, and performance measurement was the least implemented ITGI ISG focus area. The research results also revealed the ISG implementations differ significantly among the industry classifications surveyed.

Robust corporate information security is a critical exceptional management model factor (Stagliano & Sillup, 2014). Effectual ISG realization can occur through the application of sound corporate governance theories (Yaokumah & Brown, 2014). Effective ISG sustains policies, processes, personnel, and structures implemented by the corporation's oversight committee to inform, direct, manage, and monitor information security activities towards objectives achievement (R. Davis, 2008). Strategic design development typically occurs in sequential order--whether or not manager-leaders have a formal or informal strategic planning system (R. Davis, 2011). Regarding design

operationalization, ITGI ISG practice effectiveness is evident in organizationally framed domain outcomes (Yaokumah, 2014). Corporate IT leaders must evaluate and ensure the quality of implemented protection mechanisms to achieve exceptional ISG performance (Wu, Straub, & Liang, 2015).

Implicit in an aligned definition for effective ISG with corporate governance is information security management's fiduciary relationship with other stakeholders (Yaokumah, 2013). The fiduciary relationship exists because there is typically an inequality in knowledge or training (Brakewood & Poldrack, 2013) between information security management and other stakeholders. Consequently, other stakeholders entrust information security management to act in their best interest. Information security management's strategic alignment operationalization includes connection, congruence, and participation abstractions (Schobel & Denford, 2013). Organizational information asset valuation connection may only represent items that have the required criteria of aiding in achieving a corporate business objective (R. Davis, 2008). However, based on the interdependency theory, an organizational information asset unrelated to objective achievement may compromise corporate business objective realization (R. Davis, 2008; X. Zhao et al., 2013).

After deploying safeguarding mechanisms, critical business and ISG strategy alignments must occur for subsequent improved firm performance (Wu et al., 2015). To obtain an understanding of the processes and to facilitate analysis for ensuring ISG service delivery alignment with the corporation's strategic drive, each phase needs a congruence appraisal to available resources (R. Davis, 2011). Through this assessment,

ISG effectiveness can reflect the proper perspective for achieving defined corporate objectives (R. Davis, 2011). With effective ISG deployment, once ethical manager-leaders have adopted a strategic objective, courses of action by subordinates should reflect attempts to achieve the desired end (R. Davis, 2011) through prevention and promotion mindsets (Neubert, Wu, & Roberts, 2013). Therefore, ISG effectiveness induces doing the right thing.

Employee engagement affects business operations, performance, and the ability to differentiate from competitors (Brajer-Marczak, 2014). When corporate employees develop a reputation for ensuring information confidentiality, integrity, and availability; customers tend to exhibit electronic loyalty (Choi & Nazareth, 2014). Customers aid a corporation in achieving value appropriation sustainability through electronic loyalty (Price, 2014; Safa & Ismail, 2013). Manager-leaders who acquire reliable e-commerce value appropriation can more accurately forecast organizational product and service growth (Price, 2014). Consumer demand induced by enhanced e-commerce security can subsequently benefit society because of the need for additional labor to support organizational growth (Kaganer, Carmel, Hirschheim, & Olsen, 2013; Seferiadis, Cummings, Zweekhorst, & Bunders, 2015).

Exercising effective corporate governance throughout an enterprise requires the top-level oversight committee and management team have an unambiguous understanding regarding what to expect from programs, systems, and processes (R. Davis, 2008). Corporate manager-leaders should continually seek confirmation that information security is delivering reliable services supporting the organization's strategic

design for accomplishing adopted objectives (R. Davis, 2011). Without effectual ISG deployment, often the information security unit is not involved in the decision-making and approval-authorization process (R. Davis, 2011). Correspondingly, problems arise as to who enforces standards, how manager-leaders assure their intentions are carried out and how much autonomy users should have (R. Davis, 2011).

Empirical evidence exists that IT executive's involvement in the top management team relates negatively to the possibility of information security breaches (Kwon et al., 2013). Effectual ISG necessitates information security manager-leader participation in the decision-making process (R. Davis, 2011). Implementation decisions must reflect the proper authority delegation to individuals responsible for acquiring, implementing, utilizing, maintaining, as well as retiring information security systems (R. Davis, 2011). Accordingly, an appropriate corporate control environment enhances ISG effectiveness. Performance monitoring is enabled to ensure strategic alignment is earnestly pursued by employees (R. Davis, 2011).

In viewing agency within an institutional framework; sufficient universality, abstraction, and parsimony acquisition occur to aid in better understanding how, when, and why moral hazard arises (Wiseman et al., 2012). An incentive framework for corporate executives using contributions to IT can leverage the decision-making process (Abraham, 2012). Kwon et al. (2013) investigated how the compensation of IT executives relates to the risk of an information security breach. Kwon et al. found the amount of behavior-based compensation and the pay differences of outcome-based compensation between IT and nonIT executives associate negatively with the likelihood

of information security breaches. Kwon et al. suggested positions in the top management team need an appropriately designed incentive scheme to motivate manager-leaders in line with organizational goals for information security.

Strategic Alignment Variable Measurement

As a data collection tool for this study, the Yaokumah (2013) strategic alignment survey instrument allows participants to record ISG domain implementation perceptions. Yaokumah constructed the research strategic alignment instrument from the Australian Trusted Information Sharing Network literature. Instrument development occurred to measure the alignment level between ISG with business objectives and ISG effectiveness (Yaokumah, 2013). The strategic alignment variable instrument had 13 statements that used a 5-point Likert-like scale that gauged participant responses (Yaokumah, 2013). The 5-point Likert-like scale was as follows: 1 - *not implemented* (NS), 2 - *planning stages* (PS), 3 - *partially implemented* (PI), 4 - *close to completion* (CC), and 5 - *fully implemented* (FI; Yaokumah, 2013).

Similarly, Yaokumah (2014) developed survey items concerning strategic alignment based on an Educause instrument that was slightly modified to include variables defined by ITGI and the control objectives for information and related technology (COBIT) framework. The instrument was designed to compare ISG strategic alignment, risk management, value delivery, resource management, performance measurement implementations among industry sectors (Yaokumah, 2014). The five variables were measured on a 5-point Likert-like scale to gauge the responses of

participants (Yaokumah, 2014). The 5-point Likert-like scale was this: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2014).

In contrast, Yaokumah and Brown (2014) generated survey items concerning strategic alignment based on ISG literature. The instrument was developed to evaluate separately the relationship between ISG strategic alignment with business objectives and ISG risk management, value delivery, resource management, as well as performance measurement (Yaokumah & Brown, 2014). The five variables consisted of 50 items and were measured on a 5-point Likert-like scale to gauge the responses of participants (Yaokumah & Brown, 2014). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah & Brown, 2014).

Value Delivery Variable Measurement

As a data collection tool for this study, the Yaokumah (2013) value delivery survey instrument allows participants to record ISG domain implementation perceptions. Yaokumah derived the research value delivery instrument from the ITGI. The ITGI is an independent nonprofit research organization that guides the global business community regarding information and technology related issues (Yaokumah, 2013). Yaokumah developed the value delivery metric to measure the level that organizational ISG investments deliver business value. The variable instrument consisted of five questions and measurement on a 5-point Likert-like scale that gauged participant responses regarding the degree of value delivery (Yaokumah, 2013). The 5-point Likert-like scale was this: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2013).

Similarly, Yaokumah (2014) developed survey items concerning value delivery based on an Educause instrument that was slightly modified to include variables defined by ITGI and the COBIT framework. The instrument was designed to compare ISG strategic alignment, risk management, value delivery, resource management, performance measurement implementations among industry sectors (Yaokumah, 2014). The five variables were measured on a 5-point Likert-like scale to gauge the responses of participants (Yaokumah, 2014). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2014).

In contrast, Yaokumah and Brown (2014) generated survey items concerning value delivery based on ISG literature. The instrument was developed to evaluate separately the relationship between ISG strategic alignment with business objectives and ISG risk management, value delivery, resource management, as well as performance measurement (Yaokumah & Brown, 2014). The five variables consisted of 50 items and were measured on a 5-point Likert-like scale to gauge the responses of participants (Yaokumah & Brown, 2014). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah & Brown, 2014).

Risk Management Variable Measurement

As a data collection tool for this study, the Yaokumah (2013) risk management survey instrument allows participants to record ISG domain implementation perceptions. Yaokumah adapted the research risk management instruments documented by Educause and the Corporate Governance Task Force. The Corporate Governance Task Force was formed to develop ISG frameworks, promote ISG practices at the strategic management

level, and drive effectual information security program deployments (Yaokumah, 2013). Educause and the Corporate Governance Task Force extracted survey items from the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17799 and the Federal Information Security Management Act (Yaokumah, 2013). The variable instrument consisted of nine questions and measurement on a 5-point Likert-like scale that gauged participant responses regarding risk management (Yaokumah, 2013). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2013).

Similarly, Yaokumah (2014) developed survey items concerning risk management based on an Educause instrument that was slightly modified to include variables defined by ITGI and the COBIT framework. The instrument was designed to compare ISG strategic alignment, risk management, value delivery, resource management, performance measurement implementations among industry sectors (Yaokumah, 2014). The five variables were measured on a 5-point Likert-like scale to gauge the responses of participants (Yaokumah, 2014). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2014).

In contrast, Yaokumah and Brown (2014) adopted survey items concerning risk management from an Educause instrument. The instrument was used to evaluate separately the relationship between ISG strategic alignment with business objectives and ISG risk management, value delivery, resource management, as well as performance measurement (Yaokumah & Brown, 2014). The five variables consisted of 50 items and were measured on a 5-point Likert-like scale to gauge the responses of participants

(Yaokumah & Brown, 2014). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah & Brown, 2014).

Performance Measurement Variable Measurement

As a data collection tool for this study, the Yaokumah (2013) performance measurement survey instrument allows participants to record ISG domain implementation perceptions. Yaokumah adapted the research performance measurement instruments documented by Educause and the Corporate Governance Task Force. The Corporate Governance Task Force was formed to develop ISG frameworks, promote ISG practices at the strategic management level, and drive effectual information security program deployments (Yaokumah, 2013). Educause and the Corporate Governance Task Force extracted survey items from the ISO/IEC 17799 and the Federal Information Security Management Act (Yaokumah, 2013). The variable instrument consisted of four questions and measurement on a 5-point Likert-like scale that gauged participant responses regarding performance management (Yaokumah, 2013). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2013).

Similarly, Yaokumah (2014) developed survey items concerning performance measurement based on an Educause instrument that was slightly modified to include variables defined by ITGI and the COBIT framework. The instrument was designed to compare ISG strategic alignment, risk management, value delivery, resource management, performance measurement implementations among industry sectors (Yaokumah, 2014). The five variables were measured on a 5-point Likert-like scale to

gauge the responses of participants (Yaokumah, 2014). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2014).

In contrast, Yaokumah and Brown (2014) adopted survey items concerning performance measurement from an Educause instrument. The instrument was used to evaluate separately the relationship between ISG strategic alignment with business objectives and ISG risk management, value delivery, resource management, as well as performance measurement (Yaokumah & Brown, 2014). The five variables consisted of 50 items and were measured on a 5-point Likert-like scale to gauge the responses of participants (Yaokumah & Brown, 2014). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah & Brown, 2014).

Resource Management Variable Measurement

As a data collection tool for this study, the Yaokumah (2013) resource management survey instrument allows participants to record ISG domain implementation perceptions. Yaokumah adapted the research resource management instruments documented by Educause and the Corporate Governance Task Force. The Corporate Governance Task Force was formed to develop ISG frameworks, promote ISG practices at the strategic management level, and drive the deployment of effectual information security programs (Yaokumah, 2013). Educause and the Corporate Governance Task Force extracted survey items from the ISO/IEC 17799 and the Federal Information Security Management Act (Yaokumah, 2013). The variable instrument consisted of 19 questions and measurement on a 5-point Likert-like scale that gauged participant

responses regarding resource management (Yaokumah, 2013). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2013).

Similarly, Yaokumah (2014) developed survey items concerning resource management based on an Educause instrument that was slightly modified to include variables defined by ITGI and the COBIT framework. The instrument was designed to compare ISG strategic alignment, risk management, value delivery, resource management, performance measurement implementations among industry sectors (Yaokumah, 2014). The five variables were measured on a 5-point Likert-like scale to gauge the responses of participants (Yaokumah, 2014). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2014).

In contrast, Yaokumah and Brown (2014) adopted survey items concerning resource management from an Educause instrument. The instrument was used to evaluate separately the relationship between ISG strategic alignment with business objectives and ISG risk management, value delivery, resource management, as well as performance measurement (Yaokumah & Brown, 2014). The five variables consisted of 50 items and were measured on a 5-point Likert-like scale to gauge the responses of participants (Yaokumah & Brown, 2014). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah & Brown, 2014).

ISG Effectiveness Variable Measurement

As a data collection tool for this study, the Yaokumah (2013) ISG effectiveness survey instrument allows participants to record ISG domain implementation perceptions. Yaokumah derived the ISG effectiveness instrument from practice literature documented

by Westby and Allen. ISG effectiveness was the criterion variable (Yaokumah, 2013). Instrument development occurred to measure the relationship between ISG risk management, value delivery, resource management, performance measurement implementations, and ISG effectiveness (Yaokumah, 2013). The variable instrument consisted of six statements and measurement on a 5-point Likert-like scale that gauged participant responses regarding ISG effectiveness (Yaokumah, 2013). The ISG effectiveness research survey instrument used a 5-point Likert-like scale that ranged from 1 *strongly disagree* (SD), 2 - *disagree* (D), 3 - *not sure* (NS), 4 - *agree* (A), and 5 - *strongly agree* (SA; Yaokumah, 2013).

Transition

The purpose of this quantitative correlational study was to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. Section 1 of this ISG study contains foundational research information. The section also encompasses a meritorious presentation for conducting the selected doctoral research domain. Topics I covered included the background of the study, the problem and purpose statement, the nature of the study, the research question, hypotheses; theoretical framework; operational definitions, study assumptions, limitations, and delimitations; the significance of the study, and the literature review.

My ISG study addressed a population of the 500 largest for-profit United States headquartered corporations using a corporate governance theory lens. The study sample consisted of 454 strategic and tactical manager-leaders from the 500 largest for-profit

corporations headquartered within the United States geographic boundaries. The results of my study may benefit businesses by assisting manager-leaders with improving ISG practice areas for protecting information assets more effectively, and contribute to social change through increased trust of IT. The study outcomes might add to the literature by contributing to the body of knowledge related to ISG. In Section 2, I cover the purpose statement, the role of the researcher, as well as the strategy used to select participants, collect, validate, organize, and analyze data. In Section 3, I cover the presentation of research outcomes, the business and social implications of the study, recommendation for action, and recommendations for further research.

Section 2: The Project

Purpose Statement

The purpose of this quantitative correlational study was to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. The targeted population consisted of strategic and tactical leaders of the 500 largest for-profit United States headquartered corporations. The predictor variables were strategic alignment, resource management, risk management, value delivery, and performance measurement implementations. ISG effectiveness was the criterion variable. The implications for positive social change include the potential to understand the correlates of ISG effectiveness better, thus increasing the propensity for consumer trust and reducing consumers' costs.

Role of the Researcher

The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (NCPHS, 1979) wrote *The Belmont Report*, which provided ethical practices guidance for research involving human subjects regarding respect for persons, beneficence, and justice. In compliance with *The Belmont Report*, I treated all participants as independent agents and sought to protect participants from any harm related to the research process (NCPHS, 1979). I also attempted to maximize benefits and reduce risks related to the research process, as well as conduct all research with a fair distribution of burdens and benefits (NCPHS, 1979).

As a management audit consultant, senior audit manager, a freelance author, a contracted trainer, as well as a university-level instructor, I reviewed, wrote, and presented ISG subject matter. Specifically, my background encompasses more than 25 years of audit, information security, and accounting practice related to the doctoral study subject matter. My experience also includes 12 years of writing professional practice literature directly or indirectly related to ISG design, deployment, and assurance. Through professional experiences and literary research, I received communications from managers and authors indicating ISG can effectively decrease information security breaches.

Quantitative research typically reflects the postpositivist paradigm (R. Harrison, 2013). In a quantitative correlation study, a researcher examines the relationship between variables (Frels & Onwuegbuzie, 2013). When conducting a quantitative study from a postpositivism perspective, a researcher must remain objective regarding the research with limited human subject involvement (K. Davis, 2016). The role I played in this quantitative ISG study was to recruit participants and compile, organize, analyze, and interpret data to test the hypotheses and answer the research question.

Participants

The population of interest for this study was strategic and tactical leaders employed by the 500 largest for-profit corporations headquartered in the United States. Specifically, the population of interest worked for the largest enterprises that obtained articles of incorporation within United States of America territorial boundaries. Moreover, the population of interest used IT to store, process, or transmit buyer, supplier,

or intrafunctional data (Yaokumah, 2014). The Internet-based survey of the target population commenced after obtaining ethics clearance from the Walden University Institutional Review Board (IRB).

I selected stratified proportional samples from within the strategic- and tactical-level managers who were directly or indirectly responsible for organizational IAP and had at least 1 year of experience with ISG practices. For the purpose of this study, strategic- and tactical-level management were persons working as upper-level or middle-level managers, respectively. Chief executive officers, chief information officers, chief operations officers, chief information security officers, chief audit executives, chief finance officers, and other upper-level as well as middle-level business managers formed the eligible research participant list. The selected participants were comparable to other research of a similar nature, such as Yaokumah (2013).

To enable participant recruitment for the ISG study, I sought e-mail addresses and phone numbers of potential candidates. I did not involve organizational employees in the recruitment process. The information sources for potential participants were publicly available business newsletters, third-party websites, and organizational websites. Subsequently, I randomly selected three participants from each corporation using the compiled list of obtained e-mail addresses. Thereby, all sample frame participants had an equal chance of selection for participation in the study. Last, the selected participants received a personalized e-mail invitation to take part in the study. Similar to the Yaokumah (2013) dissertation sampling procedures, I envisioned this quantitative correlational study would include a stratified random selection of approximately 454

survey participants drawn from 1,500 candidates to collect data on ISG programs and acquire an adequate sample size (see Appendix B).

Research Method and Design

The research question posed by an investigator impels the choice of examination methods (Fetters, Curry, & Creswell, 2013). Based on the research question, I employed a quantitative method with a correlational design using a survey technique to collect data from willing participants. My study intent was to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. In the following research method and design subsections, I explain why a quantitative method and correlational design were more appropriate for my study.

Research Method

Research methodology choice affects the validity and generalizability of an investigated phenomenon (Wahyuni, 2012), for which due care is necessary when selecting the study methodology (Welford et al., 2012; Wester, Borders, Boul, & Horton, 2013). Considering the question and hypotheses, my quantitative research approach aligned with the general theoretical direction available for a postpositivist paradigm. The scientific method lens for postpositivism research is deterministic and reductionist (Christ, 2013; Yilmaz, 2013). I used a quantitative methodology to furnish answers to the effectual ISG question and hypotheses by examining the relationship between governance implementations and ISG practices.

Objectively collecting and disseminating information and data directly aligns with a postpositivist worldview, for which objectivity is essential to achieving competent inquiry (Christ, 2013; K. Davis, 2016; Mayoh & Onwuegbuzie, 2015). Thus, my ISG academic research findings reflected the empirical measurement of objective reality existing in the world where the postpositive epistemology and ontology invoke a quantitative survey as the strategy of inquiry. This scholarly investigation reflected a theory governing corporations that permitted testing as well as verification and refinement to gain usable understandings addressing ISG practices. In other words, this postpositivist ISG research as a scientific method began with a theory. I subsequently collected data to refute or support the governance theory and made any necessary revisions before performing additional hypotheses testing.

The primary distinction between quantitative- and qualitative-based research is the numerical value assignments to data elements (Dellis, Skolarikos, & Papatsoris, 2014; McCusker & Gunaydin, 2015; Yilmaz, 2013). Authors of ISG-related studies previously reported using the quantitative approach (e.g., K. Guo & Yuan, 2012; Hu et al., 2012; Yaokumah, 2013, 2014; Yaokumah & Brown, 2014). The quantitative method was more appropriate than qualitative or mixed methods because the study focus was to analyze numerical data and infer the results to a larger population. The qualitative methodology was inappropriate because the ISG problem analysis addresses numbers and the meaning of these numbers. In qualitative and mixed methods analysis, a researcher considers words to understand the meaning of human actions (Masa'deh et al., 2014; Parylo, 2012; Turner et al., 2013; Welford et al., 2012).

A pragmatic abstraction level to research frames mixed methods studies (R. Harrison, 2013; Siddiqui & Fitzgerald, 2014). The mixed methods approach combines quantitative and qualitative methods in the same research inquiry (R. Harrison, 2013; Ross & Onwuegbuzie, 2014; Siddiqui & Fitzgerald, 2014; Venkatesh, Brown, & Bala, 2013). Mixed methods approach application can help develop insights into various phenomena of interest that could not be fully understood with a singular quantitative or qualitative approach (Mayoh & Onwuegbuzie, 2015; Siddiqui & Fitzgerald, 2014; Venkatesh et al., 2013). Researchers advanced that a mixed methods study requires extensive data collection and analyzing the numerical data within a particular period (Mayoh & Onwuegbuzie, 2015). The mixed methods research strategy has an interdisciplinary view that contributes to the need for study team formations with members having diverse scholarly interests and approaches (McKim, 2015). The mixed method was inappropriate for this study because of the time and investigator diversity typically required to conduct sufficient research.

Research Design

Research design links methodology and a method set to enable deducing logical and valid constructs (Wahyuni, 2012). The appropriate research design is an essential element in conducting a study because this element helps determine research quality (Wahyuni, 2012). With due consideration of possible research approaches, while pursuing a quantitative strategy, I used descriptive and explanatory designs. In other words, for this study, I used a nonexperimental correlational research approach.

Correlational research enables clarifying or discovering the relationships between variables (Turner et al., 2013).

A quantitative inquiry strategy is an experimental design (Turner et al., 2013), where the choices encompass true and quasi designs (Bhattacherjee, 2012; Cokley & Awad, 2013). Considering the control, manipulation, and randomization research tenets (Welford et al., 2012), an experimental approach was inappropriate. Specifically, the phenomenon under study was inappropriate for true experiment and quasiexperiment approaches because I was not collecting data from more than one group, not performing group comparisons among variables, and not seeking a cause-and-effect relationship between variables.

In contrast, qualitative research stresses the socially constructed nature of reality, the connection between the researcher and studied phenomena, as well as the situational constraints that shape inquiry (Welford et al., 2012). There are five primary qualitative research design classifications: narrative, ethnography, grounded theory, phenomenological, and case studies (Parylo, 2012). On the one hand, an exploratory qualitative approach requires the researcher to find the theory in the collected data empirically yet inductively (Trotter, 2012). On the other hand, a confirmatory qualitative approach necessitates applying culture theory to a research topic (Trotter, 2012). The qualitative research design exploratory foundation (Khan, 2014; Parylo, 2012; Welford et al., 2012) as well as using a confirmatory basis (Trotter, 2012) did not align with the ISG research question.

Population and Sampling

Population

The population of interest was strategic and tactical managers employed by the 500 largest enterprises that obtained articles of incorporation within United States of America's territorial boundaries. Based on 2015 governmental agency report filings (e.g., USSEC, 2015), the 500 largest United States-based corporations represented 21 business sectors (see Table 2). The listed 500 companies had $17 trillion in known market value as of March 31, 2015. As reported by the corporations, at the end of 2014, the 500 largest United States corporations accounted for $12.5 trillion in revenues and employed 26.8 million individuals globally. The target population for this study was 1,500 strategic and tactical managers employed by the 500 largest for-profit corporations headquartered in the United States. The target population used IT to store, process, or transmit buyer, supplier, or intrafunctional data (Yaokumah, 2014).

Table 2

United States Business Sector Classifications of the 500 Largest Corporations

Business Code	Business Sector Type	Number of Firms	Number of employees
1	Aerospace & Defense	11	875,576
2	Apparel	5	220,047
3	Business Services	16	640,455
4	Chemicals	14	404,818
5	Energy	69	1,137,078
6	Engineering & Construction	11	284,603
7	Financials	75	3,147,085
8	Food and Drugs	8	1,280,670
9	Food, Beverages, & Tobacco	25	1,081,770
10	Healthcare	39	1,862,429
11	Hotels, Restaurants, & Leisure	12	1,809,594
12	Household Products	14	582,827
13	Industrials	14	794,676
14	Materials	19	391,241
14	Media	11	421,065
16	Motor Vehicles & Parts	14	1,040,700
17	Retailing	46	5,534,684
18	Technology	41	2,814,815
19	Telecommunications	11	773,098
20	Transportation	18	1,228,579
21	Wholesale	27	467,534
Total		500	26,793,344

Note: Number of employees reflects summarization of acquired governmental reports. See Appendix C for United States-based corporation stratification list.

Given the perceived need for centralized control of the information security function in the United States (Flores et al., 2014), the individuals I anticipated would participate in this study played strategic or tactical roles directly or indirectly responsible for organizational IAP and had at least 1 year of experience with ISG practices. Strategic and tactical corporate agents enable large supplier and buyer repositories of sensitive

business and personal information that, if compromised, would have serious organizational and personal repercussions (R. Davis, 2008; Srivastava & Kumar, 2015; Tarafdar et al., 2015). As strategic and tactical corporate agents, upper-level and middle-level business managers comprised the probabilistic stratified random sample.

Sampling

Researcher stratified subject data collection reflects dissecting and regrouping a population into subpopulations then applying appropriate sample selection methods (Bhattacherjee, 2012; Robinson, 2014). Stratified sampling is a probability sampling technique where target population division into mutually exclusive, homogeneous segments occurs first (Bhattacherjee, 2012; Walden University, 2014). In using proportional stratified sampling, participants represented in the sample from each stratum are proportionate to the total number of elements in the respective strata (Bhattacherjee, 2012). Subsequently, a simple random item selection occurs for each stratum (Bhattacherjee, 2012; Walden University, 2014)--where random sampling is item selections from within the target population list using a random selection procedure (Robinson, 2014). I deemed proportional stratified sampling more appropriate than other probabilistic techniques such as systematic sampling because the number of corporate industry sectors varies by business sector within the target research population (see Appendix C).

Probability sampling necessitates the researcher knowing the sampling frame (Acharya, Prakash, Saxena, & Nigam, 2013; Bhattacherjee, 2012; Hitchcock, Onwuegbuzie, & Khoshaim, 2015; Uprichard, 2013). As shown in Appendix C, 21 total

business sector types located within the United States comprised the stratum through my stratification of 66 sampling frame industry types. I drew the sampling units from the sampling frame of 1,500 potential participants (1,500 potential participants = 500 corporations x 3 manager-leaders) obtained through performing Internet searches based on a publicly available list of the 500 largest corporations (i.e. Zyxware Technologies, 2016).

In alignment with proportional stratified sampling technique, I used a proportionate allocation of business sector types to generate a sampling percentage based on the total target population of the 500 largest United States-based corporations. I then applied the generated sampling percentage to the eligible participants in each of the business sector strata proportional to the 500 largest United States-based corporations. Subsequently, I performed a simple random item selection for each business sector stratum representing the 500 largest United States-based corporations under study.

There are advantages and a disadvantage in using proportionally based stratified random sampling technique (Acharya et al., 2013). Advantageously, stratifying a population offers flexibility that might lead to remedies to certain issues confronting a survey designer (Yaokumah, 2013). Moreover, assuming limited missing data, a stratified random sample furnishes a sample more representative of the population under study (Acharya et al., 2013). A stratified random sample also improves the representation of particular strata within the population (Acharya et al., 2013), as well as ensuring a stratum is not overrepresented. Stratified random sampling also allows researchers to make valid statistical conclusions from the collected data (Acharya et al., 2013).

On the other hand, a stratified sampling method's disadvantage is meeting the conditions for proper researcher use (Sekaran, 2003). Specifically, to apply the stratified sampling technique, the researcher must identify every population element under study and categorize each population element into a unique subpopulation (Bhattacherjee, 2012; Walden University, 2014), which can be time-consuming. Thus, the first trial is obtaining an exhaustive and relevant list of an entire population under study (Acharya et al., 2013). The second trial is accurately sorting each population element into mutually exclusive strata (Acharya et al., 2013) which was business sector type.

Empirical evidence generated by researchers revealed the size of corporate executive teams was increasing (Guadalupe et al., 2014). Thus, the risk that there were fewer than three strategic or tactical managers per organization for the 500 largest United States-based corporations appeared unlikely. However, had I encountered a situation where less than three target population members met the eligibility criteria, there would have been a firm employees' omission from the random proportional stratified sample of the sampling frame. Inversely, when more than three target population members met the eligibility criteria a random selection occurred, then the firm and three associated employees were included in the random proportional stratified sample of the sampling frame. Resultantly, I envisioned this quantitative correlational study to include a stratified random selection of 92 survey participants drawn from 1,500 candidates to collect data on ISG programs and acquire an adequate sample size based on the power analysis.

Separate from the chosen enterprise size, other factors to consider when addressing the research question are the participation sample size and the response return

rate (Yaokumah, 2013). A low response rate could indicate nonresponse bias (Barton, 2014). Researchers have revealed a relatively low response rate expectation for ISG studies (Yaokumah, 2013, 2014; Yaokumah & Brown, 2014). A low response rate may occur because of various issues associated with Internet use (Chang & Vowles, 2013). The desire to be comprehensive and the oversurveying of manager-leaders may also generate a low survey response rate (Flores et al., 2014). Flores et al., (2014) indicated researchers should expect a very low response rate when collecting data of a sensitive nature. For example, Yaokumah (2013, 2014) as well as Yaokumah and Brown (2014) ISG studies resulted in 23% return rates.

Sensitive topics evoke concerns over information disclosure that may render a study problematic for both researchers and participants (Barton, 2014; Roster, Albaum, & Smith, 2014). Researchers advised scholars studying topics related to information security refrain from using survey instrument mass mailings to collect data of a sensitive nature (Yaokumah, 2013). The reasoning for the research advisory was that individuals within an organization are typically unwilling to disclose such information when they perceive a lack of data privacy and confidentiality (Yaokumah, 2013). The communications conducted for this Internet-based survey occurred through the participants' private e-mail addresses and an Internet-based survey site. Using the selected communication technique provides robust privacy assurance with the intent to ensure minimal risk of harm to study participants (Yaokumah, 2013).

The strategy for this study relied on both single respondents and multirespondents from each selected corporation, and a combined results analysis to determine industry

level ISG effectiveness. Respondent sample selection for this study proportionally reflected the population industry sector subsets. Thus, having corporate top management team personnel complete the survey instrument was sufficient for addressing the research question because organizational manager-leaders deal directly with enterprise governance (Kwon et al., 2013; Yaokumah & Brown, 2014).

Power analysis. Sample size determination is an essential consideration in scholarly research (Hayat, 2013; Rao, 2012; Zhan, 2013). The most commonly used sample size determination approach relies on hypothesis-based methods of power analysis (Hayat, 2013). Researchers consider the theoretical frame, population size and characteristics, and statistical analysis when performing power analysis (Trotter, 2012). Statistical power is the difference of one minus the probability of incorrect null hypothesis acceptance (1- beta error probability; Rao, 2012; Zhan, 2013). G*Power is a statistical software package that enables a priori sample size determination (Faul, Erdfelder, Buchner, & Lang, 2009). For country-level studies, lacking statistical power is more severe than at the international level (Zhan, 2013). I used G*Power version 3.1.9.2 to determine the appropriate sample size for the study.

A researcher's prior assumptions are intrinsic to sample design (Uprichard, 2013). A priori power analysis by the researcher is necessary to ensure that Type 2 errors do not affect statistical results interpretation (Wester et al., 2013). As shown in Figure 5, for the a priori power analysis, I assumed a medium effect size ($f^2 = 0.15$) and alpha = 0.05 to derive a minimum participant sample size of 92 with a power of 0.80. Increasing the sample size to 138 will increase power to 0.95 (see Figure 5). Therefore, I sought to

achieve between 92 and 138 participant responses for the study using a proportional stratified sample of corporate business sectors.

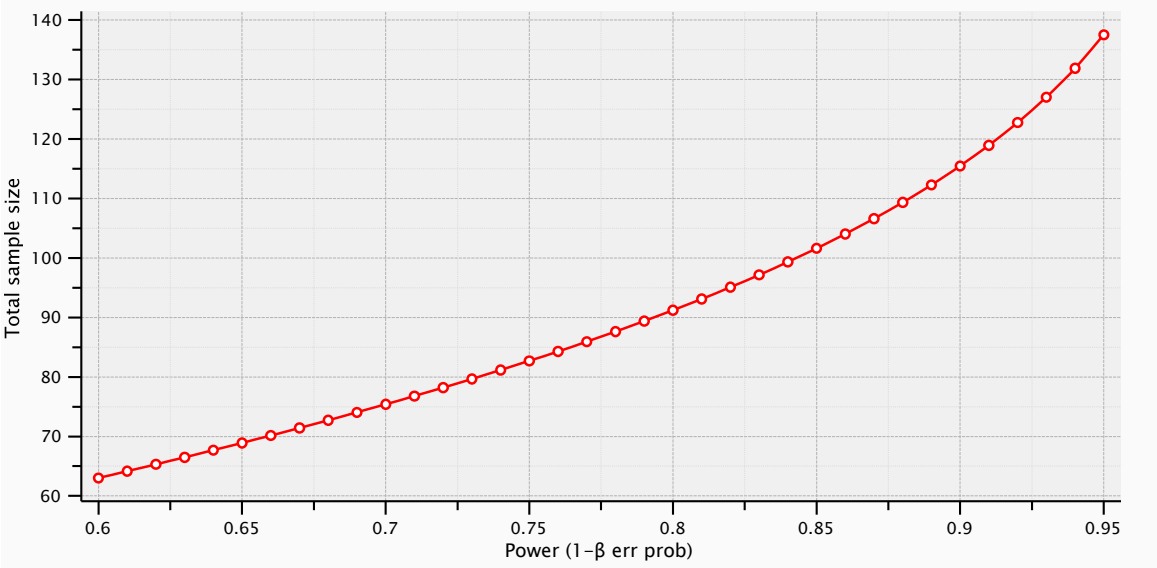

Figure 5. Power as a function of sample size. *F* tests - linear regression: Fixed model, r^2 deviation from zero. Number of predictors = 5, alpha error probability = 0.05, and effect size = 0.15.

Effect size indicators are descriptive statistics that estimate relationship magnitudes (Brooks, Dalal, & Nolan, 2014). The ratio of explained variance and error variance (f^2) serves as the effect size measure for regression analysis (Faul et al., 2009; Wester et al., 2013). The hypothesized medium effect size ($f^2 = 0.15$) reflected the analysis of a Yaokumah (2013) study where effectual ISG was the criterion measurement.

As presented in Table 3, the stratified sample formula I used to calculate the proportion of potential participants from each group in this study was strata sample size = (total sample size / total population size) x strata population size. Strata sample size was the number of sampling units for the group. Total sample size was the entire sampling

unit sample size. Total population size was the entire sampling frame. Strata population size was the sampling frame population for the group.

Table 3

Proportional Stratification of the 500 Largest United States Corporations

Business Sector Type	Number of Firms	Sample Frame	Response Range
Aerospace & Defense	11	33	2 – 3
Apparel	5	15	1 – 1
Business Services	16	48	3 – 4
Chemicals	14	42	3 – 4
Energy	69	207	13 – 19
Engineering & Construction	11	33	2 – 3
Financials	75	225	14 – 21
Food and Drugs	8	24	1 – 2
Food, Beverages, & Tobacco	25	75	5 – 7
Healthcare	39	117	7 – 11
Hotels, Restaurants, & Leisure	12	36	2 – 3
Household Products	14	42	3 – 4
Industrials	14	42	3 – 4
Materials	19	57	3 – 5
Media	11	33	2 – 3
Motor Vehicles & Parts	14	42	3 – 4
Retailing	46	138	8 – 13
Technology	41	123	8 – 11
Telecommunications	11	33	2 – 3
Transportation	18	54	3 – 5
Wholesale	27	81	5 – 7
Total	500	1,500	92[a] – 138[b]

[a]Minimum participant sample size based on power analysis at 0.80. [b]Minimum participant sample size based on power analysis at 0.95.

Ethical Research

As when performing other scholarly investigations, ISG researchers are vulnerable to ethical concerns (Yaokumah, 2013). Researchers have acknowledged

ethical matters deserve consideration when designing an Internet-based survey because of the potential influence on study quality (Chang & Vowles, 2013). These ethical concerns include respect for human subjects, informed consent, privacy issues, respondent anonymity, information confidentially, and data use preventing harm or suffering because of research participation (Yaokumah, 2013). Resultantly, a series of actions occurred to administrate ethical issues appropriately to minimize risks and safeguard research participants.

The informed consent process in this study involved two tasks. First, the potential respondents received an e-mail seeking their participatory consent. The informed consent letter included a statement that there are no foreseeable risks associated with participating in this study and that completing the study might benefit organizational practices and enable social change. The letter also contained information addressing the role of Walden University's IRB and the approval process of the IRB before collecting data. Walden University's approval number for this study is 10-24-16-0465090.

Second, voluntary participation consent occurred before full disclosure of the survey details are made available to enrollees. The purpose of this process was to ensure the respondents give prior approval to receive the survey and record the expressed intention to participate in the study (Yaokumah, 2013). Sustaining well-informed respondents during a research project can assist in avoiding ethical dilemmas (Ward & Pond, 2015).

An ISG researcher might confront concerns regarding privacy, confidentiality, and anonymity of participants (Chang & Vowles, 2013; Yaokumah, 2013). The

solicitation of respondents occurred through electronic mails. Under this circumstance, participant privacy needed adequate protection using appropriate information security (Chang & Vowles, 2013; Yaokumah, 2013). Precautions were taken to ensure participants' data was not made available to individuals external to the study. I also maintained an anonymity standard throughout the study to ensure personally identifiable information that links the participants to the study was not available to external parties. All generated data files were fingerprint protected on the local computer and password protected on the server that hosted the survey instrument.

Participants were logged out of the survey website automatically upon the respondent's successful instrument completion to maintain privacy and confidentiality. I sought an embedded website security feature that causes the survey pages to expire after 5 inactivity minutes. When the page expired, or the session ended, user automatic redirection occurred to the home page. A responding participant had the ability to re-login and complete the survey.

Downloaded data collection files from the survey application will be cryptographically stored on my personal computer for 5 years, commencing upon the publication of my doctoral study. Deletion of the research data collected from participants will occur after the 5-year retention period expires through data erasure software as well as the destruction of the personal computer hard drive containing survey participant data. During the interim, requests for a copy of the raw collected research data require a written personal appeal.

Data Collection Instruments

The survey instruments for this study furnished a system to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations as predictor variables, and ISG effectiveness as the criterion variable. Raw collected data distribution using the Yaokumah (2013) instruments requires a written appeal by the requestor. The Yaokumah (2013) instruments formulated the survey for this study that included a defined scale to measure strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness. The instruments for this study received validation in a Yaokumah (2013) doctoral study. Reapplied data collection instruments replicated validity scores when using different population and sample data (Anderson, 2015).

Instrument Appropriateness

ISG is a program with structural relationships that include systems, processes, activities, and tasks enabling a corporation to achieve enterprise-level objectives (R. Davis, 2008). The ITGI (2008) suggested that effectual ISG practices were evident in their framed domain outcomes. Effectual ISG practices should emanate from effectual ITGI ISG domains that are measurable using the previously validated instrumentation devised by Yaokumah (2013). The Yaokumah positivist instrumentation design best addressed the doctoral study research question and associated constructs. The Yaokumah survey instruments measure an effective information security program relationship with effective deployment of ISG domains. Yaokumah used multiple measures from academic

and practitioner literature to build different ISG survey instrument sections to answer research questions (see Table 4), yet disavowed copyright ownership.

Table 4

Selected Study Instrument Development Descriptions

Study Instrument	Development
Strategic alignment	Yaokumah constructed the research strategic alignment instrument from the Australian Trusted Information Sharing Network literature. The Australian Trusted Information Sharing Network is a government established institution providing national engagement mechanisms for critical infrastructure owners and operators (J. Chen, Chen, Vertinsky, Yumagulova, & Park, 2013). Instrument development occurred to measure the alignment level between ISG with business objectives and ISG effectiveness (Yaokumah, 2013).
Value delivery	Yaokumah derived the research value delivery instrument from the ITGI. The ITGI is an independent nonprofit research organization that guides the global business community regarding information and technology related issues (Yaokumah, 2013). Yaokumah developed the value delivery metric to measure the level that organizational ISG investments deliver business value.
ISG effectiveness	Yaokumah derived the ISG effectiveness instrument from practice literature documented by Westby and Allen. Instrument development occurred to measure the relationship between ISG risk management, value delivery, resource management, performance measurement implementations, and ISG effectiveness (Yaokumah, 2013).
General information, Risk management, Performance measurement, and Resource management	Yaokumah adapted the General Information, Risk Management, Performance Measurement, and Resource Management instruments documented by Educause and the Corporate Governance Task Force. The Corporate Governance Task Force was organized to develop ISG frameworks, promote ISG practices at the strategic management level, and drive the deployment of effectual information security programs (Yaokumah, 2013). Educause was formed to advance higher education through IT use (Yaokumah, 2013). Educause and the Corporate Governance Task Force extracted survey items from the ISO/IEC 17799 and the Federal Information Security Management Act (Yaokumah, 2013).

Instrument for ISG Study

Published psychometric information was not available for the original instruments from which Yaokumah (2013) derived the study measures. Given the lack of published psychometric information, reliability and validity of the measurement instruments used to collect participant data were pivotal academic concerns, particularly when the researcher sought to test relationships among constructs (Yaokumah, 2013). Consequently, the researcher conducted field and pilot tests to establish instrument validity and reliability (Yaokumah, 2013). Upon instrument acceptance, Yaokumah (2013) assessed ISG implementations among major Ghanaian industry classifications with the intent of identifying the focus areas that required improvement. Yaokumah surveyed 360 individuals within 112 Ghanaian organizations for evaluating the status of ISG deployments. Subsequently, ProQuest published the combined study instruments with participant responses during 2013. Table 5 shows the survey items and measurement scales used by the Yaokumah (2013) instrument.

Table 5

Survey Scales for the ISG Research Items and Measurement

Survey section	Survey item	Measurement scale
General information	1.1 – 1.3	Nominal and interval
Effectual ISG	2.1 – 2.6	Interval
Strategic alignment	3.1 – 3.13	Interval
Value delivery	4.1 – 4.5	Interval
Risk management	5.1 – 5.9	Interval
Performance measurement	6.1 – 6.4	Interval
Resource management	7.1 – 7.19	Interval

Nominal and interval data was the classification for the general information scale survey items (Yaokumah, 2013). The scale was X - *response*. The scale reflects industry sector, job title, and the number of years of experience (Yaokumah, 2013). Industry sector was the participant's perceived business sector type from a nominal business sector list (Yaokumah, 2013) with 21 options. The job title was the participant's employment category from a nominal work classification list (Yaokumah, 2013) with seven options. The number of years of experience was the participant's stated work familiarity interval in 5-year increments starting at 1 (Yaokumah, 2013).

Interval data was the classification for all the effectual ISG scale survey items (Yaokumah, 2013). The 5-point Likert-like scale was as follows: 1 - SD, 2 - D, 3 - NS, 4 - A, and 5 - SA (Yaokumah, 2013). SD was a level at which the respondent strongly disagrees with the parameters mentioned in the item without any cognitive reservation. D

was a level at which the respondent does not agree with the parameters described in the item, yet there was a cognitive reservation element. NS was a level at which the respondent takes a neutral stand between agreement and disagreement with the parameters mentioned in the item. A was a level at which the respondent agrees with the parameters referred to in the item, yet there was a cognitive reservation element. SA was a level at which the respondent strongly agrees with the parameters described in the item without any cognitive reservation.

Interval data was the classification for all the strategic alignment, resource management, risk management, value delivery, and performance measurement implementation scale survey items (Yaokumah, 2013). The 5-point Likert-like scale was as follows: 1 - NS, 2 - PS, 3 - PI, 4 - CC, and 5 - FI (Yaokumah, 2013). NS was the level at which the respondent perceived no deployment of the mentioned parameters. PS was the level at which the respondent perceived the parameters mentioned were in the planning stage and not deployed. PI was the level at which the respondent perceived the partial deployment of the specified parameters. CC was the level at which the respondent perceived the parameters mentioned were close to complete implementation. FI was the level at which the respondent perceived the full deployment of the specified parameters.

Validity and reliability. Researchers consider field test and pilot test appropriate for ensuring study validity and reliability (K. Guo & Yuan, 2012; Yaokumah, 2013, 2014; Yaokumah & Brown, 2014). The Yaokumah (2013) field test and pilot test provided information for determining instrument validity and reliability. The field test and pilot test aided Yaokumah in improving participant survey items. The field test and

pilot test also enhanced participant instructional understanding (Yaokumah, 2013). Moreover, the field test assisted the researcher in determining whether the instrument measured the criterion construct and whether the researcher collected scores related to external standards (Yaokumah, 2013). In reducing bias, reliability and validity are significant issues for researchers (Christ, 2013).

Validity. Validity is a significant issue in reducing error sources. From a theoretical positivist perspective, the Yaokumah (2013) research focused on achieving validity. Validity referred to the amount of systematic or inherent errors in measurement (Yaokumah, 2013). Validity establishment in the Yaokumah (2013) dissertation occurred by conducting a field test using a panel of experts. Yaokumah e-mailed draft survey instruments with the research purpose to five panelists: two security practitioners and three senior academic faculty members who had significant experience with ISG issues.

The selected experts assessed the instrument on content validity, construct validity, criterion validity, and face validity (Yaokumah, 2013). The researcher charged the panel with addressing whether the survey items adequately measure ISG effectiveness, represented subject matter content, and appropriateness for the population as well as selected sample (Yaokumah, 2013). The panel was required to assess instrumentation comprehensiveness for collecting all the needed information addressing the researcher's purpose and goals, understandability, and respondent ability to complete the survey items (Yaokumah, 2013).

Yaokumah (2013) assessed instrumentation intercorrelation for two construct variables defined as outcome realizations from effective ISG domain practices: value

delivery and risk management. Moreover, Yaokumah assessed instrumentation intercorrelation of strategic alignment and four construct variables defined as domain practices. As shown in Table 6, Yaokumah's resulting intercorrelation coefficients of the measured variables were above 0.80 and considered acceptable by the expert panel.

Table 6

Yaokumah Reported Variable Intercorrelations

Variable	1	2	3	4	5
1. Strategic alignment		.847	.915	.849	.864
2. Value delivery					
3. Risk management					
4. Performance measurement		.864	.890		
5. Resource management		.859	.922		

Expert panel feedback resulted in revisions to the survey instruments (Yaokumah, 2013). The expert panel suggested, and Yaokumah (2013) implemented a reduction from twelve to six items and re-wording the ISG effectiveness (criterion variable) instrument subsection (Yaokumah, 2013). The reduction was a result of similarities and repetitions identified among the items (Yaokumah, 2013). Amendments also occurred on the demographic data resulting in modifying Banking Institutions to Financial Institutions, Other Options to Other, and Public Utility Company to Public Utility Company (Water, Electricity, Telecommunications; Yaokumah, 2013). The researcher expanded Business Manager to Business Manager / IT Strategic Committee Member and revised the IT

Specialist category (Yaokumah, 2013). The scale on ISG effectiveness constructs was re-worded and changed from Neutral to Not Sure (Yaokumah, 2013).

Reliability testing. Pilot testing occurred to establish the reliability of the Yaokumah (2013) measurement instruments. The pilot test sought to determine whether the instruments consistently measured the intended measurement items (Yaokumah, 2013). For the pilot testing, the researcher sent an instrumentation Internet link to 20 participants selected from the sample frame (Yaokumah, 2013). The investigator's pilot testing intent was to appraise the adequacy of Internet-based survey items under simulation conditions to ascertain the completion time and whether the technology-based instrumentation worked correctly (Yaokumah, 2013). As shown in Table 7, the resulting reliability coefficients of the measured variables were above 0.70 and considered acceptable by the researcher (Yaokumah, 2013).

Table 7

Yaokumah Instrument Construct Variable Reliabilities

Construct	Cronbach's alpha
Strategic alignment	.972
Value delivery	.920
Risk management	.951
Performance measurement	.979
Resource management	.975
ISG effectiveness	.870

General information. General information collection for the ISG study occurred using three replicated items from the Yaokumah (2013) instrument pertinent to respondent demographics (see Appendix D). The items were industry sector, job title, and the number of years of experience (Yaokumah, 2013). The measurement scales for industry type, and job title was nominal, and the number of years of experience was interval, with all items having a single response option (Yaokumah, 2013). The industry type item assisted in assessing the number of years of experience (Yaokumah, 2013). These demographic variables measurement occurred by summing participant responses for each survey item within the instrument subsection (Yaokumah, 2013).

Effectual ISG. I measured effectual ISG using six replicated items from the Yaokumah (2013) instrument (see Appendix D). The measurement scale for ISG effectiveness was interval with multiple response options (Yaokumah, 2013). Item one measured the deployment level of the governing board's agenda engagement. Item two measured the level deployed security actions reflect a comprehensive risk assessment and established risk tolerances. Item three measured the deployment level of a cross-organizational security management team. Item four measured the deployment level of digital assets inventory and categorization performance. Item five measured the deployment level of active security policy monitoring and enforcement as well as manager-leader accountability. Item six measured the deployment level of security program review, audit, and continuous improvement processes.

Strategic alignment. I measured strategic alignment using 13 replicated items from the Yaokumah (2013) instrument (see Appendix D). The measurement scale for

strategic alignment was interval with multiple response options (Yaokumah, 2013). The Yaokumah instrument focused on the organization's input from stakeholders, enterprise mission support, achievement, training and awareness programs, investment allocation, as well as intellectual property accounting and protection. Participants also responded to organizational security planning (two items), enterprise information security responsibility, project development, policies and standards, administrative support, and security compliance items.

Value delivery. I measured value delivery using five replicated items from the Yaokumah (2013) instrument (see Appendix D). The measurement scale for value delivery was interval with multiple response options (Yaokumah, 2013). Participants graded the implementation of policy analysis, risk analyses and risk assessments, third party contracts, corporate policies compliance, and business decision consideration.

Risk management. I measured risk management using nine replicated items from the Yaokumah (2013) instrument (see Appendix D). The measurement scale for risk management was interval with multiple response options (Yaokumah, 2013). Participants rated the implementation of information security and privacy program documentation, risk assessment frequency, critical assets, vulnerabilities, and threats identification; as well as loss cost allocation. Participants additionally assessed the implementation of disruptive business strategies (two items), strategy review and update frequency, and state legislation or regulation monitoring as well as applicability determination.

Performance measurement. I measured performance using four replicated items from the Yaokumah (2013) instrument (see Appendix D). The measurement scale for

performance measurement was interval with multiple response options (Yaokumah, 2013). Participants gauged the implementation of periodic information security program testing and evaluation, periodic independent audits, and business unit compliance audits.

Resource management. I measured resource management using 19 replicated items from the Yaokumah (2013) instrument (see Appendix D). The measurement scale for resource management was interval with multiple response options (Yaokumah, 2013). Participants assessed the deployment level of information security responsibilities (four items), qualifications and experience requirements, authority and resources, information security staff training; as well as engagement with other critical functions. The participants evaluated the deployment level of reporting lines, accountability, compliance programs, stakeholder education and awareness program, and information security architecture (three items). Participants also appraised the deployment of preimplementation system evaluations, noncompliance change management, information asset categorization, and configuration setting documentation.

Instrument Administration

ISG instrument administration requires performing four administrative activities. First, the researcher seeks approval from the doctoral study review committee and IRB to use the study instrument. Second, the researcher prenotifies participants and seeks consent. Third, the researcher sends a Web link to participants (Yaokumah, 2013). Fourth, the researcher re-contacts participants with an appeal to complete the survey.

Upon receiving doctoral study review committee and IRB approval, I sent a prenotification e-mail message to all selected participants--informing selection to take

part in the study and seeking their willingness to participate. Participants who did not want contact e-mail address use for additional correspondence had the option to forward an alternative e-mail address to my Walden University inbox. After a week, I sent the web link to the actual survey site to the participants' e-mail application inbox. Participants had 2 weeks to complete the requested survey responses before I sent first and second reminder e-mails.

For the informed consent, two options were available; one to accept and the other to decline research participation. When the participants clicked the web link contained in the forwarded e-mail, acknowledgment of informed consent occurred. Participants who agreed to respond to the survey items received a unique access code embedded in the web link when they clicked on the application. When the participants clicked the web link contained in the forwarded e-mail, they connected to the website hosting the ISG research survey items. The survey website presented the survey questions in a random order.

Respondents were able to complete the research survey item on each web page. If a respondent decided to skip a survey question or item, the computer application allowed the respondent to proceed to the next survey page. Once the participant completed the ISG survey, the application displayed a message thanking the respondent and automatically logged out the respondent.

Given a low response rate, I extended the data collection period. As a follow-up procedure, two researcher reminder notifications were sent to all selected participants with a personalized appeal and thank you note to those who already completed the survey based on the prior participation request. If I achieved the minimum sample power after

the third week, website blockage was planned, and the participants would be unable to access the survey documents. Subsequently, I downloaded the collected participant responses to my personal computer.

Data Collection Technique

A positivistic survey is point-in-time data snapshots that allow the researcher to make relationship inferences using quantitative analytical techniques (Silic & Back, 2014). Internet-based survey use enables study participants to complete an online data request through computer network access (Chang & Vowles, 2013; King, O'Rourke, & DeLongis, 2014). Adoption of this data collection strategy assumes the target participants will comprise very active and knowledgeable top management team members (Yaokumah, 2013). Respondent data collection enables a researcher to acquire an understanding of the perceived recent state of corporate ISG realization and provide answers to the ISG research question. Supporting the selected research technique, previous ISG related studies reported using Internet-based survey data collection methods (e.g., K. Guo & Yuan, 2012; Hu et al., 2012; Yaokumah, 2014; Yaokumah & Brown, 2014). However, Internet-based surveys have unique advantages and disadvantages related to technology characteristics (Chang & Vowles, 2013; Weigold, Weigold, & Russell, 2013).

Data Collection Technique Advantages

Cross-national research can be less complicated when employing the Internet and social media (King et al., 2014). King et al. (2014) contended that in combination, using their suggested online data collection strategies can furnish advantages to social scientists

when conducting survey research. For this ISG national study, using an Internet-based survey technique provided time efficiency and flexibility, interactivity without interviewer bias, unrestricted geographic coverage, sensitive subject matter desensitizing, and careless response identification.

Time efficiency and flexibility. Internet-based surveys can occur quickly and efficiently assuming sufficient server capacity, acceptable network traffic, as well as continuous connectivity (Chang & Vowles, 2013). Researchers revealed online survey response returns can occur within two days (Chang & Vowles, 2013). Researchers have also indicated the Internet provides more flexibility with how survey response presentation occurs (Weigold et al., 2013). On the other hand, respondents can complete an Internet-based survey at nonimmediate pace and at a convenient time (Chang & Vowles, 2013).

Interactivity without interviewer bias. When performing a quantitative study, Internet-based survey application ease of use can limit dialogue between researchers and participants (King et al., 2014). Specifically, Internet-based surveys enable greater variation in item design without additional researcher involvement (Chang & Vowles, 2013) through application configuration. A well-designed study website conveys professionalism and credibility that can further facilitate data collection (King et al., 2014). Thus, Internet-based survey item design typically offers researchers the option to eliminate or reduce respondent error sources (Roster et al., 2014; Ward & Pond, 2015).

Unrestricted geographic coverage. IT networks enable research respondents to contact participants in any corner of the world as long as there is Internet accessibility

(Chang & Vowles, 2013; King et al., 2014; Weigold et al., 2013). An Internet-based survey advantage is the ability to reduce geographic boundary challenges (Chang & Vowles, 2013). With cross-national research populations, an Internet-based survey may be one of the most effective means of study data collection (King et al., 2014).

Sensitive subject matter desensitizing. Respondents can view survey items as sensitive if considered intrusive, if the questions raise fears about information disclosure repercussions, or if inquiries trigger social desirability issues (Roster et al., 2014). Topic sensitivity can vary widely across cultures and countries (Roster et al., 2014). Sensitive subject matter desensitizing can occur because stronger potential anonymity may permit less embarrassment in answering certain confidential questions or feeling more comfortable discussing controversial topics (Chang & Vowles, 2013; Roster et al., 2014). Accordingly, Internet-based surveys can enhance the reporting level of sensitive information and achieve reporting accuracy above other modes of data collection (Roster et al., 2014).

Careless response identification. The ease and utility of online data collection continue to improve in step with IT innovations (King et al., 2014). Another potential advantage of Internet-based data collection is the ability to determine how long each participant took to complete study instrumentation (King et al., 2014). This feature allows the researcher to identify participants who race through the survey items without reading the inquiry item response request (King et al., 2014). Resultantly, a researcher can indicate and exclude unacceptable responses to reduce measurement error (Chang & Vowles, 2013; King et al., 2014).

Data Collection Technique Disadvantages

Researchers have suggested that few differences exist between data acquired online and traditional self-report collection methods (King et al., 2014). However, online data collection presents challenges requiring appropriate researcher responses. For this ISG study, using the Internet-based survey technique had possible shortcomings that included access constraints, truthfulness issues, legal and ethical issues, selection bias, and inadequate response rates.

Access constraints. Survey design choices affect research quality or quantity data indices (Chang & Vowles, 2013). An online survey design was best for respondents who had easy access to the Internet and felt comfortable sharing information using technology (Chang & Vowles, 2013). Online survey restrictions can occur because the population may lack adequate physical or mental Internet access capability (Chang & Vowles, 2013; King et al., 2014).

Truthfulness issues. True respondent sentiments may be inaccurately recorded in Internet-based survey items (Roster et al., 2014; Ward & Pond, 2015). Truthfulness issues can arise because of intentional or unintentional careless responses that are difficult to detect (Chang & Vowles, 2013). Researchers have suggested that meticulously constructed Internet-based survey instructions may affect respondent attentiveness (Ward & Pond, 2015).

Legal and ethical issues. Legal and ethical issues can occur when survey data are stored online and managed by third party providers (Chang & Vowles, 2013). Under third party provider use, the researcher cannot provide complete confidentiality, anonymity,

privacy, and security (Chang & Vowles, 2013). Accordingly, the researcher must impart enhanced informed consent and potential deception care with Internet-based surveys (Chang & Vowles, 2013).

Selection bias. Though very similar individuals or groups should comprise a human subject study, population bias is an inherent issue with Internet surveys because frequent users are likely very different from infrequent users or nonusers (Chang & Vowles, 2013). Internet-based survey selection bias can occur using the same respondents for both predictor variables and criterion variable that may also generate common methods bias (CMB; N. Wang et al., 2012). As a subcategory of selection bias, sampling bias may occur because some potential respondents might not be reachable via the Internet (Chang & Vowles, 2013).

Inadequate response rates. Concerns about various issues associated with Internet use can generate a higher number of nonresponses to the survey instruments (Chang & Vowles, 2013). The survey response rate may be low as a result of the sensitive nature of an ISG study (Yaokumah, 2013). Organizational manager-leaders are frequently unwilling to participate in information security research due to the perceived disclosure risks regarding system vulnerabilities and critical data (Barton, 2014). Previous survey-based research evidence suggested that when collecting data of a sensitive nature, the researcher should expect a very low response rate (Flores et al., 2014).

Data Analysis

The purpose of data analysis was summarizing collected data for easier comprehension and furnishing answers to the research question (Yaokumah, 2013, 2014). The research question was this: What is the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations? The null hypothesis was strategic alignment, resource management, risk management, value delivery, performance measurement implementations are not significantly related to ISG effectiveness. The alternative hypothesis was strategic alignment, resource management, risk management, value delivery, performance measurement implementations are significantly related to ISG effectiveness.

The choice of statistical techniques depends on the underlying functions, assumptions, and data types of variables under study (Yaokumah, 2013). A researcher employs more than one predictor variable when performing multiple linear regression (MLR; Bhattacherjee, 2012; Green & Salkind, 2014). MLR enables researchers to answer questions concerning the effect multiple predictor variables have on the variance in a single criterion variable (Anderson, 2015; Barrett, 2016; Nathans, Oswald, & Nimon, 2012; Yaokumah, 2013). For my ISG study, there was a priori expectation that a simultaneous multiple regression analysis would occur because Walden University (2014) requires, at least, two predictor variables when employing a quantitative research method in a doctoral study. I used MLR to analyze the data. MLR was employed to

establish the extent ISG domain practices relate to effectual ISG. MLR was the omnibus analysis in this ISG study.

Regression analysis is the process of estimating regression coefficients (Bhattacherjee, 2012). With regression analysis (also known as least squares analysis), explanations of criterion variable attributes occur regarding one or more predictor variables. Regression analysis determines functional relationships between quantitative variables (Bhattacherjee, 2012). Regression analysis permits finding trend lines and developing models based on the calculated association of variables. Regression analysis extends subject correspondence seeking to find a linear relationship equation among selected variables (Green & Salkind, 2014). Standard multiple regression permits the researcher to evaluate the relationships between a predictor variable set and a criterion variable (Yaokumah, 2013).

I considered other regression techniques such as hierarchical and stepwise regression. Hierarchical regression enables researcher examination of the relationships between a predictor variable set and a criterion variable, after controlling for the effects of some other predictor variables on the criterion variable (Barrett, 2016). Stepwise regression permits the researcher performing an exploratory investigation to identify the predictor variable subset that has the strongest relationship to a criterion variable (Barrett, 2016; Cowley et al., 2015). This ISG doctoral study did not include any controlling predictor variables that justified using hierarchal regression analysis. Moreover, given this ISG doctoral study was not exploratory, and scholarly evidence was available

regarding the utility and importance of each predictor variable, using stepwise regression analysis was inappropriate.

Data Cleaning and Screening

Researcher data cleaning is an error detection and correction process for collected data (Smith, 2016). Data cleaning assist the researcher in preparing collected Internet-based survey responses for analysis (Ward & Pond, 2015). A researcher should also perform data screening to reduce the negative effect of missing data on any subsequent analysis (Badara & Saidin, 2014). The informed consent form for this study stated participants' individual identities would remain confidential, and I would not collect any names or other identifying information during the survey. Researchers can use de-identification procedures to omit personal identifiers (Bailey, 2016) linked to study participant supplied information. Given the ethical responsibilities concerning anonymity and confidentiality (Brakewood & Poldrack, 2013; NCPHS, 1979; Yaokumah, 2013), I omitted data that identified the participants and the represented corporations from the study.

In preventing harm or suffering because of research participation, participants had no requirement to answer survey questions before continuing to the next stages of the study (Nosek et al., 2012). The one-at-a-time condition existed for presenting survey instrument items to minimize the likelihood participants would choose not to convey perceptions (Nosek et al., 2012). If a respondent decided to skip a survey question or item, the computer application allowed the respondent to proceed to the next survey page. Consequently, after survey research dataset transfer to a personal computer, a response

review occurred to determine whether any requested data is missing. This ISG study necessitated a data review because researchers reported that Internet-based surveys have a higher missing data rate than paper and pencil surveys (Weigold et al., 2013). Once completed, I commenced goodness-of-fit data analysis.

MLR assumptions are linearity, independence of observations, constant variance, and normality (Green & Salkind, 2014). Scatterplots, partial regression plots, and probability-probability plots are descriptive statistics that confirm whether collected data violated statistical assumptions associated with the investigator's MLR research tools (Yaokumah, 2013). I examined the assumptions underlying MLR through computing descriptive statistics. If assumption violations occurred during my study, additional data analysis procedures were necessary for the planned data analysis. Assumption violation remediation encompassed using bootstrapping procedures.

Interpretation of Inferential Results

I reported suitable bootstrap 95% confidence intervals where appropriate. Statistical Package for the Social Sciences (SPSS) version 21 served as the data analysis tool in this ISG study. SPSS output yields various statistics requiring interpretation for this study. The research specific parameters to interpret were (a) R^2, (b) *F*, (c) *B*, (d) *SE B*, (e) β, (f) *Sig. (p)*, and (g) *t*.

- R^2: is a measure of how much variance in the criterion variable occurs through the linear combination of predictor variables (Fritz, Morris, & Richler, 2012; Green & Salkind, 2014; Nathans et al., 2012). R^2 can range from 0 to 1, where higher values represent more variance (Green & Salkind, 2014). For example,

an R^2 value of 0.17 means the predictor variables account for 17% of the variance in the criterion variable.

- *F*: is the mean regression sum of squares divided by the mean error sum of squares (Green & Salkind, 2014). An *F* value can range from 0 to a relatively large number, where unequal means imply the population has an abnormal distribution (Shaffer, Kowalchuk, & Keselman, 2013). For instance, a relatively large *F* value can indicate rejection of the null hypothesis when combined with a significant *p*-value in deciding if the overall results are significant.
- *B*: is the coefficient weight associated with the regression equation (Green & Salkind, 2014; Nathans et al., 2012) generated by subtracting the mean and dividing by the standard deviation. However, unstandardized *B* coefficients are not useful for comprehending the relative importance of the predictor variables (Green & Salkind, 2014). *B* coefficient standardization occurs so that the predictor and criterion variables have a mean of 0 and standard deviation of 1 (Green & Salkind, 2014). The standardized *B* coefficient represents the change in response to a change of 1 standard deviation in a predictor variable (Nathans et al., 2012). For example, a statistically significant *B* coefficient of 0.90 means each unit increase in the predictor variable will correspond to a 0.90 unit criterion variable increase.
- *SE B*: is the standard error (i.e. the square root of the estimated variance) weight associated with the regression equation (Green & Salkind, 2014). The

SE B coefficient is positive, where a small value represents a more precise estimate (Bhattacherjee, 2012). For instance, if the standard error of variable "A" coefficient is lower than that of variable "B", the model was able to estimate the coefficient for "A" with greater precision.

- β: is a numerical constant defining a functional relationship in the population (Green & Salkind, 2014). βs can range from a negative to a positive number, where the computed value reflect the actual criterion variable scores maximally correlated with the predicted criterion variable scores for the sample data (Green & Salkind, 2014). Resultantly, good prediction criterion variable scores will tend to equal actual criterion variable scores.
- *Sig. (p)*: is the probability value for the significance level of the tested hypothesis dependent on the sample size (Lin, Lucas Jr, & Shmueli, 2013). *Sig. (p)* can range from 0 to 1, where the value is less than or equal to the chosen α the results indicate substantial evidence against null hypothesis acceptance (Lin et al., 2013; Rao, 2012). For instance, if the SPSS calculated MLR results in a *Sig. (p)* at the 0.02 level and $\alpha = 0.05$, there is sufficient evidence against null hypothesis acceptance.
- *t* - *t* is a measure of the difference between an observed sample statistic and the hypothesized population parameter in standard error units (Bhattacherjee, 2012; Green & Salkind, 2014). The *t* value can range from a negative to a positive number, where a nonzero result indicates sample variance (Green & Salkind, 2014). For example, if the *p*-value associated with the *t* value is less

than the α-level with an imbalance between the observed sample statistic and the hypothesized population parameter, there is sufficient evidence against null hypothesis acceptance.

Study Validity

A researcher's method choice affects the validity and generalizability of the investigated phenomenon (Wahyuni, 2012). In the following study validity subsections, I explain my procedures for ensuring statistical conclusion validity and quantitative research generalizability. I describe the threats to statistical conclusion validity as well as how I addressed the threats to statistical conclusion validity. I also discuss the conditions enabling the generalizability of research findings to larger populations and settings.

Statistical Conclusion Validity

Statistical conclusion validity reflects assessing the mathematical relationships between variables, and making inferences regarding whether the statistical formulation correctly expresses the true covariation (Venkatesh et al., 2013). Statistical conclusion validity addressed statistical evidence of covariation quality for this ISG study. Statistical conclusion validity necessitates that the statistics are appropriate, and findings from the statistical analysis are adequate to construct a narrative (Zachariadis et al., 2013). Threats to study validity are a significant issue because they can reduce collected data representativeness (Christ, 2013; R. Davis, 2008). Sample size, reliability of the instrument, and data assumption violations were threats to statistical conclusion validity.

Sample size. Given an effect size and variability, the researcher's sample size estimate represents the required subject number to detect a variable association (Rao,

2012). I used the stratified sampling technique for generating a corporate sector sample frame and random sampling techniques to select sample participants from the organizations within the corporate sectors. The purpose of choosing these sampling methods was to attain sample representativeness and adequacy within the selected population. I assumed adequate sample size obtainment if the acceptable a priori power range response rate occurred. A random sample response rate of 92 manager-leaders was necessary to achieve a minimum power of 0.80.

Researchers should consider error evaluations when performing statistical testing (Gelman & Carlin, 2014). Regarding error sources, there is the risk that the sample indicates incorrect test hypothesis rejection (Rao, 2012). Sample size influences *p*-value (Lin et al., 2013; Salibian-Barrera, Aelst, & Yohai, 2016). A Type 1 error is a frequent violation of statistical conclusion validity. I reduced the Type 1 error risk threat by performing a methodical hypothesis examination. Specifically, I controlled potential Type 1 errors by requiring a *p*-value of less than 0.05. I also performed MLR assumptions examination to address potential error source threats that affect statistical conclusion validity. Selecting an appropriate sample size based on a power analysis was an attempt to combat the sample size threat.

Data assumptions. Assumptions surrounding linear regression are sample size, multicollinearity, outliers, normality, linearity, homoscedasticity, and independence of residuals (Green & Salkind, 2014; Wiedermann & Eye, 2015). For MLR, I addressed statistical assumptions concerning the multivariate independence of observations, homoscedasticity, normality, and linearity through attempting to acquire a medium

population, random sample frame selection, and descriptive statistics examination. I generated and examined scatterplots and probability-probability plots using SPSS to confirm whether the collected data violated the statistical assumptions. Where these assumption violations occurred, I intended to address the assumption violations using bootstrapping procedures.

In determining if multicollinearity exists through a technique congruent with previous research (i.e. Ferguson, Green, Vaswani, & Wu, 2013; Lin et al., 2013), I computed correlation coefficients for all pairs of predictor variables. Researchers typically consider multicollinearity a serious problem if the correlation between two variables is greater than 0.80 (D'Arcy & Greene, 2014). If an assumption violation occurred, I was prepared to remove one of the variables from the model in response to a multicollinearity condition above 0.90. Removing a predictor variable from a model may lead to specification bias (Zainodin & Yap, 2013).

Reliability of the instrument. I used the data collected from the sample respondents to evaluate the reliability coefficient (i.e. Cronbach's α). Moreover, I compared my computed reliability coefficients to the reported Yaokumah (2013) reliability coefficients in the Data Collection Instruments section. The reliability coefficient ranges from 0 to 1, where 0 represents a low internal consistency and 1 represents a high internal consistency for the research instrument (Green & Salkind, 2014; Yaokumah, 2013, 2014; Yaokumah & Brown, 2014). Higher internal consistency imparts better procedure measurement properties if the research measures do not diverge in the propensity to generate systematic responding (Nosek et al., 2012). The acceptable

reliability coefficients of measured variables are values > 0.70 (Chang & Vowles, 2013; Roster et al., 2014; Yaokumah, 2013).

Generalizability

Quantitative research generalizability is time and context-free applicability of investigator results presented in abstracted or nomothetic statements (Yilmaz, 2013). External validity addresses the degree that the research results generalize (Zachariadis et al., 2013) to larger populations (Wahyuni, 2012) and settings (Venkatesh et al., 2013). External statistical generalization stems from acquiring a representative statistical sample (Frels & Onwuegbuzie, 2013). In this study, the targeted population consisted of strategic and tactical leaders of the 500 largest for-profit United States headquartered corporations. I used the stratified sampling technique for generating a corporate sector sample frame and random sampling techniques to select sample participants from the organizations within the corporate sectors. The purpose of choosing these sampling methods was to attain sample representativeness and adequacy within the selected population.

Transition and Summary

With cyber attackers targeting large corporations achieving a 93% success rate during 2013 (Brewer, 2014), IT leaders needed to improve ISG practices (Silic & Back, 2014). Grounded in corporate governance theory, the purpose of this quantitative correlational study was to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. I sought to

collect survey data from a minimum of 92 strategic and tactical leaders of the 500 largest for-profit United States headquartered corporations.

Simultaneously, I employed MLR techniques, using SPSS version 21, to assess the relationship between the predictors and criterion variable. The implications for positive social change include the potential to understand the correlates of ISG effectiveness better, thus increasing the propensity for consumer trust and reducing consumers' costs. In Section 3, I cover the presentation of research outcomes, the business and social implications of the study, recommendation for action, recommendations for further research, my reflections, as well as a summary and study conclusions.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this quantitative correlational study was to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. I deployed a 59-item survey instrument to collect research data for correlation and regression analysis. Based on the outcomes of the proportional stratification data collection procedures (one valid response), I was unable to reject the null hypothesis. Thus, I could not indicate the relationship between implementations of strategic alignment, resource management, risk management, value delivery, performance measurement, and ISG effectiveness in United States-based corporations based on test results.

I recruited additional participants using nonprobability sampling procedures to satisfy Walden University data collection and analysis requirements. Nonprobability sampling affects the researcher support for knowledge assertions (Cheng, Dimoka, & Pavlou, 2016). Nonetheless, I subsequently performed pattern recognition and MLR analysis to test the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness. The predictor variables were strategic alignment, resource management, risk management, value delivery, and performance measurement implementations. ISG effectiveness was the criterion variable. Based on the outcomes of performed procedures, I rejected the null hypothesis. Test results indicated that strategic alignment, resource

management, risk management, value delivery, and performance measurement implementations were significant predictors of ISG effectiveness in United States-based corporations.

Presentation of the Findings

MLR was employed to assess the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. The null hypothesis was that strategic alignment, resource management, risk management, value delivery, and performance measurement implementations would not predict ISG effectiveness. The alternative hypothesis was that strategic alignment, resource management, risk management, value delivery, and performance measurement implementations would predict ISG effectiveness.

Descriptive Statistics

I requested and received permission to recruit additional sample frame participants from the Walden University IRB. The third survey response for this ISG study yielded 95 eligible participants. Table 8 depicts the means and standard deviations for the study variables.

Table 8

Mean and Standard Deviation for Study Variables (N = 95)

Variable	*M*	*SD*	Bootstrapped 95% CI (*M*)
ISG Effectiveness	3.22	0.54	[3.10, 3.32]
Strategic Alignment	3.05	0.48	[2.96, 3.15]
Value Delivery	2.99	0.71	[2.84, 3.14]
Risk Management	3.07	0.49	[2.98, 3.16]
Performance Measurement	3.03	0.73	[2.89, 3.18]
Resource Management	3.05	0.40	[2.97, 3.13]

Note. M = mean and SD = standard deviation.

Tests of MLR Assumptions

The assumptions of multicollinearity, outliers, normality, linearity, homoscedasticity, and independence of residuals were evaluated. Bootstrapping, using 2,000 samples, enabled combating the influence of assumption violations.

Multicollinearity. Multicollinearity was evaluated by viewing the correlation coefficients among the predictor variables. All bivariate correlations were small to medium (Table 9); therefore, the violation of the assumption of multicollinearity was not evident.

Table 9

Intercorrelations Among ISG Model Predictor Variables (N = 95)

Variable	1	2	3	4	5
1. Strategic alignment	1.00	0.13	0.39	0.27	0.32
2. Value delivery	0.13	1.00	0.06	-0.04	0.22
3. Risk management	0.39	0.06	1.00	0.39	0.29
4. Performance measurement	0.27	-0.04	0.39	1.00	0.20
5. Resource management	0.32	0.22	0.29	0.20	1.00

Outliers, normality, linearity, homoscedasticity, and independence of residuals. Outliers, normality, linearity, homoscedasticity, and independence of residuals were evaluated by examining the normal probability plot (P-P) of the regression standardized residual (Figure 6) and the scatterplot of the standardized residuals (Figure 7). The examinations indicated there were no major violations of these assumptions. The tendency of the points to lie in a reasonably straight line (Figure 6), diagonal from the bottom left to the top right, provides supportive evidence the assumption of normality has not been grossly violated (Pallant, 2010). The lack of a clear or systematic pattern in the scatterplot of the standardized residuals (Figure 7) supports the tenability of the assumptions being met. However, 2,000 bootstrapping samples were computed to combat any possible influence of assumption violations, and 95% confidence intervals based upon the bootstrap samples are reported where appropriate.

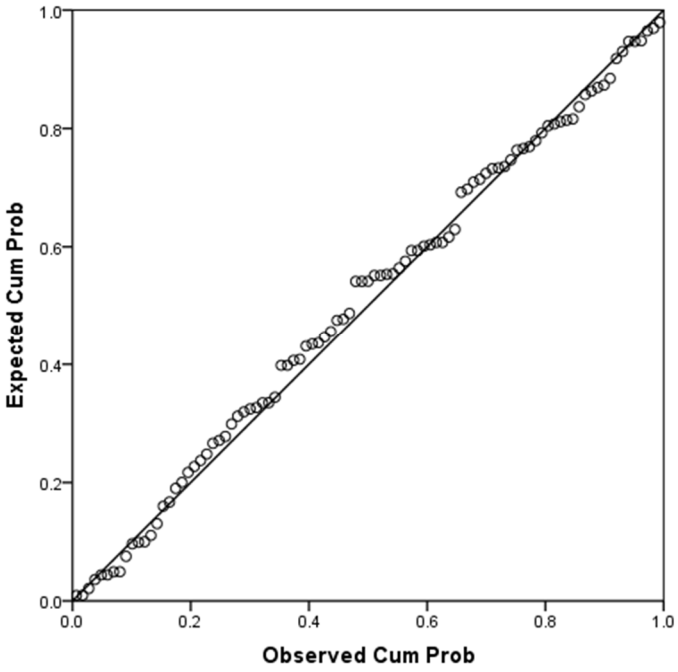

Figure 6. Normal probability plot (P-P) of the regression standardized residuals. Dependent variable: ISG Effectiveness.

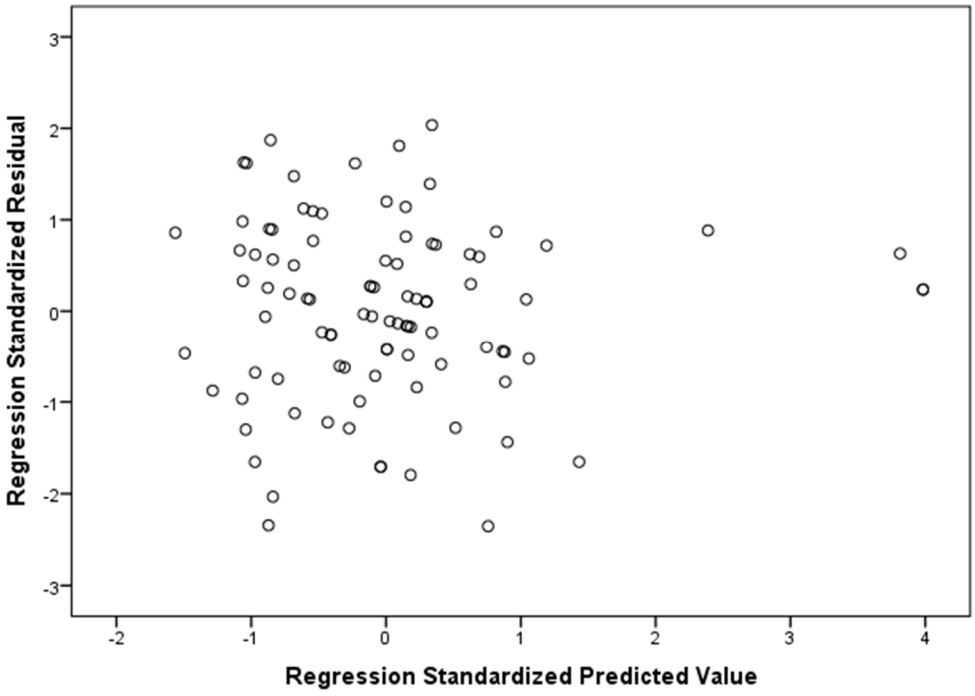

Figure 7. Scatterplot of the standardized residuals.

Inferential Statistics

Standard MLR, α = .05 (two-tailed), was employed to examine the efficacy of strategic alignment, resource management, risk management, value delivery, performance measurement implementations in predicting ISG effectiveness. The predictor variables were strategic alignment, resource management, risk management, value delivery, and performance measurement. The criterion variable was ISG effectiveness. The null hypothesis was that strategic alignment, resource management, risk management, value delivery, performance measurement implementations are not significantly related to ISG effectiveness. The alternative hypothesis was that strategic alignment, resource management, risk management, value delivery, performance measurement implementations are significantly related to ISG effectiveness. Preliminary analyses occurred to assess whether I met the independence of observations, independence of residuals, normality, linearity, homoscedasticity, multicollinearity, and outliers data assumptions using the acquired proportionally stratified and modified convenience sample. I noted no serious data assumption violations (see *Tests of MLR Assumptions*).

The model as a whole was able to significantly predict ISG effectiveness, $F(5, 89) = 3.08$, $p = 0.01$, $R^2 = 0.15$. The R^2 (0.15) value indicated that approximately 15% account for variations in ISG effectiveness by the linear combination of the predictor variables (strategic alignment, resource management, risk management, value delivery, and performance measurement). In the final model, strategic alignment was statistically significant ($t = 2.401$, $p <= 0.018$). Resource management, risk management, value delivery, and performance measurement did not explain any significant variation in ISG

effectiveness. Table 10 depicts the regression summary table, which includes the regression analysis values for resource management, value delivery, risk management, and performance measurement in predicting ISG effectiveness. The final predictive equation was as follows: ISG Effectiveness = 1.542 + 0.299(Strategic Alignment) + 0.052(Resource Management) + 0.035(Risk Management) + 0.053(Value Delivery) + 0.113(Performance Measurement).

Table 10

Regression Analysis Summary for ISG Predictor Variables (N = 95)

Variable	*B*	*SE B*	β	*t*	*p*	Bootstrapped 95% CI (*B*)
Strategic Alignment	0.299	0.124	0.265	2.401	0.018	[0.008, 0.571]
Resource Management	0.052	0.145	0.038	0.358	0.721	[-0.230, 0.335]
Risk Management	0.035	0.126	0.031	0.274	0.785	[-0.246, 0.319]
Value Delivery	0.053	0.077	0.069	0.685	0.495	[-0.100, 0.211]
Performance Measurement	0.113	0.800	0.152	1.410	0.162	[-0.027, 0.257]

Strategic alignment. The positive slope for strategic alignment (0.299), as an ISG effectiveness predictor, indicated there was approximately a 0.299 increase in ISG effectiveness for each 1-point increase in strategic alignment. In other words, ISG effectiveness tends to increase as strategic alignment increases. The squared semipartial coefficient that estimated how much variance in ISG effectiveness was uniquely predictable from strategic alignment was 0.06, indicating that 6% of the variance in ISG effectiveness is uniquely accounted for by strategic alignment, when controlling value

delivery, resource management, risk management, and performance measurement constructs.

Analysis summary. The purpose of this study was to examine the efficacy of strategic alignment, resource management, risk management, value delivery, and performance measurement in predicting ISG effectiveness in United States-based corporations. I conducted a standard MLR test. Despite the absence of any serious data assumption violations surrounding the multiple regressions analysis, I undertook a bootstrapping test using 2,000 resamples and a 95% confidence interval to combat any potential statistical assumption violations.

I concluded from the performed analysis that the combined strategic alignment, resource management, risk management, value delivery, and performance measurement implementations were able to predict ISG effectiveness for United States-based corporations, $F(5, 89) = 3.08$, $p = 0.01$, $R^2 = 0.15$. Further, strategic alignment, measured by the Yaokumah (2013) instrument, was significantly associated with ISG effectiveness for United States-based corporations. The final predictive equation was as follows: ISG Effectiveness = 1.542 + 0.299(Strategic Alignment) + 0.052(Resource Management) + 0.035(Risk Management) + 0.053(Value Delivery) + 0.113(Performance Measurement).

Theoretical Framework and Relationships

Researchers use a theoretical framework to synthesize and integrate cogitations when describing, explicating, or predicting a phenomenon under study, as well as guiding an investigation (Imenda, 2014). Corporate governance theory is an appropriate theoretical foundation to study ISG (Hu et al., 2012; Whitman & Mattord, 2012;

Yaokumah & Brown, 2014). The method used for this research included the foundational governance theory capabilities in providing holistic corporate ISG practices. The chosen theory was relevant in defining the constructs that helped evaluate ISG because corporate governance propositions furnished an organizational view and understanding of the phenomenon. Deriving constructs from a previously established and proven theory also helped measure selection as well as furnished a valid and comprehensive phenomenon understanding.

The results of my research confirmed the propositions of Yaokumah (2013) as well as Yaokumah and Brown (2014), who considered corporate governance theory as the most appropriate theoretical framework for the study of ISG processes. This study supported the understanding that ISG effectiveness realization can occur through sound corporate governance descriptive and explanatory theories. As for particulars, ISG effectiveness realization may occur when management jointly deploys stakeholder, agency, and resource-based theories. Stakeholder theory addresses the commitment to the corporation's stakeholders with the purpose of aligning perceived stakeholders' interest with corporate, business, and functional objectives for value delivery (Yaokumah, 2013). Agency theory describes the responsibility, accountability, and authority of manager-leaders as agents who ensure performance through monitoring and measurement to efficiently and effectively minimize risks. Moreover, resource-based theory models enterprise-controlled assets, capabilities, competencies, processes, and knowledge availability with the aim of strategically orchestrating resources to achieve organizational goals and enhanced competitiveness (Tabares et al., 2015; Varsei et al., 2014).

Yaokumah (2013), as well as Yaokumah and Brown (2014), found that organizational value delivery, risk management, performance measurement, resource management practices positively correlate to effective ISG strategic alignment. I extended the Yaokumah as well as Yaokumah and Brown ISG model to the relationship between strategic alignment, value delivery, risk management, resource management, performance measurement implementations, and ISG effectiveness. My study outcome indicated strategic alignment practices were the most significant predictor of ISG effectiveness.

Yaokumah (2013) found value delivery and risk management variables are significant predictors of ISG effectiveness. Moreover, Yaokumah (2013) found ISG value delivery is a less significant predictor of ISG effectiveness than risk management. My combined second and third ISG survey responses disconfirmed that the value delivery and risk management variables are significant predictors of ISG effectiveness as found by Yaokumah (2013). My combined second and third ISG survey responses also disconfirmed value delivery is a less significant predictor of ISG effectiveness than risk management as found by Yaokumah (2013).

Applications to Professional Practice

The results of my regression analysis indicated strategic alignment was the only statically significant contributor to ISG effectiveness. Strategic and tactical leaders of the 500 largest for-profit United States headquartered corporations can achieve effectual ISG by ensuring a tight coupling between the business and information security strategies. For achieving this end, strategic and tactical leaders should establish the business

objective of ensuring information security effectiveness through strategically aligned value delivery, risk management, performance measurement, and resource management policies, procedures, as well as technology.

Security threats can hinder or reduce the possibility of business and IT objective achievement, value creation, and value preservation (R. Davis, 2008; Srivastava & Kumar, 2015; Tarafdar et al., 2015). Ethically, management must protect the organization's information assets from potential external and internal threats that can compromise confidentiality, integrity, and availability to preserve processing, presentation, and use value (Ahmad et al., 2014; R. Davis, 2008; Whitman & Mattord, 2012). Legally, within the information security control system, corporate manager-leaders as agents are responsible and accountable for deploying controls inhibiting security breaches mandated by laws and regulations (Clark & Harrell, 2013; R. Davis, 2008). Information security management should actively participate in ensuring their enterprise has an appropriate control environment that protects information assets (Flores et al., 2014; R. Davis, 2008).

Without regard to whether scholars view information security as a program supporting corporate governance (e.g., Bahl & Wali, 2014; Edwards, 2013) or an IT governance program subset (e.g., Kwon et al., 2013; Yaokumah, 2013), IAP is necessary. An adaptive balance between sound management and applied technology reflects effectual information security (Ahmad et al., 2014; Safa et al., 2016). Corporate management's development and deployment of sound information security policies and procedures enable ensuring appropriate information assets safeguarding while

efficaciously applied technology can increase effectiveness to address potential exterior and interior threats (Ahmad et al., 2014). My doctoral study results might assist IT leaders with improving ISG practice areas to protect information assets more effectively with a concomitant reduction in recovery costs.

Implications for Social Change

The implications for positive social change include potential increased trust and reduced costs from e-commerce use. Trust is a perception desire to rely on something or someone for security (Safa & Solms, 2016). Consumer perceptions of Internet information security can influence trust beliefs and trusting intentions (Bahmanziari & Odom, 2015). An e-commerce related information security incident can cause a measurable negative influence on customer behaviors (Arief et al., 2015; Choi & Nazareth, 2014; Lee & Lee, 2012). Effectual security solutions are imperative to achieving trust relationships, especially with new customers (Choi & Nazareth, 2014). A higher perceived Internet security level leads to greater intent to purchase products using B2C e-commerce websites (Hartono, Holsapple, Kim, Na, & Simpson, 2014). The potential exists to provision IT leaders with a better understanding of the factors related to designing and deploying effectual ISG for B2C e-commerce that enables consumer trust.

Corporate IT leaders can improve the trust factor for stakeholders in technology containing personally identifiable information through effectual ISG (R. Davis, 2008). Personal privacy and identity are among the most valuable intangible assets individuals ever own (R. Davis, 2008). Nonetheless, technological manipulation continually enables

intentional or unintentional privacy invasions (R. Davis, 2008). Cyber attackers have ranged from hobbyist to spies typically motivated by personal, financial, or political factors (Arief & Adzmi, 2015). IT related identity theft had cost consumers over $5 billion yearly (Trautman, Truche, & Wetherbe, 2013). Cyber defenders were unable to adequately address cybercrime through only implementing technical information security solutions (Arief & Adzmi, 2015). Therefore, corporate cyber defenders needed to consider the human factors involved in cybercrime (Arief & Adzmi, 2015). Arief and Adzmi (2015) suggested an efficient approach for preventing cybercrime could include cyber attacker identification as well as arrest, and profiling potential victims.

Information security breaches were a controversial concern (Safa et al., 2016; Safa & Solms, 2016). A researcher argued that individuals engaged in cybercrime due to the lack of deterrents as well as psychological factors (Holt & Bossler, 2014). The invasion of privacy is only symptomatic of a critical question confronting individuals living in the information age (R. Davis, 2008): How can corporate information security protect citizenry rights and freedoms while simultaneously controlling criminal inclinations? Choi and Nazareth (2014) suggested substantial investments if properly directed can serve as an effectual information security breach deterrent. More secure IT operations can benefit communities through enhanced governance quality that consequently would increase trust and reduce costs from e-commerce use (Bahmanziari & Odom, 2015; Ludin & Cheng, 2014; Starbuck, 2014; Yaokumah, 2014).

My study results support positive social change aimed at broadening the understanding of activities that influence trust and cost through ISG practices. The

current study uncovered a predictive relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness using my second and third survey outcomes. My first and second ISG survey response rates revealed external security knowledge sharing issues in United States-based corporations. The findings suggest IT leaders have the potential to design and deploy an effective ISG program in their organization by engaging ITGI ISG domain processes that enable consumer trust and reduce consumers' costs.

Recommendations for Action

IT leaders should pay attention to the results, as well as evaluate which ITGI (2008) practice implementations correlate with ISG effectiveness in United States-based corporations. Information security breaches lead to additional costs for corporations and significantly affect the corporate reputation (Safa et al., 2016). IT leaders should work toward fully implementing ITGI ISG domain processes to address the challenges for preventing and deterring information security breaches. IT leaders should also ensure these ITGI ISG domain processes are transparent for sharing with stakeholders. The knowledge furnished by this study can aid IT leaders in deploying measures that can significantly improve an information security program. Corporate manager-leaders, as well as other stakeholders, may use the constructed model for this study as an analytical tool to assist in predicting ISG effectiveness realization.

Upon my graduation from Walden University, my ISG doctoral study will become available through the ProQuest dissertation and thesis database for review by

students, scholars, librarians, and professionals. I will disseminate a summary of findings to research participants interested in reviewing my study results. I will also actively pursue publication in academic journals and practitioner workbooks with references to my doctoral study. Moreover, potential venues for sharing my ISG study outcomes include academic and practitioner conferences, association meetings, as well as Internet-based webinars such as information systems conferences, professional organization meetings, and sponsored compliance training.

Recommendations for Further Research

My study holistically employed five information security domain areas to examine ISG correlates of United States-based corporate business sector types. The sample selection for this ISG study comprised wide population subcategories (United States business sector types). As such, the investigated population findings might be generalizable to large developed country corporations. Though intercorporate ISG business sector predictability matters, there is the need to redress ISG effectiveness at the individual industry type because no single approach to an ISG implementation strategy and devised tactics ensures successful realization (Silic & Back, 2014; Yaokumah, 2013). Consequently, future studies should evaluate ISG effectiveness in corporations within the same industry type.

My study was not without limitations. The response sample size was not large for my first and second ISG surveys. Future researchers should pursue ISG research using a large sample size with innovative survey techniques that generate high response rates to verify the presented model. Alternatively, Barton (2014) suggested future researchers

consider replacing self-reported information security surveys with an investigator or third-party assessments.

Only a few studies have specifically examined the maturity of ISG implementations (e.g., Yaokumah, 2014). However, the degree of ISG realization in developed countries remains an open question (Flores et al., 2014). In particular, two subject related issues are prominent concerning developed countries deploying domain practices to ensure effectual ISG. First, what is the ISG deployment level in United States of America private as well as public corporations? Second, are there any differences in the implementation level of ISG focal areas among developed and developing countries? Through addressing these questions, future researchers will extend available academic literature enabling potential strategic improvements necessary for reasonably ensuring prevention and deterrence of information security threats.

Reflections

After years of serving as an IT auditor and consultant, I have extrapolated that many of the largest organizational formations needed effective leadership in generating consumer confidence regarding information systems management. The research project origin stems from media reported information security breaches. Particularly, based on recent information security debacles documented by journalists, organizational management lacked effective ISG practices when designing, constructing, and deploying information systems and associated technologies. Reflecting on this assessment, my personal integrity, commitment, and reliability values for ensuring appropriate IAP aligned with my professional motivations for pursuing scholarly research enabling

optimal strategic alignment, resource management, risk management, value delivery, and performance measurement implementations for effective ISG of entrusted data.

The performed research improved my understanding regarding the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. Committee members appointed to guide me through the doctoral study process suggested proper research construction. Continuous monitoring and feedback from committee members and making revisions to my study strengthened the scholarly writing in this ISG examination. Following the Walden University (2014) Doctor of Business Administration rubric guidelines was an essential task that benchmarked and measured study progression.

Based on the research question, I employed a quantitative research method with a correlational research design to examine the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. The research environment is becoming increasingly complex (Ross & Onwuegbuzie, 2014), interdisciplinary (Lunde, Heggen, & Strand, 2013), and dynamic. Researchers need a firm understanding of multiple methods employed by other scholars to facilitate communication, to foster collaboration, and to provide rigorous research (Lunde et al., 2013). Thus, quantitative research methods presented through analyzing and synthesizing resources (e.g., Yaokumah, 2013, 2014; Yaokumah & Brown, 2014) assisted in

answering the posed doctoral study research question concerning corporate information security in the United States.

Considering the literature read and evaluated; this ISG study confirmed the research method choice directly affects the validity and generalizability of an undertaken research project. At the detail level, the literature read and evaluated during this ISG study confirmed quantitative research analyses of collected data should address threats to conclusion validity. Moreover, my first and second ISG survey response rates confirmed the significance of culture as an Internet-based data collection factor as suggested by Roster, Albaum, and Smith (2014), and elevated the effect of national cultural norms on external information security knowledge sharing.

My first and second ISG survey response rates also confirmed organizational manager-leaders are frequently unwilling to participate in information security research as suggested by Barton (2014). There are potentially three conceptual metaphors applicable to scholar-practitioners: connector, recycler, and translator (Kram, Wasserman, & Yip, 2012). Within these three conceptual metaphors, I perceived my academic role to encompass business subject matter expert, thought leader, as well as a social change catalyst.

Summary and Study Conclusions

With cyber attackers targeting large corporations achieving a 93% success rate during 2013 (Brewer, 2014), IT leaders needed to improve ISG practices (Silic & Back, 2014). Grounded in corporate governance theory, the purpose of this quantitative correlational study was to examine the relationship between strategic alignment, resource

management, risk management, value delivery, performance measurement implementations, and ISG effectiveness in United States-based corporations. There are two data sources used when performing my doctoral study research: primary and secondary. Preceding the primary data collection, secondary source data generation for my ISG study included a literature review employing online periodical interrogation consisting of a five-step process: journal, database, keywords, and backward as well as forward searches.

Primary data collection for each predictor and criterion variable occurred through an Internet-based survey. I sought to collect survey data from a minimum of 92 strategic and tactical leaders of the 500 largest for-profit United States headquartered corporations. I selected standard MLR techniques to assist in analyzing the data to answer the research question. I applied multiple regression analysis using SPSS version 21 software in assessing the relationship between the predictor variables and criterion variable to enable forecasting secure IT operations. Secure IT operations can benefit communities interfacing with corporate information systems economically and socially (Price, 2014). Effectual security solutions are imperative to achieve trust relationships with stakeholders.

Trust is a social commitment variable (Edwards, 2013). Enabling and maintaining positive trust perceptions are increasingly challenging for business leaders (Kamisan & King, 2013). A corporation lacking trust in deployed information security is an enterprise destined to attain organizational discontinuity (Edwards, 2013). Researchers found trust influence a consumer's purchase decision and affect long-term loyalty through

satisfaction (Choi & Nazareth, 2014). Given information security breaches can have a detrimental satisfaction effect (Arief et al., 2015); public and private stakeholders are increasingly demanding ISG institutionalization with program oversight (Srivastava & Kumar, 2015). Nonetheless, scholarly research furthering understanding the relationship between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness within a particular organizational formation type is sparse. I responded to this information research deficiency by examining prominent ITGI ISG domain practices that may have an influence on corporate ISG effectiveness.

I attempted to demonstrate the influence ITGI ISG domain practices have on ISG effectiveness through receiving responses from my first recruitment effort. Given the 100% nonresponse rate from my first recruitment effort, the regression model was not tested to indicate the variance in ISG effectiveness explained by ISG domain practices. Moreover, the second recruitment effort only generated one complete participant response which precluded regression model testing using SPSS version 21.

My first and second Internet-based survey outcomes implied that a cultural difference regarding ISG knowledge sharing exists between strategic and tactical managers in developed versus developing countries. Shaaban and Conrad (2013) found national culture influences information security in Zanzibar. Other researchers suggested organizational cultures encapsulated within a national culture influence the information security culture (Alnatheer, 2014; Karlsson, Åström, & Karlsson, 2015). Though my adopted research methodology did not encompass testing why this is the case, I suspect

United States national cultural norms for nonmandatory disclosures influence corporate management's security culture for voluntary knowledge sharing through surveys.

Given the low response rates from my first and second surveys, I sought additional survey participants through partnering with professional association managers. I requested professional association managers extract and send my survey participation requests to members who met the eligibility requirements for working in the 500 largest United States-based corporations with at least 1 year of professional experience. I subsequently received 94 responses through deploying my third participant recruitment procedures. The regression model was tested using participant responses from my second and third surveys to indicate the variance in ISG effectiveness explained by ISG domain practices. The results implied that a significant association exists between strategic alignment, resource management, risk management, value delivery, performance measurement implementations, and ISG effectiveness.

My contribution to understanding the effect of ITGI domain practices extends corporate governance theory. My doctoral study results might assist IT leaders with improving ISG practice areas to protect information assets more effectively with a concomitant reduction in recovery costs. However, perhaps more importantly, this study provides corporate IT manager-leaders with the knowledge to develop and deploy an effective ISG program that increases the propensity for consumer trust and reduces consumers' costs.

References

Abraham, E. S. (2012). Information technology, an enabler in corporate governance. *Corporate Governance: The International Journal of Business in Society, 12*, 281-291. doi:10.1108/14720701211234555

Acharya, A. S., Prakash, A., Saxena, P., & Nigam, A. (2013). Sampling: Why and how of it. *Indian Journal of Medical Specialties, 4*, 330-333. doi:10.7713/ijms.2013.0032

Aguirre, I., & Alonso, S. (2012). Improving the automation of security information management: A collaborative approach. *IEEE Security & Privacy, 10*(1), 55-59. doi:10.1109/MSP.2011.153

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*, 357-370. doi:10.1007/s10845-012-0683-0

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management, 35*, 717-723. doi:10.1016/j.ijinfomgt.2015.08.001

Al-Azzam, Z. F., Al-Qura'an, A. B., & Al-Mohameed, H. (2015). How the corporate governance affects organizational strategy: Lessons from Jordan environment. *Journal of Business and Management (IOSR-JBM), 17*(4), 52-56. doi:10.9790/487X-17415266

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567-575. doi:10.1016/j.chb.2015.03.054

Alnaser, N., Shaban, O. S., & Al-Zubi, Z. (2014). The effect of effective corporate

governance structure in improving investors' confidence in the public financial information. *International Journal of Academic Research in Business and Social Sciences, 4*(1), 556-569. doi:10.6007/IJARBSS/v4-i4/562

Alnatheer, M. A. (2014). A conceptual model to understand information security culture. *International Journal of Social Science and Humanity, 4*(2), 104-107. doi:10.7763/IJSSH.2014.V4.327

Alsudiri, T., Al-Karaghouli, W., & Eldabi, T. (2013). Alignment of large project management process to business strategy: A review and conceptual framework. *Journal of Enterprise Information Management, 26*, 596-615. doi:10.1108/JEIM-07-2013-0050

Anderson, L. E. (2015). *Relationship between leadership, organizational commitment, and intent to stay among junior executives* (Doctoral study). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3708010)

Arief, B., & Adzmi, M. A. B. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 2 - defenders and victims. *IEEE Security & Privacy*, *13*(2), 84-88. doi:10.1109/MSP.2015.44

Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 1--attackers. *IEEE Security & Privacy, 13*(1), 71-76. doi:10.1109/MSP.2015.19

Arif, S. (2016). Leadership for change: Proposed organizational development by incorporating systems thinking and quality tools. *Business Process Management Journal, 22*, 939-956. doi:10.1108/BPMJ-01-2016-0025

Atoum, I., Otoom, A., & Ali, A. A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security, 22*, 251-264. doi:10.1108/IMCS-02-2013-0014

Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology,* 12, 529-534. doi:10.1016/j.protcy.2013.12.525

Babar, M. I., Ghazali, M., Jawawi, D. N., & Zaheer, K. B. (2015). StakeMeter: Value-Based stakeholder identification and quantification framework for value-based software systems. *PLoS One, 10*(3), e0121344. doi:10.1371/journal.pone.0121344

Babrahem, A. S., Alharbi, E. T., Alshiky, A. M., Alqurashi, S. S., & Kar, J. (2015). Study of the security enhancements in various e-mail systems. *Journal of Information Security, 6*, 1-11. doi:10.4236/jis.2015.61001

Badara, M. S., & Saidin, S. Z. (2014). Internal audit effectiveness: Data screening and preliminary analysis. *Asian Social Science, 10*(10), 76-85. doi:10.5539/ass.v10n10p76

Bahl, S., & Wali, O. P. (2014). Perceived significance of information security governance to predict the information security service quality in software service industry. *Information Management & Computer Security, 22*, 2-23. doi:10.1108/IMCS-01-2013-0002

Bahmanziari, T., & Odom, M. D. (2015). Prospect theory and risky choice in the ecommerce setting: Evidence of a framing effect. *Academy of Accounting & Financial Studies Journal, 19*(1), 85-106. Retrieved from

http://www.alliedacademies.org

Bailey, M. W. (2016). Seduction by technology: Why consumers opt out of privacy by buying into the Internet of Things. *Texas Law Review, 94*, 1023-1054. Retrieved from http://www.texaslrev.com

Baltatzis, D., Ilioudis, C., & Pangalos, G. (2012). A role engineering framework to support dynamic authorizations in collaborative environments. *Information Security Journal: A Global Perspective, 21*, 12-27. doi:10.1080/19393555.2011.624161

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! discouraging neutralization to reduce IT policy violation. *Computers & Security, 39*, 145-159. doi:10.1016/j.cose.2013.05.006

Barrett, S. (2016). *Effects of information technology risk management and institution size on financial performance.* Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10148398)

Barton, K. A. (2014). *Information system security commitment: A study of external influences on senior management* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3666132)

Barton, K. A., Tejay, G., Lane, M. & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security, 59*, 9-25. doi:10.1016/j.cose.2016.02.007

Berman, S., & Marshall, A. (2014). Reinventing the rules of engagement: Three strategies for winning the information technology race. *Strategy & Leadership,*

42, 22-32. doi:10.1108/SL-05-2014-0036

Bertels, H. M., Koen, P. A., & Elsum, I. (2015). Business models outside the core. *Research Technology Management, 58*(2), 20-29. doi:10.5437/08956308X5802294

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly, 37*, 471-482. Retrieved from http://www.misq.org

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices* [PDF version]. Retrieved from http://scholarcommons.usf.edu

Bishara, A. J., & Hittner, J. B. (2015). Reducing bias and error in the correlation coefficient due to nonnormality. *Educational and Psychological Measurement, 75*, 785-804. doi:10.1177/0013164414557639

Bosco, F. A., Aguinis, H., Singh, K., Field, J. G., & Pierce, C. A. (2015). Correlational effect size benchmarks. *Journal of Applied Psychology, 100*, 431-449. doi:10.1037/a0038047

Boshkoska, M. (2015). Agency problem: Measures for its overcoming. *International Journal of Business and Management,* 10(1), 204-209. doi:10.5539/ijbm.v10n1p204

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review, 5*(4), 28-34. Retrieved from http://timreview.ca

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation, 34*, 342-353.

doi:10.1016/j.technovation.2014.02.001

Brajer-Marczak, R. (2014). Employee engagement in continuous improvement of processes. *Management, 18*(2), 88-103. doi:10.2478/manment-2014-0044

Brakewood, B., & Poldrack, R. A. (2013). The ethics of secondary data analysis: Considering the application of Belmont principles to the sharing of neuroimaging data. *NeuroImage, 82*, 671-676. doi:10.1016/j.neuroimage.2013.02.040

Brewer, R. (2014). Advanced persistent threats: Minimising the damage. *Network Security, 2014*(4), 5-9. doi:10.1016/S1353-4858(14)70040-6

Brooks, M. E., Dalal, D. K., & Nolan, K. P. (2014). Are common language effect sizes easier to understand than traditional effect sizes? *Journal of Applied Psychology, 99*, 332-340. doi:10.1037/a0034745

Brutus, S., Aguinis, H., & Wassmer, U. (2013). Self-reported limitations and future directions in scholarly reports analysis and recommendations. *Journal of Management, 39*, 48-75. doi:10.1177/0149206312455245

Cantor, D. E., Blackhurst, J., Pan, M., & Crum, M. (2014). Examining the role of stakeholder pressure and knowledge management on supply chain risk and demand responsiveness. *International Journal of Logistics Management, 25*, 202-223. doi:10.1108/IJLM-10-2012-0111

Carlo, J. L., Gaskin, J., Lyytinen, K., & Rose, G. M. (2014). Early vs. late adoption of radical information technology innovations across software development organizations: An extension of the disruptive information technology innovation model. *Information Systems Journal, 24*, 537-569. doi:10.1111/isj.v24.6

Carlson, L. V. (2014). *Worker perceptions of the relationship between information security and productivity*. Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3645776)

Catinean, I., & Cândea, D. (2013). Characteristics of the cloud computing model as a disruptive innovation. *Review of International Comparative Management, 14*, 783-803. Retrieved from http://www.rmci.ase.ro

Cavusoglu, H. (Huseyin), Cavusoglu, H. (Hasan), Son, J. Y., & Benbasat, I. (2013). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*, 385-400. doi:10.1016/j.im.2014.12.004

Cegielski, C. G., Bourrie, D. M., & Hazen, B. T. (2013). Evaluating adoption of emerging IT for corporate IT strategy: Developing a model using a qualitative method. *Information Systems Management, 30*, 235-249. doi:10.1080/10580530.2013.794632

Chang, T. Z. D., & Vowles, N. (2013). Strategies for improving data reliability for online surveys: A case study. *International Journal of Electronic Commerce Studies, 4*, 121-130. doi:10.1016/j.cose.2012.09.010

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems, 31*(4), 49-87. doi:10.1080/07421222.2014.1001257

Chen, C. X., Lu, H., & Sougiannis, T. (2012). The agency problem, corporate

governance, and the asymmetrical behavior of selling, general, and administrative costs. *Contemporary Accounting Research, 29*(1), 252-282. doi:10.1111/j.1911-3846.2011.01094.x

Chen, J., Chen, T., Vertinsky, I., Yumagulova, L., & Park, C. (2013). Public-private partnerships for the development of disaster resilient communities. *Journal of Contingencies and Crisis Management, 21*, 130-143. Retrieved from http://onlinelibrary.wiley.com

Chen, Y., Ramamurthy, K., & Wen, K. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188. doi:10.2753/MIS0742-1222290305

Cheng, Z. A., Dimoka, A., & Pavlou, P. A. (2016). Context may be king, but generalizability is the emperor! *Journal of Information Technology, 31*, 257-264. doi:10.1057/s41265-016-0005-7

Chernyak-Hai, L., & Tziner, A. (2014). Relationships between counterproductive work behavior, perceived justice and climate, occupational status, and leader-member exchange. *Journal of Work and Organizational Psychology, 30*, 1-12. doi:10.5093/tr2014a1

Choi, J., & Nazareth, D. L. (2014). Repairing trust in an e-commerce and security context: An agent-based modeling approach. *Information Management & Computer Security, 22*, 490-512. doi:10.1108/IMCS-09-2013-0069

Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of*

Software: Evolution and Process, 26, 496-503. doi:10.1002/smr.1609

Chopra, S., & Sodhi, M. S. (2014). Reducing the risk of supply chain disruptions. *MIT Sloan Management Review, 55*(3), 73-80. Retrieved from http://sloanreview.mit.edu

Chou, D. C. (2015). Cloud computing: A value creation model. *Computer Standards & Interfaces, 38*, 72-77. doi:10.1016/j.csi.2014.10.001

Christ, T. W. (2013). The worldview matrix as a strategy when designing mixed methods research. *International Journal of Multiple Research Approaches, 7*, 110-118. doi:10.5172/mra.2013.7.1.110

Clark, M., & Harrell, E. C. (2013). Unlike chess, everyone must continue playing after a cyber-attack. *Journal of Investment Compliance, 14*(4), 5-12. doi:10.1108/JOIC-10-2013-0034

Claycomb, W. R., Huth, C. L., Flynn, L., Mcintire, D. M., & Lewellen, T. B. (2012). Chronological examination of insider threat sabotage: Preliminary observations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *3*(4), 4-20. Retrieved from http://resources.sei.cmu.edu

Cokley, K. O., & Awad, G. H. (2013). In defense of quantitative methods: Using the "master's tools" to promote social justice. *Journal for Social Action in Counseling and Psychology*, *5*(2), 26-41. Retrieved from http://jsacp.tumblr.com

Cowley, J. A., Greitzer, F. L., & Woods, B. (2015). Effect of network infrastructure factors on information system risk judgments. *Computers & Security, 52*, 142-158. doi:10.1016/j.cose.2015.04.011

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101. doi:10.1016/j.cose.2012.09.010

Cui, M., & Pan, S. L. (2015). Developing focal capabilities for e-commerce adoption: A resource orchestration perspective. *Information & Management, 52*, 200-209. doi:10.1016/j.im.2014.08.006

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security, 22*, 474-489. doi:10.1108/IMCS-08-2013-0057

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285-318. doi:10.2753/MIS0742-1222310210

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review, 31*, 243-256. doi:10.1016/j.clsr.2015.01.005

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy & Security, 8*(4), 27-55. doi:10.1080/15536548.2012.10845665

Davis, K. (2016). A method to measure success dimensions relating to individual stakeholder groups. *International Journal of Project Management, 34*, 480-493.

doi:10.1016/j.ijproman.2015.12.009

Davis, R. E. (2008). *IT auditing: Assuring information assets protection* [CD-ROM version]. Mission Viejo, CA: Pleier.

Davis, R. E. (2011). *Assuring IT governance* [Kindle version]. Retrieved from https://www.amazon.com

Davis, R. E. (2012). *Assuring information security governance* [Kindle version]. Retrieved from https://www.amazon.com

De Haes, S., Grembergen, W., V., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems, 27*(1), 307-324. doi:10.2308/isys-50422

Dellis, A., Skolarikos, A., & Papatsoris, A. G. (2014). Why should I do research? Is it a waste of time? *Arab Journal of Urology, 12*(1), 68-70. doi:10.1016/j.aju.2013.08.007

Denscombe, M. (2013). The role of research proposals in business and management education. *The International Journal of Management Education, 11*, 142-149. doi:10.1016/j.ijme.2013.03.001

Deursen, N. V., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. *Computers & Security, 37*, 31-45. doi:10.1016/j.cose.2013.04.005

Di Gregorio, D. (2013). Value Creation and value appropriation: An integrative, multi-level framework. *The Journal of Applied Business and Economics, 15*, 39-53.

Retrieved from http://www.na-businesspress.com

Drnevich, P. L., & Croson, D. C. (2013). Information technology and business-level strategy: toward an integrated theoretical perspective. *MIS Quarterly, 37*, 483-509. Retrieved from http://www.misq.org

Edwards, C. K. (2013). *A framework for the governance of information security*. Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3607548)

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41*, 1149-1160. doi:10.3758/brm.41.4.1149

Feldman, E. R., & Montgomery, C. A. (2015). Are incentives without expertise sufficient? Evidence from Fortune 500 firms. *Strategic Management Journal, 36*, 113-122. doi:10.1002/smj.2211

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security, 22*, 410-430. doi:10.1108/IMCS-07-2013-0053

Ferguson, C., Green, P., Vaswani, R., & Wu, G. H. (2013). Determinants of effective information technology governance. *International Journal of Auditing, 17*, 75-99. doi:10.1111/j.1099-1123.2012.00458.x

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving integration in mixed methods designs, principles and practices. *Health Services Research, 48*, 2134-2156. doi:10.1111/1475-6773.12117

Findikli, M., Yozgat, U., & Rofcanin, Y. (2015). Examining organizational innovation

and knowledge management capacity: The central role of strategic human resources practices (SHRPs). *Procedia - Social and Behavioral Sciences, 181*, 377-387. doi:10.1016/j.sbspro.2015.04.900

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90-110. doi:10.1016/j.cose.2014.03.004

Foss, N. J., & Dobrajska, M. (2015). Valve's way: Vayward, visionary, or voguish? *Journal of Organization Design, 4*(2), 12-15. doi:10.7146/jod.20162

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development, 91*, 184-194. doi:10.1002/j.1556-6676.2013.00085.x

Fritz, C. O., Morris, P. E., & Richler, J. J. (2012). Effect size estimates: Current use, calculations, and interpretation. *Journal of Experimental Psychology: General*, *141*(1), 2-18. doi:10.1037/a0024338

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy and Security, 11*, 38-54. doi:10.1080/15536548.2015.1010985

Gelman, A., & Carlin, J. (2014). Beyond power calculations assessing type s (sign) and type m (magnitude) errors. *Perspectives on Psychological Science, 9*, 641-651. doi:10.1177/1745691614551642

Gil-Lafuente, A., & Paula, L. B. (2013). Algorithm applied in the identification of stakeholders. *Kybernetes, 42*, 674-685. doi:10.1108/K-04-2013-0073

Glavas, A., & Mish, J. (2015). Resources and capabilities of Triple Bottom Line firms: Going over old or breaking new ground? *Journal of Business Ethics, 127*, 623-642. doi:10.1007/s10551-014-2067-1

Glinkowska, B., & Kaczmarek, B. (2015). Classical and modern concepts of corporate governance (stewardship theory and agency theory). *Management, 19*(2), 84-92. doi:10.1515/manment-2015-0015

Green, S. B., & Salkind, N. J. (2014). *Using SPSS for Windows and Macintosh: Analyzing and understanding data*. Upper Saddle River, NJ: Pearson Education.

Guadalupe, M., Li, H., & Wulf, J. (2014). Who lives in the C-suite? Organizational structure and the division of labor in top management. *Management Science, 60*, 824-844. doi:10.1287/mnsc.2013.1795

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*, 320-326. doi:10.1016/j.im.2012.08.001

Guo, L., Smallman, C., & Radford, J. (2013). A critique of corporate governance in China. *International Journal of Law and Management, 55*, 257-272. doi:10.1108/IJLMA-10-2011-0012

Hardcopf, R., Gonçalves, P., Linderman, K., & Bendoly, E. (2016). Short-term bias and strategic misalignment in operational solutions: Perceptions, tendencies, and traps. *European Journal of Operational Research*. Advance online publication.

doi:10.1016/j.ejor.2016.09.036

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*, 97-114. doi:10.1108/IMCS-03-2013-0019

Harrison, J. S., & Wicks, A. C. (2013). Stakeholder theory, value, and firm performance. *Business Ethics Quarterly, 23*, 97-124. doi:10.5840/beq20132314

Harrison, R. L. (2013). Using mixed methods designs in the Journal of Business Research, 1990-2010. *Journal of Business Research, 66*, 2153-2162. doi:10.1016/j.jbusres.2012.01.006

Hartono, E., Holsapple, C. W., Kim, K. Y., Na, K. S., & Simpson, J. T. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision Support Systems, 62*, 11-21. doi:10.1016/j.dss.2014.02.006

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 1-13. doi:10.1186/1869-0238-4-5

Hayajneh, T., Mohd, B. J., Itradat, A., & Quttoum, A. (2013). Performance and information security evaluation with firewalls. *International Journal of Security and Its Applications, 7*(6), 355-372. doi:10.14257/ijsia.2013.7.6.36

Hayat, M. J. (2013). Understanding sample size determination in nursing research. *Western Journal of Nursing Research, 35*, 943-956. doi:10.1177/0193945913482052

Heracleous, L., & Lan, L. L. (2012). Agency theory, institutional sensitivity, and inductive reasoning: Towards a legal perspective. *Journal of Management Studies, 49*, 223-239. doi:10.1111/j.1467-6486.2011.01009.x

Herath, H. S., & Herath, T. C. (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems, 57*, 54-63. doi:10.1016/j.dss.2013.07.010

Hitchcock, J. H., Onwuegbuzie, A. J., & Khoshaim, H. B. (2015). Examining the consequential validity of standardized examinations via public perceptions: A review of mixed methods survey design considerations. *International Journal of Multiple Research Approaches, 9*, 24-39. doi:10.1080/18340806.2015.1076757

Hilb, M. (2012). *New corporate governance: Successful board management tools*. New York, NY: Springer Science & Business Media.

Hilt, E. (2014). History of American corporate governance: Law, institutions, and politics. *Annual Review of Financial Economics, 6*(1), 1-21. doi:10.1146/annurev-financial-110613-034509

Hodgkinson, I. R., Ravishankar, M. N., & Aitken-Fischer, M. (2014). A resource-advantage perspective on the orchestration of ambidexterity. *The Service Industries Journal, 34*, 1234-1252. doi:10.1080/02642069.2014.942655

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*, 20-40. doi:10.1080/01639625.2013.822209

Homsud, S., & Chaveesuk, S. (2014). Understanding a proposed model of customer loyalty formation in B2C e-commerce. *International Journal of Future Computer*

and Communication, 3, 191-196. doi:10.7763/IJFCC.2014.V3.294

Htay, S. N. N., Salman, S. A., & Meera, A. K. M. (2013). Let's move to "universal corporate governance theory". *Journal of Internet Banking and Commerce, 18*(2), 1-11. Retrieved from http://www.alliedacademies.org

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*, 615-660. doi:10.1111/j.1540-5915.2012.00361.x

Hughes, D., Bon, J., & Rapp, A. (2013). Gaining and leveraging customer-based competitive intelligence: The pivotal role of social capital and salesperson adaptive selling skills. *Journal of the Academy Of Marketing Science, 41*, 91-110. doi:10.1007/s11747-012-0311-8

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*, 69-79. doi:10.1016/j.im.2013.10.001

Imenda, S. (2014). Is there a conceptual difference between theoretical and conceptual frameworks? *Journal of Social Sciences, 38*, 185-195. Retrieved from http://www.krepublishers.com

Information Technology Governance Institute. (2008). *Information security governance: Guidance for information security managers*. Rolling Meadows, IL: Author.

Jaferian, P., Hawkey, K., Sotirakopoulos, A., Velez-Rojas, M., & Beznosov, K. (2014). Heuristics for evaluating IT security management tools. *Human–Computer*

Interaction, 29, 311-350. doi:10.1080/07370024.2013.819198

Jaffe, R., & Cowell, J. M. (2014). Approaches for improving literature review methods. *The Journal of School Nursing, 30*, 236-239. doi:10.1177/1059840514540427

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security, 20*, 332-349. doi:10.1108/09685221211286511

Julisch, K. (2013a). Understanding and overcoming cyber security anti-patterns. *Computer Networks, 57*, 2206-2211. doi:10.1016/j.comnet.2012.11.023

Julisch, K. (2013b). Leading information security. *ISACA Journal, 6*, 27-30. Retrieved from http://www.isaca.org

Kaganer, E., Carmel, E., Hirschheim, R., & Olsen, T. (2013). Managing the human cloud. *MIT Sloan Management Review, 54*(2), 23-32. Retrieved from http://sloanreview.mit.edu

Kalloniatis, C., Mouratidis, H., & Islam, S. (2013). Evaluating cloud deployments scenarios based on security and privacy requirements. *Requirements Engineering, 18*, 299-319. doi:10.1007/s00766-013-0166-7

Kamisan, P. A., & King, B. E. M. (2013). Transactional and transformational leadership: A comparative study of the difference between Tony Fernandes (Airasia) and Idris Jala (Malaysia Airlines) leadership styles from 2005-2009. *International Journal of Business & Management*, *8*(24), 107-116. doi:10.5539/ijbm.v8n24p107

Kapooria, P., Sharma, R., & Kaul, D. (2014). Compliance of corporate governance and

its impact on firm performance: An empirical analysis with dummy variables. *International Journal of Research in Commerce, IT & Management,* 4, 9-12. Retrieved from http://ijrcm.org.in

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. *Information & Computer Security, 23*, 246-285. doi:10.1108/ICS-05-2014-0033

Kasum, A. S., & Etudaiye-Muthar, O. F. (2014). Corporate governance breach: An overview of the owner-manager agency problem in the Nigerian banking industry. In S. O. Idowu and K. T. Çaliyurt (Eds.), *Corporate Governance* (pp. 187-196). Heidelberg, Germany: Springer-Verlag.

Kearney, W. D., & Kruger, H. A. (2013). A framework for good corporate governance and organisational learning–an empirical study. *International Journal of Cyber-Security and Digital Forensics, 2*, 36-47. Retrieved from http://sdiwc.net

Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. *Computers, 3*, 1-35. doi:10.3390/computers3010001

Khan, S. N. (2014). Qualitative research method - phenomenology. *Asian Social Science, 10*(21), 298-310. doi:10.5539/ass.v10n21p298

Kim, A. C., Lee, S. M., & Lee, D. H. (2012). Compliance risk assessment measures of financial information security using system dynamics. *International Journal of Security and Its Applications, 6*(4), 191-200. Retrieved from http://www.sersc.org

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal, 2014*,

463870. doi:10.1155/2014/463870

King, D. B., O'Rourke, N., & DeLongis, A. (2014). Social media recruitment and online data collection: A beginner's guide and best practices for accessing low-prevalence and hard-to-reach populations. *Canadian Psychology, 55*, 240-249. doi:10.1037/a0038087

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security, 33*, 3-11. doi:10.1016/j.cose.2012.07.001

Konieczny, F., Trias, E., & Taylor, N. J. (2015). SEADE: Countering the futility of network security. *Air & Space Power Journal, 29*(5), 4-14. Retrieved from http://www.airpower.maxwell.af.mil

Kozlenkova, I. V., Samaha, S. A., & Palmatier, R. W. (2014). Resource-based theory in marketing. *Journal of the Academy of Marketing Science, 42*, 1-21. doi:10.1007/s11747-013-0336-7

Kram, K. E., Wasserman, I. C., & Yip, J. (2012). Metaphors of identity and professional practice: Learning from the scholar–practitioner. *The Journal of Applied Behavioral Science, 48*, 304-341. doi:10.1177/0021886312439097

Kumar, S., Himes, K. J., & Kritzer, C. P. (2014). Risk assessment and operational approaches to managing risk in global supply chains. *Journal of Manufacturing Technology Management, 25*, 873-890. doi:10.1108/JMTM-04-2012-0044

Kushwaha, P. (2016). Amalgamation of the information security management system with business - paradigm shift. *International Journal of Computer Science and Information Security, 14*(1), 105-111. Retrieved from

https://sites.google.com/site/ijcsis

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems, 27*(1), 219-236. doi:10.2308/isys-50339

L'Huillier, B. M. (2014). What does "corporate governance" actually mean? *Corporate Governance, 14*, 300-319. doi:10.1108/CG-10-2012-0073

Lambert, S. C., & Davidson, R. A. (2013). Applications of the business model in studies of enterprise success, innovation and classification: An analysis of empirical research from 1996 to 2010. *European Management Journal,* 31, 668-681. doi:10.1016/j.emj.2012.07.007

Lanz, J. (2014). Cybersecurity governance: The role of the audit committee and the CPA. *The CPA Journal*, *84*(11), 6-10. Retrieved from https://www.nysscpa.org

Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the Internet. *Information Systems Frontiers, 14*, 375-393. doi:10.1007/s10796-010-9253-1

Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *IEEE Security & Privacy, 11*(1), 78-81. doi:10.1109/MSP.2013.15

Liang-Chuan, W., & Liang-Hong, W. (2015). Improving the global supply chain through service engineering: A services science, management, and engineering-based framework. *Asia Pacific Management Review, 20*, 24-31. doi:10.1016/j.apmrv.2014.12.002

Lin, M., Lucas Jr, H. C., & Shmueli, G. (2013). Research commentary-too big to fail:

Large samples and the p-value problem. *Information Systems Research, 24*, 906-917. doi:10.1287/isre.2013.0480

Liu, H., Ke, W., Wei, K. K., & Hua, Z. (2013). The impact of IT capabilities on firm performance: The mediating roles of absorptive capacity and supply chain agility. *Decision Support Systems, 54*, 1452-1462. doi:10.1016/j.dss.2012.12.016

Lopez, R. H. (2012). *Information data security specialists' and business leaders' experiences regarding communication challenges*. Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3503982)

Looy, A. V., De Backer, M., Poels, G., & Snoeck, M. (2013). Choosing the right business process maturity model. *Information & Management, 50*, 466-488. doi:10.1016/j.im.2013.06.002

Ludin, I. H. B. H., & Cheng, B. L. (2014). Factors influencing customer satisfaction and e-loyalty: Online shopping environment among the young adults. *Management Dynamics in the Knowledge Economy, 2*, 462-471. Retrieved from http://www.managementdynamics.ro

Lunde, Å., Heggen, K., & Strand, R. (2013). Knowledge and power exploring unproductive interplay between quantitative and qualitative researchers. *Journal of Mixed Methods Research, 7*(2), 197-210. doi:10.1177/1558689812471087

Magdaraog-Jr, G. A. (2014). Warning signs in the workplace: An analysis of risk factors in employee fraud. *The Carrington Rand Journal of Social Sciences, 1*(1), 73-82. Retrieved from http://www.carringtonrand.com

Manzouri, M., Rahman, M. N. A., Nasimi, F., & Arshad, H. (2013). A model for securing

sharing information across the supply chain. *American Journal of Applied Sciences, 10*(3), 253-258. doi:10.3844/ajassp.2013.253.258

Markus, M. L., & Loebbecke, C. (2013). Commoditized digital processes and business community platforms: New opportunities and challenges for digital business strategies. *MIS Quarterly, 37*, 649-654. Retrieved from http://www.misq.org

Masa'deh, R. (2013). The impact of information technology infrastructure flexibility on firm performance: An empirical study of Jordanian public shareholding firms. *Jordan Journal of Business Administration, 9*, 204-224. doi:10.12816/0002054

Masa'deh, R., Maqableh, M., & Karajeh, H. (2014). A theoretical perspective on the relationship between leadership development, knowledge management capability, and firm performance. *Asian Social Science, 10*(6), 128-137. doi:10.5539/ass.v10n6p128

Mayoh, J., & Onwuegbuzie, A. J. (2015). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research, 9*, 91-107. doi:10.1177/1558689813505358

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion, 30*, 537-542. doi:10.1177/0267659114559116

McKim, C. A. (2015). The value of mixed methods research: A mixed methods study. *Journal of Mixed Methods Research, 9*, 1-21. doi:10.1177/1558689815607096

Meng, G., Liu, Y., Zhang, J., Pokluda, A., & Boutaba, R. (2015). Collaborative security: A survey and taxonomy. *ACM Computing Surveys, 48*, 1-42.

doi:10.1145/2785733

Miles, S. (2012). Stakeholders: Especially contested or just confused? *Journal of Business Ethics, 108*, 285-298. doi:10.1007/s10551-011-1090-8

Misangyi, V. F., & Acharya, A. G. (2014). Substitutes or complements? A configurational examination of corporate governance mechanisms. *Academy of Management Journal, 57*(6), 1681-1705. doi:10.5465/amj.2012.0728

Mishra, S., & Mohanty, P. (2014). Corporate governance as a value driver for firm performance: Evidence from India. *Corporate Governance, 14*, 265-280. doi:10.1108/CG-12-2012-0089

Mohare, R., & Lanjewar, U. (2012). Determinants of business information security. *International Journal of Marketing and Technology, 2*(7), 203-209. Retrieved from http://www.ijmra.us

Murray, J. (2013). Likert data: What to use, parametric or non-parametric? *International Journal of Business and Social Science, 4*(11), 258-264. Retrieved from http://ijbssnet.com

Nalband, N. A., & Kelabi, S. L. (2014). Redesigning Carroll's CSR pyramid model. *Journal of Advanced Management Science, 2*, 236–239. doi:10.12720/joams.2.3.236-239

Nathans, L. L., Oswald, F. L., & Nimon, K. (2012). Interpreting multiple linear regression: A guidebook of variable importance. *Practical Assessment, Research & Evaluation, 17*(9), 1-19. doi:10.3102/00346543074004525

National Commission for the Protection of Human Subjects of Biomedical and

Behavioral Research. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research*. Retrieved from http://hhs.gov/ohrp/humansubjects/guidance/belmont.html

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management, 52*, 123-134. doi:10.1016/j.im.2014.10.009

Neubert, M., Wu, C., & Roberts, J. (2013). The influence of ethical leadership and regulatory focus on employee outcomes. *Business Ethics Quarterly, 23*, 269-296. doi:10.5840/beq201323217

Nosek, B. A., Sriram, N., & Umansky, E. (2012). Presenting survey items one at a time compared to all at once decreases missing data without sacrificing validity in research with internet volunteers. *PLoS One, 7*(5), e36771. doi:10.1371/journal.pone.0036771

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *SAGE Open, 5*, e2158244015580372. doi:10.1177/2158244015580372

Pagani, M. (2013). Digital business strategy and value creation: Framing the dynamic cycle of control points. *MIS Quarterly, 37*, 617-632. Retrieved from http://www.misq.org

Pallant, J. (2010). *SPSS survivor manual* (4th ed.). Berkshire. England: McGraw-Hill.

Pan, G., Pan, S-L., & Lim, C-Y. (2015). Examining how firms leverage IT to achieve firm productivity: RBV and dynamic capabilities perspectives. *Information &*

Management, 52, 401-412. doi:10.1016/j.im.2015.01.001

Pande, S., & Ansari, V. A. (2014). A theoretical framework for corporate governance. *Indian Journal of Corporate Governance, 7*(1), 56-72. Retrieved from http://ijc.sagepub.com

Parylo, O. (2012). Qualitative, quantitative, or mixed methods: An analysis of research design in articles on principal professional development (1998–2008). *International Journal of Multiple Research Approaches, 6*, 297-313. doi:10.5172/mra.2012.6.3.297

Pautasso, M. (2013). Ten simple rules for writing a literature review. *PLoS Computational Biology, 9*(7), e1003149. doi:10.1371/journal.pcbi.1003149

Pérez-Méndez, J. A., & Machado-Cabezas, Á. (2015). Relationship between management information systems and corporate performance. *Spanish Accounting Review, 18*, 32-43. doi:10.1016/j.rcsar.2014.02.001

Pfaff, O., & Ries, S. (2014). Integrating enterprise security infrastructure with cloud computing. *Journal of Internet Technology and Secured Transactions, 3*, 338-343. Retrieved from http://www.infonomics-society.org

Pitesa, M., & Thau, S. (2013). Masters of the universe: How power and accountability influence self-serving decisions under moral hazard. *Journal of Applied Psychology, 98*, 550-558. doi:10.1037/a0031697

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders.

Information & Management, 51, 551-567. doi:10.1016/j.im.2014.03.009

Price, J. D. (2014). *Reducing the risk of a data breach using effective compliance programs*. Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3619214)

Priyadarshi, G. (2013). Leveraging and securing the bring your own device and technology approach. *ISACA Journal, 4*, 47-51. Retrieved from http://www.isaca.org

Raelin, J. D., & Bondy, K. (2013). Putting the good back in good corporate governance: The presence and problems of double-layered agency theory. *Corporate Governance: An International Review, 21*, 420-435. doi:10.1111/corg.12038

Rai, R., Sahoo, G., & Mehfuz, S. (2015). Exploring the factors influencing the cloud computing adoption: A systematic study on cloud migration. *SpringerPlus,* 4, 197-208. doi:10.1186/s40064-015-0962-2

Rao, U. K. (2012). Concepts in sample size determination. *Indian Journal of Dental Research, 23*, 660-664. doi:10.4103/0970-9290.107385

Rasheed, S., ChangFeng, W., & Yaqub, F. (2015). Towards program risk management and perceived risk management barriers. *International Journal of Hybrid Information Technology, 8*, 323-338. doi:10.14257/ijhit.2015.8.5.35

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58*, 44-57. doi:10.1016/j.infsof.2014.10.003

Renders, A., & Gaeremynck, A. (2012). Corporate governance, principal-principal agency conflicts, and firm value in European listed companies. *Corporate Governance: An International Review, 20*(2), 125-143. doi:10.1111/j.1467-8683.2011.00900.x

Rijke, J., Herk, S. V., Zevenbergen, C., Ashley, R., Hertogh, M., & Heuvelhof, E. T. (2014). Adaptive programme management through a balanced performance/strategy oriented focus. *International Journal of Project Management, 32*, 1197-1209. doi:10.1016/j.ijproman.2014.01.003

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*, 25-41. doi:10.1080/14780887.2013.801543

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies, 11*, 74-104. doi:10.1111/jels.12035

Ross, A., & Onwuegbuzie, A. J. (2014). Complexity of quantitative analyses used in mixed research articles published in a flagship mathematics education journal. *International Journal of Multiple Research Approaches, 8*, 63-73. doi:10.5172/mra.2014.8.1.63

Roster, C. A., Albaum, G., & Smith, S. M. (2014). Topic sensitivity and Internet survey design: A cross-cultural/national study. *Journal of Marketing Theory and Practice, 22*, 91-102. doi:10.2753/MTP1069-6679220106

Roy, O., & Pacuit, E. (2013). Substantive assumptions in interaction: A logical perspective. *Synthese, 190*(5), 891-908. doi:10.1007/s11229-012-0191-y

Rubino, M., & Vitolla, F. (2014). Corporate governance and the information system: How a framework for IT governance supports ERM. *Corporate Governance: The International Journal of Business in Society*, *14*, 320-338. doi:10.1108/CG-06-2013-0067

Saber, Z., Bahraami, H. R., & Haery, F. A. (2014). Analysis of the impact of supply chain management techniques: A competitive advantage in the market. *International Journal of Academic Research in Economics and Management Sciences, 3*(1), 75- 88. doi:10.6007/IJAREMS/v3-i1/579

Sachdeva, G. (2014). Corporate governance, concepts and practices: A survey. *The International Journal of Business & Management, 2*(2), 51-60. Retrieved from http://www.sobiad.org

Safa, N. S., & Ismail, M. A. (2013). A customer loyalty formation model in electronic commerce. *Economic Modelling, 35*, 559-564. doi:10.1016/j.econmod.2013.08.011

Safa, N. S., & Solms, R. V. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. doi:10.1016/j.chb.2015.12.037

Safa, N. S., Solms, R. V., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82. doi:10.1016/j.cose.2015.10.006

Safa, N. S., Sookhak, M., Solms, R. V., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations.

Computers & Security, 53, 65-78. doi:10.1016/j.cose.2015.05.012

Salibian-Barrera, M., Aelst, S. V., & Yohai, V. J. (2016). Robust tests for linear regression models based on τ-estimates. *Computational Statistics and Data Analysis, 93*, 436-455. doi:10.1016/j.csda.2014.09.012

Samanthula, B. K., Elmehdwi, Y., Howser, G., & Madria, S. (2015). A secure data sharing and query processing framework via federation of cloud computing. *Information Systems, 48*, 196-212. doi:10.1016/j.is.2013.08.004

Scharff, R. (2013). Being Post-Positivist . . . or just talking about it? *Foundations of Science, 18*(2), 393-397. doi:10.1007/s10699-011-9249-4

Schobel, K., & Denford, J. S. (2013). The chief information officer and chief financial officer dyad in the public sector: How an effective relationship impacts individual effectiveness and strategic alignment. *Journal of Information Systems, 27*(1), 261-281. doi:10.2308/isys-50321

Schryen, G. (2013). Revisiting IS business value research: What we already know, what we still need to know, and how we can get there. *European Journal of Information Systems, 22*(2), 139-169. doi:10.1057/ejis.2012.45

Seddon, P. B. (2014). Implications for strategic IS research of the resource-based theory of the firm: a reflection. *The Journal of Strategic Information Systems, 23*, 257-269. doi:10.1016/j.jsis.2014.11.001

Seferiadis, A. A., Cummings, S., Zweekhorst, M. B., & Bunders, J. F. (2015). Producing social capital as a development strategy: Implications at the micro-level. *Progress in Development Studies, 15*, 170-185. doi:10.1177/1464993414565530

Sekaran, U. (2003). *Research method for business: A skill building approach* (4th ed.). New York, NY: John Wiley & Sons.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*, 314-341. doi:10.1080/07421222.2015.1063315

Shaaban, H., & Conrad, M. (2013). Democracy, culture and information security: A case study in Zanzibar. *Information Management & Computer Security, 21*, 191-201. doi:10.1108/IMCS-09-2012-0057

Shaffer, J. P., Kowalchuk, R. K., & Keselman, H. J. (2013). Error, power, and cluster separation rates of pairwise multiple testing procedures. *Psychological Methods, 18*, 352-367. doi:10.1037/a0032478

Sharma, J. P., & Khanna, S. (2014). Corporate social responsibility, corporate governance and sustainability: Synergies and inter-relationships. *Indian Journal of Corporate Governance, 7*(1), 14-38. Retrieved from http://ijc.sagepub.com

Sheikhpour, R., & Modiri, N. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security and Its Applications, 6*(2), 13-28. Retrieved from http://www.sersc.org

Siagian, F., Siregar, S. V., & Rahadian, Y. (2013). Corporate governance, reporting quality, and firm value: Evidence from Indonesia. *Journal of Accounting in Emerging Economies, 3*, 4-20. doi:10.1108/20440831311287673

Siddiqui, N., & Fitzgerald, J. A. (2014). Elaborated integration of qualitative and quantitative perspectives in mixed methods research: A profound enquiry into the

nursing practice environment. *International Journal of Multiple Research Approaches, 8*, 137-147. doi:10.5172/mra.2014.8.2.137

Sila, I. (2013). Factors affecting the adoption of B2B e-commerce technologies. *Electronic Commerce Research, 13*, 199-236. doi:10.1007/s10660-013-9110-7

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security, 22*, 279-308. doi:10.1108/IMCS-05-2013-0041

Sindhuja, P. N. (2014). Impact of information security initiatives on supply chain performance: An empirical investigation. *Information Management & Computer Security, 22,* 450-473. doi:10.1108/IMCS-05-2013-0035

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management, 14*, 225-239. doi:10.1007/s40171-013-0047-4

Singh, S. (2015). Hello, limitations! The paradoxical power of limits in scientific writing. *Indian Journal of Dermatology, Venereology and Leprology, 81*(1), 4-6. doi:10.4103/0378-6323.148555

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*, 217-224. doi:10.1016/j.im.2013.08.006

Smith, T. T. (2016). *Examining Data Privacy Breaches in Healthcare*. Retrieved from ProQuest Dissertations & Theses Global. Retrieved from ProQuest Dissertations

& Theses Global. (Order No. 10144075)

Soava, G., & Raduteanu, M. (2014). Digital economy-economy of the new millennium. *Economics World, 2*, 45-57. Retrieved from http://www.davidpublisher.org

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security, 58*, 216-229. doi:10.1016/j.cose.2015.12.006

Srivastava, H., & Kumar, S. A. (2015). Control framework for secure cloud computing. *Journal of Information Security, 6*, 12-23. doi:10.4236/jis.2015.61002

Stagliano, A. J., & Sillup, G. P. (2014). Transparency and risk assessment reporting: A case study sector survey of cybercrime disclosures. *Journal of Business and Economics, 5*, 1134-1140. doi:10.15341/jbe(2155-7950)/07.05.2014/017

Stahl, B. C., Eden, G., Jirotka, M., & Coeckelbergh, M. (2014). From computer ethics to responsible research and innovation in ICT. The transition of reference discourses informing ethics-related research in information systems. *Information & Management, 51*, 810-818. doi:10.1016/j.im.2014.01.001

Stahl, B. C., Timmermans, J., & Flick, C. (2016). Ethics of emerging information and communication technologies: On the implementation of responsible research and innovation. *Science and Public Policy, 0*, 1-13. doi:10.1093/scipol/scw069

Starbuck, W. H. (2014). Why corporate governance deserves serious and creative thought. *Academy of Management Perspectives, 28*, 15-21. doi:10.5465/amp.2013.0109

Steiger, J. S., Hammou, K. A., & Galib, M. H. (2014). An examination of the influence of

organizational structure types and management levels on knowledge management practices in organizations. *International Journal of Business and Management, 9*(6), 43-57. doi:10.5539/ijbm.v9n6p43

Stewart, G., & Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security, 20*(1), 29-38. doi:10.1108/09685221211219182

Sun, Y., & Bhattacherjee, A. (2014). Looking inside the "IT Black Box": Technological effects on IT usage. *Journal of Computer Information Systems, 54*(2), 1-15. doi:10.1080/08874417.2014.11645681

Tabares, A., Alvarez, C., & Urbano, D. (2015). Born globals from the resource-based theory: A case study in Colombia. *Journal of Technology Management & Innovation,* 10(2), 155-165. doi:10.4067/S0718-27242015000200011

Tarafdar, M., D'Arcy, J., Turel, O., & Gupta, A. (2015). The dark side of information technology. *MIT Sloan Management Review, 56*(2), 61-70. Retrieved from http://sloanreview.mit.edu

Tashman, P., & Raelin, J. (2013). Who and what really matters to the firm: Moving stakeholder salience beyond managerial perceptions. *Business Ethics Quarterly, 23*, 591-616. doi:10.5840/beq201323441

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security, 2012*(2), 5-8. doi:10.1016/S1353-4858(12)70013-2

Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security, 2013*(4), 12-13. doi:10.1016/S1353-4858(13)70050-3

Too, E. G., & Weaver, P. (2014). The management of project management: A conceptual framework for project governance. *International Journal of Project Management, 32*, 1382-1394. doi:10.1016/j.ijproman.2013.07.006

Trautman, L. J., Triche, J., & Wetherbe, J. C. (2013). Corporate information technology governance under fire. *Journal of Strategic and International Studies, 8*(3), 105-114. Retrieved from http://www.isisworld.org

Trotter, R. T. (2012). Qualitative research sample design and sample size: Resolving and unresolved issues and inferential imperatives. *Preventive Medicine, 55*, 398-400. doi:10.1016/j.ypmed.2012.07.003

Tseng, C. Y., Wu, Z. J., & Lin, C. Y. (2013). Corporate governance and innovation ability: Empirical study of Taiwanese electronics manufactures. *International Business Research, 6*(7), 70-78. doi:10.5538/ibr.v6n7p70

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People, 25*, 327-352. doi:10.1108/09593841211254358

Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. *European Journal of Information Systems, 23*, 223-239. doi:10.1057/ejis.2012.61

Turner, T. L., Balmer, D. F., & Coverdale, J. H. (2013). Methodologies and study designs relevant to medical education research. *International Review of Psychiatry, 25*, 301-310. doi:10.3109/09540261.2013.790310

United States Securities and Exchange Commission. (2015). *Form 10-K: NCR Corporation*. Retrieved from https://www.sec.gov/archives

Uprichard, E. (2013). Sampling: Bridging probability and non-probability designs. *International Journal of Social Research Methodology, 16*, 1-11. doi:10.1080/13645579.2011.633391

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing, 24*(1), 21-41. doi:10.4018/joeuc.2012010102

Varsei, M., Soosay, C., Fahimnia, B., & Sarkis, J. (2014). Framing sustainability performance of supply chains with multidimensional indicators. *Supply Chain Management: An International Journal, 19*, 242-257. doi:10.1108/SCM-12-2013-0436

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly, 37*, 21-54. Retrieved from http://www.misq.org

Wahl, A., & Bull, G. Q. (2013). Mapping research topics and theories in private regulation for sustainability in global value chains. *Journal of Business Ethics, 124,* 585-608. doi:10.1007/s10551-013-1889-6

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research, 10*(1), 69-80. doi:10.2139/ssrn.2103082

Walden University. (2014). *DBA doctoral study rubric and research handbook*. Minneapolis, MN: Author.

Wang, C., Chow, S., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public

auditing for secure cloud storage. *IEEE Transactions on Computers (TC). 62*, 362-375. doi:10.1109/TC.2011.245

Wang, N., Liang, H., Zhong, W., Xue, Y., & Xiao, J. (2012). Resource structuring or capability building? An empirical study of the business value of information technology. *Journal of Management Information Systems, 29*(2), 325-367. doi:10.2753/MIS0742-1222290211

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013a). The association between the disclosure and the realization of information security risk factors. *Information Systems Research, 24*, 201-218. doi:10.1287/isre.1120.0437

Wang, T., Ulmer, J. R., & Kannan, K. (2013b). The textual contents of media reports of information security breaches and profitable short-term investment opportunities. *Journal of Organizational Computing and Electronic Commerce, 23*, 200-223. doi:10.1080/10919392.2013.807712

Wang, Z., Huang, J., & Tan, B. (2013). Managing organizational identity in the e-commerce industry: An ambidexterity perspective. *Information & Management, 50*, 673-683. doi:10.1016/j.im.2013.05.002

Ward, M. K., & Pond, S. B. (2015). Using virtual presence and survey instructions to minimize careless responding on Internet-based surveys. *Computers in Human Behavior, 48*, 554-568. doi:10.1016/j.chb.2015.01.070

Watfa, M., Khan, S., & Radmehr, A. (2014). Implications of SSO solutions on cloud applications. *Communications and Networks, 6*, 186-190. doi:10.4236/cn.2014.63020

Weigold, A., Weigold, I. K., & Russell, E. J. (2013). Examination of the equivalence of self-report survey-based paper-and-pencil and Internet data collection methods. *Psychological Methods, 18*, 53-73. doi:10.1037/a0031607

Welford, C., Murphy, K., & Casey, D. (2012). Demystifying nursing research terminology: Part 2. *Nurse Researcher, 19*(2), 29-35. doi:10.7748/nr2012.01.19.2.29.c8906

Wester, K. L., Borders, L. D., Boul, S., & Horton, E. (2013). Research quality: Critique of quantitative articles in the Journal of Counseling & Development. *Journal of Counseling & Development, 91*, 280-290. doi:10.1002/j.1556-676.2013.00096.x

Whitman, M. E., & Mattord, H. J. (2012). Information security governance for the non-security business executive. *Journal of Executive Education, 11*, 97-111. Retrieved from http://digitalcommons.kennesaw.edu

Wiedermann, W., & Eye, A. V. (2015). Direction of effects in multiple linear regression models. *Multivariate Behavioral Research, 50*, 23-40. doi:10.1080/00273171.2014.958429

Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets, 23*, 341-354. doi:10.1007/s12525-013-0137-3

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*, 1-20. Retrieved from http://www.misq.org

Wiseman, R. M., Cuevas-Rodríguez, G., & Gomez-Mejia, L. R. (2012). Towards a social theory of agency. *Journal of Management Studies, 49*, 202-222. doi:10.1111/j.1467-6486.2011.01016.x

Wlosinski, L. G. (2016). Mobile computing device threats, vulnerabilities and risk factors are ubiquitous. *ISACA Journal, 4*, 45-49. Retrieved from http://www.isaca.org

Wu, S. P. J., Straub, D. W., & Liang, T. P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. *MIS Quarterly, 39*, 497-518. Retrieved from http://www.misq.org

Yaokumah, W. (2013). *Evaluating the effectiveness of information security governance practices in developing nations: A case of Ghana*. Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3557634)

Yaokumah, W. (2014). Information security governance implementation within Ghanaian industry sectors: An empirical study. *Information Management & Computer Security, 22*, 235-250. doi:10.1108/IMCS-06-2013-0044

Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Business Systems, Governance & Ethics, 9*(2), 50-65. doi:10.15209/jbsge.v9i2.718

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*, 311-325. doi:10.1111/ejed.12014

Zachariadis, M., Scott, S., & Barrett, M. (2013). Methodological implications of critical realism for mixed-methods research. *MIS Quarterly, 37*, 855-879. Retrieved from http://www.misq.org

Zainodin, H., & Yap, S. (2013). Overcoming multicollinearity in multiple regression using correlation coefficient. *AIP Conference Proceedings,* 1557, 416-419. doi:101063/1.4823947

Zhan, G. (2013). Statistical power in international business research: Study levels and data types. *International Business Review, 22*, 678-686. doi:10.1016/j.ibusrev.2012.10.004

Zhao, H., Peng, Z., & Sheard, G. (2013). Workplace ostracism and hospitality employees' counterproductive work behaviors: The joint moderating effects of proactive personality and political skill. *International Journal of Hospitality Management, 33*, *33*219-227. doi:10.1016/j.ijhm.2012.08.006

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems, 30*(1), 123-152. doi:10.2753/MIS0742-1222300104

Zyxware Technologies. (2016). *List of Fortune 500 companies and their websites (2015)* [Data file]. Retrieved from http://www.zyxware.com

Appendix A: Copyright Permission E-mails

E-mail Request 1

From: Dr Winfred Yaokumah <XXXXX>
To: Robert Davis <XXXXX>
Date: Mon, May 16, 2016 at 6:28 AM
Subject: Re: Permission to Use Dissertation Research
Mailed-by: gmail.com
Signed-by: gmail.com

Dear Robert,
Find the permission attached.
--
Winfred Yaokumah (PhD)
Pentecost University College (Ag Dean, Faculty of Science, Engineering and Computing)

From: Robert Davis <XXXXX>
To: Dr Winfred Yaokumah <XXXXX>,
"Brown, Steven" <XXXXX>
Bcc: Alexandre Lazo <XXXXX>
Date: Sun, May 15, 2016 at 1:57 PM
Subject: Permission to Use Dissertation Research
Mailed-by: waldenu.edu

Dear Dr. Yaokumah and Dr. Brown:

I am completing a doctoral study at Walden University, entitled "Corporate Information Security Governance within the United States." Dr. Lazo is supervising my doctoral study. I would like your permission to modify "Figure 1: Mapping Corporate Governance Theories to ISG Domain Areas" in my doctoral study from the following quantitative cross-sectional survey research that examines the relationship between information security/business strategic alignment and information security governance (ISG) domain areas:

Yaokumah, W., & Brown, S. (2015). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Business Systems, Governance & Ethics, 9*(2), 50-65. doi:10.15209/jbsge.v9i2.718

The figure change will encompass the linkages from corporate governance domains to ISG domains. The requested permission extends to any future revisions and editions of my dissertation by ProQuest Information and Learning (ProQuest) through its UMI® Dissertation Publishing business. ProQuest may produce and sell copies of my

dissertation on demand and will make my dissertation available for free Internet download through the Open Access publishing method required by California State University, Long Beach. These rights will in no way restrict republication of the material in any other form by you or by others authorized by you. Your signing of this letter will also confirm that you own (or your company owns) the copyright to the above-described material.

If these arrangements meet with your approval, please electronically sign this letter where indicated below and return it to me. Thank you very much.

Sincerely,
Robert E. Davis, MBA, CISA, CICA

PERMISSION GRANTED FOR THE USE REQUESTED ABOVE:

_____
Dr. Winfred Yaokumah

_____
Dr. Steven Brown

E-mail Request 2

From: Robert E. Davis MBA CISA CICA <XXXXX>
Reply-to: "Robert E. Davis MBA CISA CICA" <XXXXX>
To: Robert Davis <XXXXX>
Date: Thu, Jul 7, 2016 at 6:17 PM
Subject: Re: Permission to Use Book Research
Mailed-by: yahoo.com
Signed-by: yahoo.com

On Thursday, July 7, 2016 6:15 PM, Robert Davis <XXXXX> wrote:

Dear Mr. Robert E. Davis:

I am completing a doctoral study at Walden University, entitled "Corporate Information Security Governance within the United States." Dr. Lazo is supervising my doctoral study. I would like your permission to modify "Figure 2.1 Governance Alignments" in my doctoral study from the following qualitative research that examines auditing information assets protection:

Davis, R. E. (2008). *IT auditing: Assuring information assets protection* [CD-ROM version]. Mission Viejo, CA: Pleier.

The figure change will encompass renaming a node from entity governance to corporate governance. The requested permission extends to any future revisions and editions of my dissertation by ProQuest Information and Learning (ProQuest) through its UMI® Dissertation Publishing business. ProQuest may produce and sell copies of my dissertation on demand and will make my dissertation available for free Internet download through the Open Access publishing method required by California State University, Long Beach. These rights will in no way restrict republication of the material in any other form by you or by others authorized by you. Your signing of this letter will also confirm that you own (or your company owns) the copyright to the above-described material.

If these arrangements meet with your approval, please electronically sign this letter where indicated below and return it to me. Thank you very much.

Sincerely,
Robert E. Davis, MBA, CISA, CICA

PERMISSION GRANTED FOR THE USE REQUESTED ABOVE:

Robert E. Davis

Appendix B: Calculations for Sample Size Determination

Equation 1: Sample size determination formula:

$n_o = (t)^2 \times (s)^2/(d)^2$

t is the selected alpha level value = 1.96

s is the estimate of standard deviation in the population = 1.25

d is the acceptable margin of error for estimated mean = .15

$n_o = (1.96)^2 \times (1.25)^2/(.15)^2 = 267$

Equation 2: Required return sample size when the sample size is greater than 5% of the population:

$n_1 = n_o/(1 + ((n_o - 1)/ \text{Population}))$

$n_o = 267$

Population = 1500

$n_1 = 267/(1 + ((267 - 1)/1500)) = 227$

Equation 3: Survey oversample adjustment:

n_2 = Sample size/Estimated nonresponse rate

Sample size = 227

Estimated nonresponse rate = .50

$n_2 = 227/.5 = 454$

Appendix C: Target Population Stratification

Stratified Sample Frame Industry Types by Business Sectors

Business Sector Type	Industry Type
Aerospace & Defense (1 industry)	Aerospace and Defense
Apparel (1 industry)	Apparel
Business Services (6 industries)	Advertising, marketing; Temporary Help, Diversified Outsourcing Services, Waste Management, Financial Data Services, Miscellaneous
Chemicals (1 industry)	Chemicals
Energy (5 industries)	Energy, Mining, Crude-Oil Production; Oil and Gas Equipment, Services; Petroleum Refining, Pipelines, Utilities
Engineering & Construction (2 industries)	Engineering, Construction; Homebuilders
Financials (4 industries)	Commercial Banks, Diversified Financials, Insurance, Real Estate, Securities
Food & Drugs (1 industry)	Food and Drug Stores
Food, Beverages, & Tobacco (4 industries)	Beverages, Food Consumer Products, Food Production, Tobacco
Healthcare (5 industries)	Insurance and Managed Care, Pharmaceuticals, Pharmacy and Other Services, Medical Facilities, Medical Products and Equipment, Wholesalers
Hotels, Restaurants, & Leisure (2 industries)	Food Services, Hotels, Casinos, Resorts
Household Products (4 industries)	Home Equipment, Furnishings; Household and Personal Products, Toys, Sporting Goods; Miscellaneous

(table continues)

Business Sector Type	Industry Type
Industrials (3 industries)	Construction and Farm Machinery, Electronics, Electrical Equipment; Industrial Machinery
Materials (4 industries)	Building Materials, Glass; Forest and Paper Products; Metals, Packaging, Containers; Miscellaneous
Media (2 industries)	Entertainment, Publishing, Printing
Motor Vehicles & Parts (1 industry)	Motor Vehicles and Parts
Retailing (3 industries)	Automotive Retailing, Services; General Merchandisers, Specialty Retailers
Technology (8 industries)	Computers, Office Equipment; Computer Peripherals, Computer Software, Information Technology Services, Internet Services and Retailing, Network and Other Communications Equipment, Scientific, Photographic and Control Equipment; Semiconductors and Other Electronic Components
Telecommunications (1 industry)	Telecommunications
Transportation (4 industries)	Airlines, Mail, Package, and Freight Delivery; Transportation and Logistics, Trucking, Truck Leasing
Wholesale (4 industries)	Diversified, Electronics and Office Equipment, Food and Grocery, Health Care

Appendix D: Data Collection Instrument

Table 11

General Information

Code	Items	Frequency	Percentage
CGI1	What is the corporation's industry sector?		
	Aerospace & Defense	4	4.20
	Apparel	2	2.10
	Business Services	4	4.20
	Chemicals	5	5.30
	Energy	8	8.40
	Engineering & Construction	0	0.00
	Financials	13	13.70
	Food and Drugs	1	1.10
	Food, Beverages, & Tobacco	5	5.30
	Healthcare	4	4.20
	Hotels, Restaurants, & Leisure	5	5.30
	Household Products	3	3.20
	Industrials	3	3.20
	Materials	6	6.30
	Media	5	5.30
	Motor Vehicles & Parts	3	3.20
	Retailing	6	6.30
	Technology	4	4.20
	Telecommunications	4	4.20
	Transportation	7	7.40
	Wholesale	3	3.20
CGI2	What is your job title/function?		
	Chief executive officer	0	0.00
	Chief information officer	2	2.10
	Chief operations officer	0	0.00
	Chief information security officer	10	10.50
	Chief audit executive	5	5.30
	Chief finance officer	4	4.20
	Other: _____	74	77.90

(table continues)

Code	Items	Frequency	Percentage
CGI3	What is your work experience level?		
	1 -5 years	7	7.40
	6 – 10 years	10	10.50
	11 – 15 years	22	23.20
	16 – 20 years	29	30.50
	Over 20 years	27	28.40

Table 12

Effectual ISG Measures

		Frequency						
Code	Items	SD	D	NS	A	SA	*M*	*SD*
CES1	On the board's agenda risk and audit committees are actively engaged. IT executives are most often engaged by the board not only when a major incident occurs.	14	19	20	24	18	3.14	1.34
CES2	Security actions in my organization are not done in an ad hoc manner, but are based on a comprehensive risk assessment and established risk tolerances.	20	16	14	28	17	3.06	1.43
CES3	Security is managed by a cross organizational team. Security is not viewed as a tactical IT concern but involves business leaders.	17	15	28	16	19	3.05	1.36
CES4	Digital assets are inventoried and categorized with assigned owners.	12	19	17	22	25	3.31	1.38
CES5	Security policy is actively monitored and enforced and leaders are held accountable.	18	16	19	22	20	3.11	1.42
CES6	Security program is regularly reviewed, audited, and subject to continuous improvement.	12	11	18	18	36	3.58	1.42

Table 13

Strategic Alignment Measures

Code	Items	Frequency					*M*	*SD*
		NI	PS	PI	CC	FI		
CSA1	Information security strategy considers the input from the stakeholders.	20	12	27	17	19	3.03	1.40
CSA2	Information security strategy provides a clear statement of how security supports enterprise mission.	16	14	21	22	22	3.21	1.40
CSA3	The information security governance program seeks to achieve the information security strategy.	21	20	12	24	18	2.98	1.46
CSA4	Training and awareness programs are provided for enhancing information security acceptance.	19	23	23	16	14	3.67	1.11
CSA5	Information security investment is allocated efficiently on the basis of quantitative analysis.	28	15	18	22	12	2.74	1.42
CSA6	All organizational intellectual property is accounted for and protected.	22	20	14	14	25	3.00	1.54
CSA7	Long term information security planning supports the organization's mission and long-term strategy by minimizing losses, protecting brand and competitive advantage.	15	26	16	27	15	3.09	1.29
CSA8	Short term planning supports organization's objectives and strategy by controlling project risks and managing vulnerabilities.	17	21	27	13	17	2.92	1.34
CSA9	Ultimate responsibility for the state of enterprise information security lies with executive management.	11	26	22	12	24	3.13	1.37
CSA10	Security is incorporated into the project development process.	24	16	17	20	18	2.92	1.47
CSA11	Information security policies and standards are applicable to executive management.	13	20	15	23	24	3.26	1.40

(table continues)

Code	Items	Frequency NI	PS	PI	CC	FI	*M*	*SD*
CSA12	Legal, Audit or Risk department is supported by the Information Security Team in determining appropriate information security implications of regulations.	13	11	22	25	24	3.38	1.35
CSA13	Metrics are developed and used for validation of security compliance requirements.	16	11	26	25	17	3.17	1.33

Table 14

Value Delivery Measures

Code	Items	Frequency NI	PS	PI	CC	FI	*M*	*SD*
CVD1	When policies are updated or new policies are developed, is an analysis conducted to determine the financial and resource implications of implementing the new policy?	16	16	31	14	18	3.02	1.33
CVD2	Do your security policies effectively address the risks identified in your risk analysis/risk assessments?	19	20	25	15	16	2.88	1.36
CVD3	Are relevant security policies included in all of your third-party contracts?	16	17	24	22	16	3.05	1.33
CVD4	Are consequences for non-compliance with corporate policies clearly communicated and enforced?	16	20	19	19	21	3.09	1.41
CVD5	Are information security issues considered in all the important business decisions within the company (product development, vendor selection, purchasing, etc.)?	20	20	24	12	19	2.89	1.41

Table 15

Risk Management Measures

Code	Items	Frequency					*M*	*SD*
		NI	PS	PI	CC	FI		
CRK1	Does your organization have a documented information security and privacy program?	16	17	22	20	20	3.12	1.38
CRK2	Has your organization conducted a risk assessment within the last two years to identify the key objectives that need to be supported by your information security and privacy program?	15	13	22	20	25	3.28	1.40
CRK3	Has your organization identified critical assets and the business functions that rely on them?	23	22	25	9	16	2.72	1.38
CRK4	Have the information security threats and vulnerabilities associated with each of the critical assets and functions been identified?	13	22	23	18	19	3.08	1.33
CRK5	Has a cost been assigned to the loss of each critical asset or function?	17	19	22	24	13	2.97	1.32
CRK6	Does your organization have a written information security strategy that seeks to cost-effectively measure risk and specify actions to manage risk at an acceptable level, with minimal business disruptions?	19	13	19	22	22	3.16	1.45
CRK7	Does your organization have a written information security strategy including plans that seek to cost effectively reduce the risks to an acceptable level, with minimal business disruptions?	19	12	20	21	23	3.18	1.45
CRK8	Is the strategy reviewed and updated at least annually or more frequently when significant business changes require it?	14	13	19	26	23	3.33	1.37
CRK9	Does your organization have a process in place to monitor state legislation or regulations and determine their applicability to your organization?	25	24	12	17	17	2.76	1.47

Table 16

Performance Measurement Measures

Code	Items	Frequency					*M*	*SD*
		NI	PS	PI	CC	FI		
CPM1	Does your organization periodically test and evaluate/audit your information security program, practices, controls, and techniques to ensure they are effectively implemented?	18	16	15	26	20	3.15	1.43
CPM2	Does your organization conduct a periodic independent evaluation/audit of your information security program and practices for each business unit?	16	17	24	14	24	3.14	1.42
CPM3	Does each periodic independent evaluation/audit test the effectiveness of information security policies, procedures, and practices of a representative subset of each business unit's information systems?	20	15	16	22	22	3.12	1.47
CPM4	Does each periodic independent evaluation/audit assess the compliance of each business unit with the requirements of a standard information security framework and related information security policies, standards, procedures, and guidelines?	24	21	19	18	13	2.74	1.39

Table 17

Resource Management Measures

Code	Items	Frequency					*M*	*SD*
		NI	PS	PI	CC	FI		
CRM1	Is there a person in your organization that has information security as primary duty, with responsibility for maintaining the security program and ensuring compliance?	10	29	19	14	23	3.12	1.36
CRM2	Do the leaders and staff of your information security organization have the necessary experience and qualifications? (e.g. CISSP, CISM, CISA certification)	17	17	26	15	20	3.04	1.38
CRM3	Does your information security function have the authority and resources it needs to manage and ensure compliance with the information security program?	17	20	29	10	19	2.94	1.36
CRM4	Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes, and audits?	15	23	15	22	20	3.09	1.40
CRM5	Has specific responsibility been assigned for the execution of business continuity and disaster recovery plans (either within or outside of the Information Security Department)?	21	18	16	19	21	3.01	1.48
CRM6	Do you have an ongoing training program in place for information security staff?	9	17	33	15	21	3.23	1.25
CRM7	Is someone in the information security department responsible for liaising with business units to identify any new security requirements based on changes in the business?	21	19	12	21	22	3.04	1.50

(table continues)

Code	Items	Frequency NI	PS	PI	CC	FI	*M*	*SD*
CRM8	Does the information security function actively engage with other critical functions, such as Human Resources and Legal, to develop and enforce compliance with information security policies and practices?	19	19	16	18	23	3.07	1.47
CRM9	Does the information security department report regularly to the executive staff and Board of Directors on the compliance of the business and the effectiveness of the information security program and policies?	20	18	16	21	20	3.03	1.45
CRM10	Is the executive staff ultimately responsible and accountable for the information security program, including approval of information security policies?	14	19	26	13	23	3.13	1.38
CRM11	Do the business unit heads and senior managers have specific programs in place to comply with information security policies and standards with the goal of ensuring the security of the information and systems that support the operations and assets under their control?	13	22	24	19	17	3.05	1.31
CRM12	Has your organization implemented an information security education and awareness program such that all employees, contractors, and external providers know the information security policies that apply to them and understand their responsibilities?	18	17	20	22	18	3.05	1.39
CRM13	Does your organization have official information security architecture, based on your risk management analysis and information security strategy?	10	11	35	13	26	3.36	1.29
CRM14	Is the security architecture updated periodically to take into account new business needs and strategies as well as changing security threats?	20	19	22	19	15	2.89	1.37

(table continues)

Code	Items	Frequency NI	PS	PI	CC	FI	*M*	*SD*
CRM15	As the architecture evolves, is there a process to review existing systems and applications for compliance and for addressing cases of non-compliance?	15	19	22	18	21	3.12	1.38
CRM16	Has your organization instituted processes and procedures for involving the security personnel in evaluating and addressing any security impacts before the purchase or introduction of new systems?	22	21	19	14	19	2.86	1.45
CRM17	If a deployed system is found to be in noncompliance with your official architecture, is there a process and defined time frame to bring it into compliance or to remove it from service, applications, or business processes?	19	18	22	15	21	3.01	1.43
CRM18	Does your organization have a process to appropriately evaluate and classify the information and information assets that support the operations and assets under your control, to indicate the appropriate levels of information security?	19	18	17	17	24	3.09	1.48
CRM19	Are there specific, documented, security-related configuration settings for all systems and applications?	22	16	26	19	12	2.82	1.34