A Causal-Comparative Study on Information Technology (IT) Control Material Weaknesses and the Financial Performance of U.S. Corporations

Dissertation Manuscript

Submitted to Northcentral University

Graduate Faculty of the School of Business and Technology Management in

Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPHY

By

Daniel A. Sherwood

La Jolla, California

December 2019

Approval Page

Causal-Comparative Study on Information Technology (IT) Control Material Weaknesses and the Financial Performance of U.S. Corporations

By

Daniel A. Sherwood

Approved by the Doctoral Committee:

DocuSigned by: Mary Dereshiwsky 9F015187E50440D...	PhD, MS	12/19/2019 | 16:49:14 MST
Dissertation Chair: Mary Dereshiwsky	Degree Held	Date
DocuSigned by: Khaled Ghany 6445764E8881416...	PhD, CPA	12/19/2019 | 11:00:36 MST
Committee Member: Khaled Ghany	Degree Held	Date
DocuSigned by: Leila Sopko 1F89B29081C9435...	Ph.D., MBA	12/19/2019 | 10:36:39 MST
Committee Member: Leila Sopko	Degree Held	Date

Abstract

The Sarbanes-Oxley (SOX) Act of 2002 was created in response to the number of corporate scandals and significantly impacted how businesses report financial statements. Section 404 of the SOX Act of 2002 establishes the requirement for public corporations to disclose an assessment of their internal control material weaknesses. This research addresses the problem that there is a need to understand the differences in the possible effects of various types of IT control weaknesses on the financial performance of publicly traded U.S. corporations. The purpose of this quantitative causal-comparative research study was to identify the differences that may exist in the effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses. The theoretical framework of this study includes the convergence of IT Governance Theory, Accounting Theory, Audit Theory, and Internal Control Theory. The research questions are developed to inquire about the difference in the level of financial performance using Tobin's Q and Open Market Value (OMV) between public businesses that experience various types of IT control material weaknesses and public businesses that do not experience IT control material weaknesses. A non-random quota sampling method is used to select a minimum sample size of 46 from the target population using matched-pair *t*-tests to statistical measure the differences between the mean of Group 1 (μ_1) with the mean of Group 2 (μ_2). This research is not intended to recreate prior studies reflecting the holistic negative impact of IT controls material weaknesses on the financial performance of public businesses. Instead, this research focused on measuring the extent of the negative impacts that individual types of IT control material weaknesses may have on the financial performance of public businesses. The results of this research have the potential to drastically change how stakeholders perceive and react to IT control material weaknesses that are reported by public businesses.

Keywords: information technology (IT) control material weaknesses, internal controls, financial performance, public businesses, Sarbanes-Oxley (SOX) Act of 2002, risk management, enterprise risk management (ERM), IT governance, accounting, auditing, COSO, COBIT, enterprise resource planning (ERP), Tobin's Q, Open Market Value (OMV)

Acknowledgments

I would like to thank our Lord and Savior, Jesus Christ for His many blessings and ultimate sacrifice. I thank my father, mother, and sisters for the many wonderful memories. I thank my wife, Shana, and my children for their continued loving support. There have been many along my academic journey that have given me encouragement and motivation. I sincerely thank all of you.

I would like to acknowledge Dr. Matthew W. Sherwood, Ph.D. Since our childhood, you have always been a spiritual leader to me and a source of faithful inspiration. You were crucial in my developed understanding of how someone like me could overcome great obstacles (Philippians 4:13) and I thank you.

I thank Northcentral University for their continued service and dedication in providing me with the opportunity to achieve my educational goals. I would also like to thank my Dissertation Chair Dr. Mary Dereshiwsky Ph.D., for your continued guidance, mentorship, and words of encouragement. I also thank my Subject Matter Expert (SME) Dr. Khaled Abdel Ghany Ph.D., Academic Reader Dr. Leila Sopko Ph.D., and Dr. John Kuhn Jr. Ph.D. for their support and guidance throughout the program.

Lastly, I want to dedicate this achievement to my mother, Melida C. Sherwood (1954-2007), born and raised in a grass hut in the Federated States of Micronesia. She migrated to the United States with less than a sixth-grade education. In my first semester, she spent the majority of her life savings in cash to ensure her son would at least get a start at a college education. I pray that you look down from heaven and are pleased with your investment, and with all my heart I thank you, I love you, and I miss you.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

The Sarbanes-Oxley (SOX) Act of 2002 drastically changed the way businesses operate in the United States (U.S.). Under Section 404 of SOX, public businesses are now required to provide an assessment of their internal controls during financial reporting (Erickson, Lukes, & Weber, 2014). The change in regulation significantly impacted the strategic approach used by many businesses to ensure a sufficient level of internal controls (internal controls) exists within their business processes and financial procedures (Deng, Xiao, & Zhou, 2017). Many companies have continued to invest large amounts of time and resources in implementing Enterprise Resource Planning (ERP) in order to improve IT governance, competitive position, and overall performance (Deng et al., 2017). A benefit to using ERP is the ability to comply with the strict internal controls guidelines of Section 404 of SOX through the application of the Control Objectives for Information and Related Technology (COBIT) (Rubino & Vitolla, 2014). The COBIT is a fundamental framework for IT controls which assist businesses with achieving government compliance, mitigating risk, and improving performance (Rubino & Vitolla, 2014).

The enactment of SOX, specifically Section 404 of SOX, has changed the way corporations, investors, and auditors have defined internal controls (Jahmani et al., 2014). The requirement for corporations to report internal controls material weaknesses within their financial reports has provided new areas that need exploration and further research (Jahmani et al., 2014). The intent of conducting this study was to fill the existing gaps in internal controls literature and IT governance literature through gaining a deeper understanding of the differences in the possible effects of various types of IT control weaknesses on the financial performance of U.S. publicly traded corporations. The focus of this quantitative study was to provide empirical measurements that display the extent of the differences between various types of IT control weaknesses and the financial performance of the corporations that have reported them to the Securities Exchange Commission (SEC). This research will provide businesses, investors, accounting professionals, government officials, and educators with a better understanding of the differences in the effects of various types of IT controls weaknesses on the financial performance of public businesses in the U.S (Kinkela & Harris, 2013).

Background

Sarbanes-Oxley (SOX) Act of 2002. The government's implementation of the SOX Act of 2002 emphasized internal controls and the reporting of more thorough financial disclosures by corporations. These changes were meant to reinstall confidence in the American public and investors about the accuracy and reliability of financial reports (Clements, Neill, & Wertheim, 2015). Internal controls encompass the processes and procedures that ensure compliance with generally accepted accounting principles (GAAP), enable corporate governance, and mitigate risks (Jahmani & Dowling, 2015). IT controls are the subset of internal controls that assist businesses with improving IT governance. Businesses that fail to maintain the integrity of IT controls must disclose this information within the annual financial reports of a business entity as IT control weaknesses.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework was created in 1992 and updated in 2013 (Jahmani, Ansari, & Dowling, 2014). COSO has become the generally accepted framework for implementing internal controls for many corporations (Rubino & Vitolla, 2014). Many U.S. public companies have adopted the COSO framework even though it is not a requirement of the Public Company Accounting Oversight Board (PCAOB) (Rubino & Vitolla, 2014). Companies that have registered with the SEC have recognized the effectiveness of the COSO framework in meeting the standards of SOX Section 404 (Kinkela & Harris, 2013). COSO classifies internal controls into five categories: the control environment, risk assessment, control activities, information/communication, and monitoring activities (Rubino & Vitolla, 2014). The COSO framework is useful in assisting businesses with improving governance over processes and internal controls for financial reporting (Jahmani et al., 2014).

2013 COSO Updates. The 2013 updates to the COSO framework primarily assist management and the board of directors with improving IT governance (Kinkela & Harris, 2013). These changes enabled the internal control process to be implemented universally by different entities and at all levels and functions (Kinkela & Harris, 2013). Many public companies use the 2013 updates to the COSO framework, which has shown to be effective in today's markets (Samithisomboon & Chantatub, 2016). The changes in the COSO framework were intended to improve compliance and quality of reporting through aligning with current business practices and modern technology (Kimbell, 2017).

Control Objectives for Information and Related Technology (COBIT). The initial COBIT framework was created in 1996 by the Information System Audit and Control Association (ISACA). COBIT was designed to assist organizations with more efficiently managing their IT (Samithisomboon & Chantatub, 2016). An advantage of the COBIT framework is the ability to assist managers with balancing expected benefits and risks, meanwhile supplementing the COSO framework (Samithisomboon & Chantatub, 2016). The progression of the COBIT framework has been from COBIT 1 to COBIT5, which begins with a primary focus as an audit tool and progresses to controls, management, IT governance, and the governance of enterprise/information systems (Rubino & Vitolla, 2014). The increased reliance on IT and the use of ERP have added significant value to the application of the COBIT framework (Rubino & Vitolla, 2014).

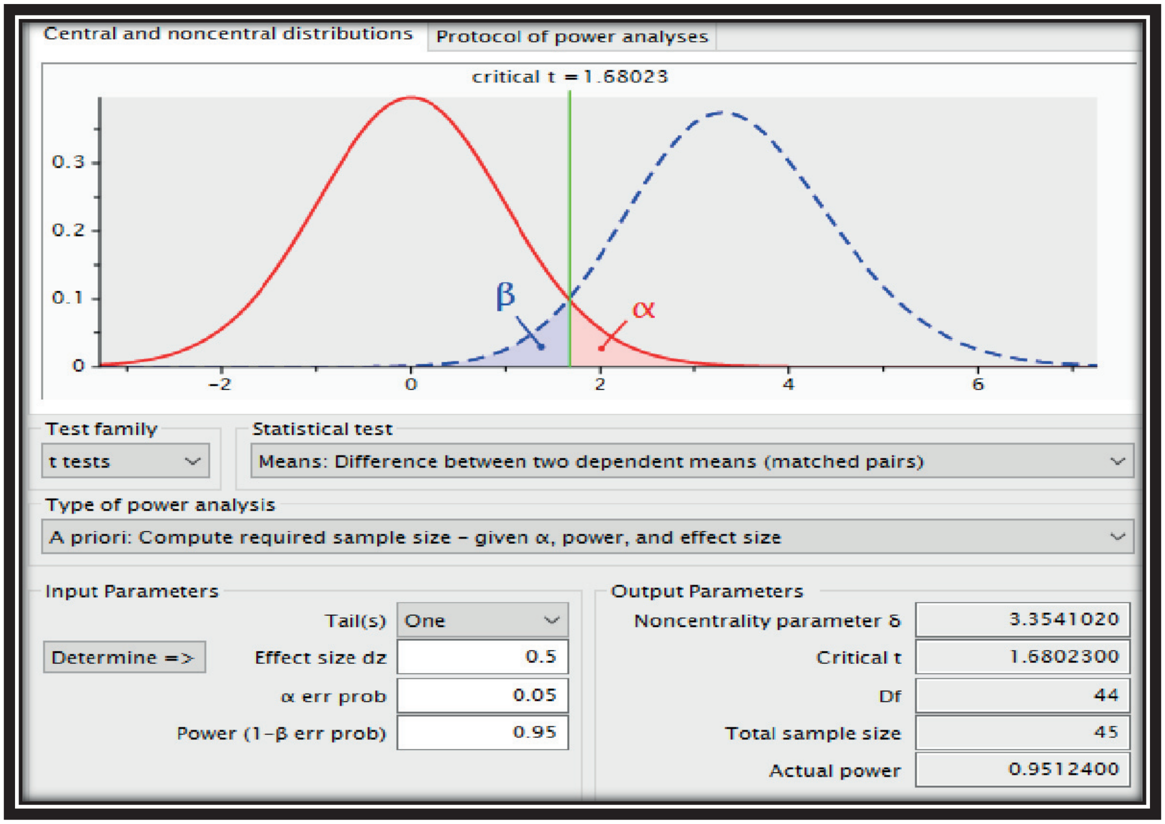
Enterprise Resource Planning (ERP). ERP is a business software tool that has gained in popularity and use since the 1990s (Lipaj & Davidaviciene, 2013). ERP has dramatically impacted the way that organizations operate in today's complex business environment. Globalization, advancements in IT, and new developments in accounting software continue to shape how businesses conduct daily operations, both domestically and internationally (Grabski, Leech, & Schmidt, 2011). A common objective of many organizations is to improve performance and IT governance with technologies such as ERP (Kimbell, 2017). The increased complexity in business arrangements, globalization, and advancements in ERP software continues to impact the types of internal controls weaknesses that are reported by businesses (Miller, Bunn, & Noe, 2016). The world is becoming more interconnected as ERP software continues to evolve (Lipaj & Davidaviciene, 2013). Nations around the world are now aware of the socio-economic relationship created from having closely interconnected global markets and the increased reliance on IT (Grabski et al., 2011). In the United States, government officials recognized the need for businesses to ensure they equip themselves with adequate internal controls to protect investors and the economy (Kimbell, 2017). The implementation of government regulations, such as the Sarbanes-Oxley Act of 2002, has added pressure to businesses to improve IT governance and report internal controls material weaknesses (Gray & Ehoff, 2015). In response, the majority of public businesses have reinforced their organizational objectives to improve audibility and performance through the use of ERP, the COSO framework, and the Control Objectives for Information and Related Technology (COBIT) (Kimbell, 2017; Miller et al., 2016; Rubino & Vitolla, 2014).

Statement of the Problem

The intent of conducting this research was to address the need to understand further the differences in the possible effects of various types of IT control weaknesses on the financial performance of publicly traded U.S. corporations. Companies are required per government regulation to report material internal controls weaknesses on their annual financial statements. There is little research that explains the extent to which various types of IT control weaknesses negatively impact the financial performance of public firms in the United States. In general, internal controls weaknesses can have devastating effects on the effectiveness and efficiency of businesses. Stakeholders must understand the risks that are involved with their investments. Internal and external stakeholders greatly benefit from knowing what types of internal controls weaknesses are impacting their investments along with knowing the extent of each of those impacts. SOX Section 404 was implemented to improve the reliability of financial reports and protect investors (Erickson et al., 2014). Businesses have reported many different types of internal controls material weaknesses since the establishment of the SOX Act of 2002. There are two major categories of internal controls weaknesses. The first is IT control weaknesses and the second is Non-IT control weaknesses (Kuhn, Ahuja, & Mueller, 2013). Corporations can be negatively impacted depending on the type of material internal controls weakness they incur. Also, the type of internal controls weakness that businesses report may drastically impact the perspective and confidence of investors (Erickson et al., 2014). There is much research within the literature of internal controls which describes the effects of Non-IT vs. IT Weaknesses and the different types of Non-IT weaknesses, but there is little research which explains the effects of different types of IT control material weaknesses on the financial performance of publicly traded corporations (Erickson et al., 2014). Research is needed to gain a better understanding of the effects of various types of IT control weaknesses.

Purpose of the Study

The purpose of this quantitative study was to identify the differences that possibly exist in the effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses. The basis for conducting this research stems from the research conducted by Kuhn et al. (2013), which shows that companies who report both materials IT and Non-IT control weaknesses experience lower levels of financial performance. Also, a foundation for this study extends to the research of Ragothaman & Cornelsen (2017), which uses a sample of 395 companies to show that internal control material weaknesses and gross margin have a negative relationship. These previous studies have both shown evidence of an existing negative relationship between IT control weaknesses and the financial performance of corporations. The proposed study is intended to contribute to the literature through gaining a deeper understanding of the differences in the effects between the independent variables of various types of reported IT control weaknesses and the operational efficiency and effectiveness of corporations using Tobin's Q (Ragothaman & Cornelsen, 2017). The dependent variables used in this study include Tobin's Q or Q-ratio, which is a measure of a firm's financial performance along with the measurement of firm valuation through the analysis of Open Market Value (OMV) (Ragothaman & Cornelsen, 2017; Rognlie, 2015). The calculation for Tobin's Q is a firm's market value of physical assets divided by the replacement cost of assets (Ragothaman & Cornelsen, 2017). The target population of this study includes all U.S. corporations that are required by Section 404 of the SOX Act of 2002 to disclose an assessment of all internal control weaknesses that are deemed material in nature (Erickson et al., 2014). This secondary archival data is available to the public and retrievable through the Electronic Data Gathering Analysis Retrieval System (EDGAR), an online database controlled by the SEC.


Central and noncentral distributions
Protocol of power analyses
critical t = 1.68023
0.3
0.2
0.1
0
−2
0
2
4
6
β
α
Determine =>

Test family: t tests

Statistical test: Means: Difference between two dependent means (matched pairs)

Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters		Output Parameters	
Tail(s)	One	Noncentrality parameter δ	3.3541020
Effect size dz	0.5	Critical t	1.6802300
α err prob	0.05	Df	44
Power (1−β err prob)	0.95	Total sample size	45
		Actual power	0.9512400

Figure 1. G*Power Analysis

The G*Power output in Graph 1 (Appendix A) provides a measurement of a sufficient total sample size required for this study. The statistical *t*-test would measure the differences between the means of two dependent groups (matched pairs). The statistical analysis would use an input parameter with an effect size (d) of .5, the α error probability of .05, β of .5, and Power (1- β error probability) of .95. A study based on a priori of the stated α, power, and effect size would require a minimum total sample size of 46 (i.e., 23 businesses that did not report an IT control material weakness matched with 23 comparable businesses that did report an IT control material weaknesses). The publicly traded U.S. businesses are matched based on the industry type and size of earnings. Quota sampling entails finding participants which can be described by a particular set of characteristics and are representative of a population. The ability to identify appropriate participants is based solely on convenience and the categorical application of definitive characteristics. The quota sampling method is used in this study to support the achievement of the stated purpose of measuring the differences in the possible effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses.

Theoretical Framework

Overview. Several theories contribute to the theoretical framework of this study. These theories include IT Governance Theory, Accounting Theory, Audit Theory, and Internal Control Theory and will be used to assist in closing the gap in internal controls and IT governance literature (Ragothaman & Cornelsen, 2017; Rubino & Vitolla, 2014; Weng et al., 2015). These theories are inter-connected through the concept of financial reporting, which is a governmental requirement of every public business. Corporations must overcome many obstacles in order to achieve an Unqualified Opinion from an external auditing entity (AICPA, n.d.). Businesses must account for financial transactions accurately, timely, and per government regulation (Baker & Burlaud, 2015). Also, businesses must have the ability to provide accurate and timely financial reports, which include an assessment of the firm's internal controls (Baranov, Shaposhnikov, Maksimova, & Fadeykina, 2017). Businesses must have the ability to maintain a sufficient level of control in order to operate effectively and efficiently (Weng et al., 2015).

IT Governance Theory. IT governance enables businesses to effectively align their organizational objectives with their IT strategies (Ragothaman & Cornelsen, 2017). Businesses that can effectively control their IT infrastructures can mitigate costs through increased operational efficiency and accountability (Ragothaman & Cornelsen, 2017). A common framework employed by many businesses to improve IT controls is the COBIT framework (Rubino & Vitolla, 2014). Businesses have used COBIT since the mid-1990s to improve IT governance. The increase in IT dependency, increase in ERP popularity and application, and the implementation of SOX has led to a greater need and application of IT governance frameworks such as COBIT (Rubino & Vitolla, 2014).

Accounting Theory. Accounting Theory follows a primary principle that financial information should be relevant, reliable, accurate, and timely (Baker & Burlaud, 2015). Many principles stated in accounting theory have been codified into what is known as GAAP (AICPA, n.d.). The components of accounting theory are assumptions, frameworks, and methodologies, which describe the approaches used by businesses to record and report financial transactions (Baker & Burlaud, 2015). Accounting Theory provides the foundation necessary to examine Audit Theory (Baker & Burlaud, 2015).

Audit Theory. Audit Theory states the purpose of an audit is to test the reliability of a business' financial information along with an examination of the policies, practices, and procedures of the business (Baranov et al., 2017). In the U.S., government regulation, such as the Securities Act of 1933 and the Securities Exchange Act of 1934, requires public companies to conduct annual external audits (Zogning, 2017). Recent legislation, such as the Sarbanes-Oxley Act of 2002, has provided further guidelines for conducting external audits and the approach that businesses should use to ensure they maintain a high standard of auditability (Chiu, Liu, & Vasarhelyi, 2014). A primary proposition of the Sarbanes-Oxley Act of 2002 is the requirement of internal controls (Chiu et al., 2014). According to the SEC, the use of ERP was deemed to be a viable instrument of internal controls that could be used by businesses to meet the requirements of section 404 of the Sarbanes-Oxley Act of 2002 (Zogning, 2017).

Internal Control Theory. Internal controls are a proponent of Control Theory, which is used to explain the processes within a system that isolate the number of outcomes when responding to a particular inducement (Wang, 2015). The application of internal controls in the field of accounting and auditing is based on the recognized need for businesses to operate at a maximum level of performance while remaining compliant with government laws and regulations (Ling, 2015). Compliance with the Sarbanes-Oxley Act of 2002 section 404 requires that business managers implement internal controls and ensure the segregation of duties to maintain a sufficient standard of governance (AICPA, n.d.). Many businesses have invested in ERP as a means of meeting the requirements of the Sarbanes-Oxley Act of 2002 (Zogning, 2017).

Theoretical Framework Summary. IT Governance Theory, Accounting Theory, Audit Theory, and Internal Control Theory are used to describe the fundamental practices and procedures used by businesses to produce financial statements (Ragothaman & Cornelsen, 2017; Rubino & Vitolla, 2014; Weng et al., 2015). The standard practices and procedures used by society to engage in accounting and auditing are continually changing (Baker & Burlaud, 2015). Businesses have turned to ERP as a means to improve their accounting practices, auditability, and strengthen internal controls (Kuo, 2014). Government regulations, such as SOX, also support the use of ERP to ensure compliance with sufficient levels of internal controls (Zogning, 2017). In order to more accurately gain an understand about the impacts of reported material internal controls weaknesses on the financial performance of public businesses it is vital to understand IT Governance Theory, Accounting Theory, Audit Theory, and Internal Control Theory as a theoretical framework (Ragothaman & Cornelsen, 2017; Rubino & Vitolla, 2014; Weng et al., 2015).

Nature of the Study

Technological and software advancements have contributed to the vast integration of ERP (Al-Sabaawi, 2015). ERP has become a commonly used solution for achieving the demands of more strict government regulations, improving IT governance, and improving corporate social responsibility (CSR) (Miller et al., 2016). Many business leaders and political leaders have made it a point to emphasize the importance of maintaining a high level of auditability in response to a substantial public outcry during the period of 1990-2010 (Richardson, Dellaportas, Perera, & Richardson, 2015). During this time, a large number of corporate scandals such as Enron, WorldCom, Tyco, and Waste Management were devastating markets and destroying families, communities, and the accounting profession around the world (Moore, 2018). The massive influx of corporate scandals led to increased public scrutiny and a greater need for further government regulation (Richardson et al., 2015). SOX Act of 2002 was intended to reinstall confidence in investors about the accuracy and reliability of the financial statements that were reported by corporations (Clements, Neill, & Wertheim, 2015).

The fundamental framework of this study was built on the research of Kuhn, Ahuja, & Mueller (2013), which states companies that report both material IT and Non-IT control weaknesses to experience lower levels of financial performance. A gap in both internal controls and IT governance literature exists between the impacts of different types of reported internal controls weaknesses on the financial performance of public U.S. firms. These variables have been identified within the theoretical framework of IT Governance Theory, Accounting Theory, Audit Theory, and Internal Control Theory (Ragothaman & Cornelsen, 2017; Rubino & Vitolla, 2014; Weng et al., 2015).

The research design for this study was selected in order to effectively analyze archival public data on U.S. publicly traded companies that are matched based on size and industry (Apuke, 2017). The focus of this study was to contribute to gaining a better understanding of the effects of IT control material weaknesses on the financial performance of the U.S. corporations that reported them on their annual 10-K reports (Kuhn et al., 2013). These disclosures have been required since the establishment of the SOX Act of 2002 (Jahmani et al., 2014). Public firms are required to provide an assessment of any material internal controls weakness that significantly increases the firm’s operational risk (Jahmani et al., 2014). Businesses continue to report many kinds of internal controls weaknesses. The COSO framework provides descriptions and methods of categorizing internal controls weaknesses (Rubino & Vitolla, 2014). The COSO framework uses five categories to identify material internal controls weaknesses. These five categories include the control environment, risk assessment, control activities, information/communication, and monitoring activities (Rubino & Vitolla, 2014). This framework is useful when analyzing both IT and Non-IT control weaknesses. A primary focus of this research is on IT control weakness and use the CORBIT 5 framework, which allows for the category of IT control weaknesses to be out into two groups: IT general controls and IT application controls (Rubino & Vitolla, 2014). The nature of this study was built upon the current literature and identified the effects of different types of IT control weaknesses that have been reported by public U.S. businesses.

Research Questions

The following research questions align with the hypotheses in the subsequent section. These research questions were designed to provoke inquiry into the actual effects of IT control weaknesses on the financial performance of public businesses. The hypotheses are designed to support the purpose of this study and provide statistical evidence required to answer each research question (Rubino & Vitolla, 2014).

Q1: What are the differences in financial performance between U.S. publicly traded businesses that report various types of IT control material weaknesses and U.S. publicly traded businesses that do not report IT control material weaknesses?

Q2: What are the differences in market valuation between U.S. publicly traded businesses that report various types of IT control material weaknesses and U.S. publicly traded businesses that do not report IT control material weaknesses?

Q3: What are the differences in financial performance between U.S. publicly traded business that resolved a various type of IT control material weakness in a given year and did not report any in the following year and U.S. publicly traded business that did not report an IT control material weakness in the same given year or the following year?

Hypotheses

H1: There is no significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded businesses that report various types of IT control material weaknesses (*x*) and U.S. publicly traded businesses that do not report IT control material weaknesses (*x*).

$H1_0$: $\mu_1 = \mu_2$

$H1_a$: There is a significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded businesses that report various types of IT control material weaknesses (*x*) and U.S. publicly traded businesses that do not report IT control material weaknesses (*x*).

$H1_a$: $\mu_1 \neq \mu_2$

H2: There is no significant difference in the Open Market Value (OMV) (*y*) between U.S. publicly traded businesses that report various types of IT control material weaknesses (*x*) and U.S. publicly traded businesses that do not report various types of IT control material weaknesses (*x*). **$H2_0$: $\mu_1 = \mu_2$**

$H2_a$: There is a significant difference in the Open Market Value (OMV) (*y*) between U.S. publicly traded businesses that report various types of IT control material weaknesses (*x*) and U.S. publicly traded businesses that do not report various types of IT control material weaknesses (*x*). **$H2_a$: $\mu_1 \neq \mu_2$**

H3: There is no significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded business that resolved a various type of IT control material weakness (*x*) in a given year (t) and did not report any in the following year (t+1) and U.S. publicly traded business that did not report a various type of IT control material weakness (*x*) in the same given year (t) or the following year (t+1). **$H3_0$: $\mu_1 = \mu_2$**

H3 $_a$: There is a significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded business that resolved a various type of IT control material weakness (*x*) in a given year (t) and did not report any in the following year (t+1) and U.S. publicly traded business that did not report a various type of IT control material weakness (*x*) in the same given year (t) or the following year (t+1). **$H3_0$: $\mu_1 \neq \mu_2$**

Significance of the Study

This study is an essential contribution to the fields of accounting, auditing, and IT governance. The use of IT and enterprise systems such as ERP has wholly taken over how organizations conduct business. The widespread use of IT has inevitably resulted in an increased dependency on IT among businesses (Grabski et al., 2011). Businesses rely heavily on the integrity of IT controls and the accuracy of financial data (Ragothaman & Cornelsen, 2017). Also, investors depend significantly on the assurance of financial statements and therefore have a deeply vested interest in the types of IT control weaknesses that are being reported by businesses (Rubino & Vitolla, 2014). Managers, investors, and accounting professionals benefit from the findings of this research through gaining a more precise definition of specific types of IT control weaknesses and the ability to understand better the extent of the impacts of IT control weaknesses on the financial performance of publicly-traded businesses (Rubino & Vitolla, 2014).

This research was necessary to gain a deeper understanding of the effects of IT control weaknesses on the financial performance of U.S. publicly traded businesses. The basis for this research was derived from previous studies found within the literature and went further to more clearly define individual types of IT control weaknesses and the extent of the negative impacts they may have on the financial performance of businesses. This study describes an examination of different types of IT material weaknesses that can derive from faults from either of the two main categories of IT controls (i.e., IT general controls and IT application controls) (Rubino & Vitolla, 2014). A goal of this research was to provide empirical evidence that identifies further detailed facts about internal controls weaknesses and answer the proposed research questions that have yet to be examined or described throughout internal controls or IT governance literature (Ragothaman & Cornelsen, 2017). The answers to the research questions proposed in this study will allow government officials, educators, business managers, investors, IT specialists, accounting professionals, ERP developers, and many other professionals to understand better the impact of IT control weaknesses on the financial performance of publicly traded U.S. businesses.

Definition of Key Terms

Accounting. Accounting is a business function of maintaining financial accounts, recording financial transactions, and reporting financial information (Baker & Burlaud, 2015). There are several fields of accounting, such as financial accounting, managerial accounting, taxation, and auditing.

Accounting Information System (AIS). An information system programmed and designed to collect, store, and recall the financial data of an organization (Miller et al., 2016).

Audit. An audit is an internal or external inspection of the financial accounts of an organization (Baranov et al., 2017). Publicly traded businesses in the U.S. are required to conduct an annual audit by an external, independent, and qualified Certified Public Accountant (CPA). An auditor must conduct this type of audit within accordance with government regulation (e.g., the Securities Acts of 1933, the Securities Acts of 1934, and the Sarbanes-Oxley Act of 2002) (Zogning, 2017).

Audit Finding. An audit finding is everything related to a statement of fact and takes the form of either conformity or non-conformity determination made as a result of analyzing the variance between the audit evidence and audit criteria (Agustiningsih, Murni, & Putri, 2017).

Auditability. Auditability is a fundamental element of the financial reporting of an organization that describes the ability of an organization to record and report financial transactions accurately, timely, and reliable (Johari & Hussin, 2016).

Auditor's Opinion. An auditor's opinion is ultimately a certification or attestation to the accuracy of a business' financial statements. Under GAAP, an auditor's opinion can come in the form of one of four various statements (e.g., unqualified, qualified, adverse, or disclaimer of opinion) (Tahinakis & Samarinas, 2016).

Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a five-component internal control framework that was created in 1992 and has been generally accepted by the Public Company Accounting Oversight Board (PCAOB) and the majority of U.S. corporations (Rubino & Vitolla, 2014).

Control Objectives for Information and Related Technology (COBIT). COBIT is a basic IT framework created in 1996 by the Information System Audit and Control Association (ISACA). COBIT is intended to assist organizations with more efficiently managing their IT domains and processes and aligning them with their objectives (Samithisomboon & Chantatub, 2016).

Enterprise Resource Planning (ERP). ERP is a web-based, real-time, business application with software capable of integrating the electronic data created from significant business processes of an organization. These business processes include functions such as accounting, human resources, purchasing, sales, customer service, manufacturing, and inventory (Debreceny, Gray, Joeson, Lee, & Woon-Foong, 2005).

Generally Accepted Accounting Principles (GAAP). GAAP is a list of business rules, standard practices, and procedures that the U.S. publicly traded companies must use when reporting their financials for public use (AICPA, n.d.).

Generally Accepted Auditing Standards (GAAS). GAAS is a list of codified auditing standards instituted by the Public Company Accounting Oversight Board (PCAOB) to measure audit quality and the level of objectivity that must be met during every external audit (PCAOB, n.d.).

Information Technology (IT). IT is a subset of information systems (IS) and encompasses the computer hardware, network, software, and databases used within a system to create, transfer, and store electronic data (Kloviene & Gimzauskiene, 2014).

Information Systems (IS). An IS encompasses an entire system of people, processes, and technology which creates, stores, manipulates, and transfers information (Miller et al., 2016).

Internal Controls. Internal controls are the rules and procedures set emplace to ensure the handling of financial and accounting information complies with GAAP (Kuo, 2014).

Information Technology (IT) Controls. IT controls are a subset of internal controls, and there are two major categories (i.e., general controls and application controls). These processes and procedures are intended to maintain the integrity and confidentiality of data and ensure the governance and management of IT (Rubino & Vitolla, 2014).

Open Market Value (OMV). The OMV or market value is the price of an asset in a fair and competitive marketplace. The formula for calculating the OMV is the product of the number of outstanding shares and the business' current share price (Rognlie, 2015).

Sarbanes-Oxley Act of 2002. The Sarbanes-Oxley Act of 2002 was legislation put in place in response to the number of corporate scandals that occurred during the turn of the century. Corporate scandals such as Tyco, WorldCom, and Enron became infamous for their unethical business practices (Gray & Ehoff, 2015). The Sarbanes-Oxley Act of 2002 established more strict auditing standards and included the requirement of internal controls, more detailed financial disclosures, and specific penalties for violations of accounting or auditing standards (Chiu et al., 2014).

Summary

Information about the effects of different types of IT control weaknesses on the financial performance of U.S. businesses is significant to businesses, investors, accountants, government organizations, and many others within the fields of IT and business. The corporate scandals of recent history have shown the negative results of businesses operating with internal controls weaknesses and displayed the devastating impacts they can have on markets and communities (Gray & Ehoff, 2015). These are a few reasons which make it more vital to conduct this study and better understand the effects of IT control weaknesses on the financial performance of publicly traded businesses in the U.S. The focus of this research is to identify different types of IT control weaknesses that are commonly reported by businesses on their 10K annual reports. A significant benefit to conducting this study was the ability to close the gap in internal controls and IT governance literature by applying the COBIT framework to better understand the impacts of various types of IT control material weaknesses (Rubino & Vitolla, 2014). The results of this study have the potential to drastically change how internal and external stakeholders interpret and react to IT control weaknesses that have been reported by businesses.

Chapter 2: Brief Review of IT Controls Literature

IT controls are the policies, processes, and procedures that provide reasonable assurance of data and contribute to organizations achieving their goals and objectives (Erickson et al., 2014). The passage of the Sarbanes-Oxley (SOX) Act of 2002 drastically changed the strategic approach used by businesses in the United States when attempting to engage in IT controls (Deis & Byus, 2016). Section 404 of the SOX Act of 2002 requires all SEC registrants such as public businesses to provide an assessment of any internal control material weaknesses to include an account for any IT control weaknesses that are deemed to be material in their annual financial reports (Deng et al., 2017). Many companies have continued to invest large amounts of time and resources in implementing ERP in order to improve IT governance, competitive positioning, and overall performance (Deng et al., 2017). The extensive use of ERP offers businesses the additional ability to comply with the strict internal controls guidelines of Section 404 of the SOX Act of 2002 through the application of the Control Objectives for Information and Related Technology (COBIT) (Deis & Byus, 2016; Rubino & Vitolla, 2014). A review of the current literature is necessary to conduct a quantitative study to identify the effects of different types of IT control weaknesses on the financial performance of publicly traded U.S. businesses. This literature review is intended to describe the theories and constructs associated with IT controls and to assist with researching the effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. corporations. The framework of this study builds on the research of Kuhn et al., (2013), whose study shows companies that report both material IT and Non-IT control weaknesses to reflect lower levels of financial performance.

Database & Source Information

The literature for this quantitative study was collected and reviewed from many databases and search engines in order to measure differences in the possible effects of various IT control weaknesses on the financial performance of U.S. publicly traded corporations. The databases employed to gather scholarly sources of information for this literature review included EBSCOhost Business Source Complete, ProQuest Central, Sage Journals, and EDGAR Database. These databases were accessed through the Northcentral University (NCU) library. The NCU library was used as the primary resource due to easy accessibility, and a large amount of comprehensive research material relevant to the research topic of IT control weaknesses. The use of keywords and phrases as single and combined search criteria included the following; IT controls, Internal Controls, IT control weaknesses, Internal Control Weaknesses, Sarbanes-Oxley Act of 2002, Information Technology, IT Governance, Corporate Governance, Control Environment, Internal Control Framework, COSO, COBIT, Risk Management, ERM, Enterprise Risk Management, ERP, Enterprise Resource Planning, Accounting Information System, AIS, IT Security, Corporate Fraud, Fraud Detection, Corporate Social Responsibility, CSR, AICPA, Accounting, and Auditing. The nature and scope of the sources used for this literature review were academic and professional. Additionally, these sources consisted of peer-reviewed articles and scholarly journals.

ANALYSIS OF SOURCES

Year of Publication	Count	Percentage of Sources
<2014	13	14%
No Date (n.d.)	6	7%
≥2014	73	79%
≥2014 + (n.d.)	**79**	**86%**
Total	92	100%

Table 1. Analysis of sources used for this study.

The publication dates for more than 85 percent of the sources referenced in this literature review were published within the past five years. Table 1 displays an analysis of the references used for this study. A total of 92 references were used with 79 of those sources comprised of scholarly sources that were published within the past five years or indicated to have no date (n.d.) of publication. There were 13 scholarly sources used in this research that were older than five years. These 13 sources were deemed relevant, unique, and pertinent to achieving the purpose of this research.

Theoretical Framework

IT Governance Theory, Accounting Theory, Audit Theory, and Internal Control Theory are used to describe the fundamental practices and procedures used by businesses to produce financial statements (Ragothaman & Cornelsen, 2017; Rubino & Vitolla, 2014; Weng et al., 2015). The standard practices and procedures used by society to engage in accounting and auditing are continually changing (Baker & Burlaud, 2015). Businesses have turned to ERP to improve their accounting practices, auditability, and strengthen internal controls (Kuo, 2014). Government regulations, such as SOX, also support the use of ERP to ensure compliance with sufficient levels of internal controls (Zogning, 2017). In order to more accurately gain an understand about the impacts of reported material internal controls weaknesses on the financial performance of public businesses it is essential to understand IT Governance Theory, Accounting Theory, Audit Theory, and Internal Control Theory as a theoretical framework (Ragothaman & Cornelsen, 2017; Rubino & Vitolla, 2014; Weng et al., 2015). The theoretical framework of IT controls encompasses several prominent and recurring theories and constructs. The framework of this literature review of IT controls includes the following sections; Twenty-One Types of IT Control Weaknesses, Background of the Sarbanes-Oxley (SOX) Act of 2002, Components of IT Controls, Internal Control Frameworks, Information Technology (IT), Enterprise Resource Planning (ERP), Corporate Governance, Risk Management, Enterprise Risk Management (ERM), Security, Ethics and Responsibility, and Accounting. These primary constructs have been identified through a holistic lens to make up the theoretical framework of IT controls literature. A description of each theory and construct is necessary to provide a systematic review of recent studies about IT controls and the surrounding topics. Businesses rely heavily on computer technology and IT systems to improve productivity and performance (Kuhn & Morris, 2017). Business' dependency on IT comes at a tremendous financial cost and requires significant upfront investments (Dogaru, 2015). This research was intended to assist with gaining a better understanding of the impact of IT control weaknesses on the financial performance of U.S. public businesses.

AuditAnalytics Typology of Internal Control Material Weaknesses

There are twenty-one categories of internal control material weaknesses that have been identified by Ives Group, Inc. providers of AuditAnalytics. AuditAnalytics is one of the leading sources of SOX Section 404 research and is vastly accepted throughout industries and academia (Kim, Richardson, & Watson, 2018). This section is used to define each of the twenty-one internal control weaknesses and identify the differences and interconnectivity that may or may not exist between each one. This study was intended to focus solely on furthering the academic understanding of the specific internal control weakness identified in this section as Internal Control - Information technology, software, security & access issues. IT is vital to the success of businesses in today's environment due to the high requirement for interconnectivity between large and complex business processes (Kuhn & Morris, 2017). The dependency between business processes and IT is one reason why it is essential to explore the occurrence of IT control weaknesses and understand how they impact businesses.

I. **Internal Control: Accounting Documentation, Policies, and Procedures.** When internal control systems do not have an adequate level of documentation, policies, or other justification for account balances, accounting documentation, policies, and procedures, internal control weakness has occurred. Internal control material weaknesses such as accounting documentation, policies, and procedures will often result in businesses failing to maintain financial records that align with the proper governing standard such as Staff Accounting Bulletin (SAB), GAAP, Financial Accounting Standards Board (FASB). Businesses with these types of issues will often find it difficult with the closing process of year-end and producing accurate and timely financial statements (AuditAnalytics, n.d.).

II. **Internal Control: Accounting Personnel Resources, Competency, and Training.** Any shortfalls that result in issues with the resources, competency, training, and experience of accounting personnel is considered to be an accounting personnel resource, competency/training internal control weakness. In order for this type of internal control weakness to be reported in a filing, management must have a documented remediation plan (AuditAnalytics, n.d.).

III. **Internal Control: Ethical or Compliance Issues with Personnel.** Ethical or compliance issues with personnel are internal control weaknesses that describe problems with an individual's ability or willingness to comply with policies or ethical standards. The individual has heightened risks of committing fraud or intentional acts that have led to could potentially lead to the misstatement of account balances or financial reports (AuditAnalytics, n.d.).

IV. **Internal Control: Inadequate Disclosure Controls (Timely, Accuracy, Completeness).** These types of internal control weaknesses are tied closely to many of the other internal controls that have been identified. Inadequate disclosure controls are related to the shortfalls in the quality of information that are required to meet the standard for properly disclosing financial statements (AuditAnalytics, n.d.).

V. **Internal Control: Ineffective Regulatory Compliance Issues.** Ineffective regulatory compliance issues are internal control weaknesses that result from the failures to meet any regulatory requirement except for tax code (AuditAnalytics, n.d.).

VI. **Internal Control: Ineffective, Non-existent, or Understaffed Audit Committee.** Internal control weaknesses surrounding the audit committee are defined by situations where an organization has failed to assemble an audit committee or assemble an audit committee with personnel with the experience, resources, or independence required to perform their duties to meet the standards required by legislation (AuditAnalytics, n.d.).

VII. **Internal Control: Information Technology, Software, Security & Access Issues.** IT control weaknesses are the primary focus of this study. These types of internal control weaknesses are a result of deficient program controls, software programs implementation issues, segregation of duties, compliance issues with systems accesses. Many examples find IT control weaknesses are simply a result of a failure to control authorized users, roles, and permissions within Enterprise Systems, AIS, and many other types of business information systems that are used throughout the industries (AuditAnalytics, n.d.).

VIII. **Internal Control: Insufficient or Non-existent Internal Audit Function.** These types of internal control weaknesses occur when a business fails to set up an internal audit department or has an internal audit department that cannot identify, advise, or take corrective action towards the occurrence of an internal control weakness (AuditAnalytics, n.d.).

IX. **Internal Control: Journal Entry Control Issues.** Journal entry control issues are a type of internal control weaknesses that describe deficiencies associated with the journal entry process. These types of internal control weaknesses arise from several issues associated with incorrect data entry, validation, workflow process, error identification, and error resolution (AuditAnalytics, n.d.).

X. **Internal Control: Management/Board/Audit Committee Investigation(s).** Management/Board/Audit Committee investigation(s) describes an internal control that involves various teams with a specific objective. The committees' objectives are commonly centralized around the review and development of internal control reports that pertain to accounting and financial reporting matters (AuditAnalytics, n.d.).

XI. **Internal Control: Material and Numerous Auditor Year-End Adjustments.** These types of internal controls are used to indicate potential material weaknesses that may exist based on the prima facie evidence of transactional errors found by the auditors. These errors and adjustments identified during year-end audits are often described in the footnotes of financial reports. The occurrence of several auditors initiated year-end adjustments are a crucial indicator of an existing material weakness (AuditAnalytics, n.d.).

XII. **Internal Control: Non-routine Transaction Control Issues.** This type of internal control weakness becomes a concern when a business reports internal control issues that are a result of non-routine transactions. Non-routine transactions can occur from several events such as contracts, asset sales, and the implementation of new systems (AuditAnalytics, n.d.).

XIII. **Internal Control: Restatement of Previous Section 404 Disclosures.** A restatement of prior section 404 related events that currently impact or could potentially impact a Registrants financials has the potential for the discovery of an internal control material weakness. Businesses will often have to restate their section 404 opinions commonly due to financial transactions that have occurred after they have filed their financial reports (AuditAnalytics, n.d.).

XIV. **Internal Control: Restatement or Non-reliance of Company Filings.** Restatement or non-reliance of company filings are prima facia evidence for the existence of internal control material weaknesses. This type of internal control consists of material weakness opinions about the original events that created the need for restatements (AuditAnalytics, n.d.).

XV. **Internal Control: SAB 108 Adjustments Noted.** These types of internal control material weaknesses are examined when the Internal Control over Financial Reporting (ICFR) disclosures identify a SAB No. 108 instead of a financial restatement. The beginning retained earnings balances associated with previous period accounting errors are corrected through a transactional adjustment (AuditAnalytics, n.d.).

XVI. **Internal Control: Scope (Disclaimer of Opinion) or Other Limitations.** This type of material weakness when the registrant fails to complete their review of their internal controls. The Registrant's internal controls are not able to be audited until the internal review and assessment are completed (AuditAnalytics, n.d.).

XVII. **Internal Control: SEC or Other Regulatory Investigations and Inquiries.** This type of internal control indicates there is an ongoing investigation into the affairs of the Registrant's accounting or financial reporting deficiencies. The investigation is commonly conducted by the SEC or another similar regulatory body. The registrant uses the 404 assertions to proclaim the SEC investigation or inquiry is underway (AuditAnalytics, n.d.).

XVIII. **Internal Control: Segregations of Duties - Design of Controls (Personnel).** This internal control describes the deficiencies that may exist with the design and structure of roles and permissions within an organization's informational, operational, and financial framework (AuditAnalytics, n.d.).

XIX. **Internal Control: Senior Management Competency, Tone, and Reliability Issues.** This internal control is used to address the negligent and improper actions at the senior management level of an organization (AuditAnalytics, n.d.).

XX. **Internal Control: Treasury Control Issues.** This internal control is established to address issues with treasury related activities and transactions such as cash disbursements (AuditAnalytics, n.d.).

XXI. **Internal Control: Untimely or Inadequate Account Reconciliations.** Untimely or inadequate account reconciliations is an internal control that is used to identify material weaknesses with financial reconciliations and the occurrence of repetitive transactional adjustments required by the auditor (AuditAnalytics, n.d.).

Background of Sarbanes-Oxley (SOX) Act of 2002

The SOX Act of 2002 was created in response to the number of corporate scandals that occurred during the turn of the century (Moore, 2018). New government regulation was in high demand in response to the way businesses were unethically reporting their finances. During the time just before the signing of the SOX Act of 2002, businesses and accounting firms would work together to fraudulently report financial figures filled with false accounts and fake revenue (Sorensen & Miller, 2017). Independent accounting firms, such as Arthur Anderson would fraudulently certify financial statements containing material misstatements (Sorensen & Miller, 2017). Once the business filed for bankruptcy, investors would be baffled about how the company's incredible gains turned out to be actual losses (Deis & Byus, 2016). These types of cases became a plague during this period, and the government had to react due to the vast public outcry (Chiu et al., 2014). A few famous corporate scandals such as Tyco, WorldCom, and Enron made the public aware of the unethical practices and the negative impact this type of behavior had on the economy (Kuhn & Morris, 2017; Chiu, Liu, & Vasarhelyi, 2014). These scandals destroyed the lives of employees, investors, and was extremely damaging to the profession of accounting (Chiu et al., 2014). The number and scope of these corporate scandals left a negative impression even on the world economy. The effects of these unethical practices reached into the period known as the Great Recession and are still felt even today (Deis & Byus, 2016). The enactment of the SOX Act of 2002 completely changed how public corporations operated (Deis & Byus, 2016). SOX impacted how businesses processed their financial transactions, controlled financial operations, and reported financial statements.

Section 404. Section 404 of the SOX Act of 2002 establishes the requirement for public corporations to disclose assessments of their internal control's weaknesses. The requirement for corporations to report internal controls material weaknesses within their financial reports has provided new areas that need exploration and further research (Jahmani et al., 2014). This study intends to fill the existing gaps in internal controls literature and IT governance literature through gaining a deeper understanding of the effects of different types of IT control weaknesses on the financial performance of U.S. publicly traded corporations. The focus of this quantitative study was to provide an empirical measurement that displays the extent of the differences in the effects of various types of IT control weaknesses and the financial performance of the corporations that have reported them to the SEC. This research will provide businesses, investors, accounting professionals, government officials, and educators with a better understanding of the differences between the effects of various types of IT controls material weaknesses on the financial performance of public businesses in the U.S (Kinkela & Harris, 2013).

Section 409. The purpose of Section 409 of the SOX Act of 2002 is to ensure businesses provide financial disclosures that are clear and accurately describe the current conditions of the business that is issuing their financial statements (Chiu et al., 2014). In some cases, this means the business should provide visual displays such as graphic presentations. The disclosures or footnotes should provide qualitative information that is supportive of the quantitative data expressed by the company’s financial figures. Many businesses provide a Summary of Significant Accounting Policies after the footnotes. These sections allow preparers of financial reports the opportunity to provide further details about the information that is considered by the business to be material but not required by GAAP (Brown & Nasuti, 2005).

In general, the SOX Act of 2002 has seemed to have slowed down the number of corporate scandals that have occurred when compared to the time just before the enactment of the SOX Act of 2002. The economy continues to recover from the tremendous impact of unethical practices occurring throughout corporations, accounting firms, and government offices (Brown & Nasuti, 2005). Section 409 of the SOX Act of 2002 has provided businesses with clear guidance and standards about the proper disclosure of financial and non-financial information. Enhanced disclosures are meant to provide users of financial information such as investors with a clear picture of the current status of the business's financial position.

Paragraph I of Section 409 of the SOX Act of 2002 describes real-time issuer disclosures. Real-time issuer disclosures encompass the concept that information is only useful if it is timely and relevant. Businesses must provide disclosures on a rapid basis, which allows investors to more accurately capture the financial conditions of a business and allow them to better understand the effects of any current material changes (Brown & Nasuti, 2005). Companies that provide disclosures that are within compliance of Section 409 of the SOX Act of 2002 are abiding by principles described by the AICPA Code of Professional Conduct and protecting investors and the public interest through their actions (Chiu et al., 2014).

PCAOB. The implementation of the SOX Act of 2002 is one of the most significant pieces of accounting and auditing legislation in U.S. history (King & Case, 2014). A significant accomplishment of the SOX Act of 2002 is that it establishes the Public Company Accounting Oversight Board (PCAOB) (Knechel, 2015). The PCAOB is responsible for the oversight of audits of public companies to ensure the independence and accuracy of audit reports (King & Case, 2014). The primary mission of the PCAOB is to provide oversight of the audits of public companies, protect investors, and serve the public interest through mitigating the occurrence of fraudulent and erroneous audit reports (King & Case, 2014). In addition to the creation of the authority of the PCAOB, the SOX Act of 2002 established the first auditing standard for both the audit and reported assessment of the business' internal controls (Brown & Trainor, 2014).

The PCAOB executes their duties through inspecting accounting firms which conduct thousands of audits of issuers, brokers, and other SEC registrants (King & Case, 2014). Knechel (2015) states that before the establishment of the PCAOB, peer-reviews among firms within the auditing profession was used to inspect the quality of audit practices. According to Brown & Trainor (2014), the establishment of the PCAOB considerably changed the long-standing condition of the auditor's reporting model for public businesses. The nature of the audit process has drastically evolved in recent history due to factors such as data processing, IT, cloud computing, and ERP (Knechel, 2015). The service of auditing continues to be a commercial activity associated with deliverables (i.e., audit reports) (Knechel, 2015). The PCAOB plays a vital role in standardizing audit reports, providing staff-audit alerts, and publishing staff questions and answers (King & Case, 2014). The PCAOB has provided the following standards to auditors in the preparation of audit reports. First, the audit report must include a description of the nature of the audit (Brown & Trainor, 2014). Second, the audit report must identify whether or not the auditor's opinion of the financial statements reflect relevant and accurate information that is void of material misstatements (Brown & Trainor, 2014). Third, the financial statements reflect information that conforms to the applicable financial reporting framework (Brown & Trainor, 2014).

Impact of the SOX Act of 2002. A major controversy that surrounded the enactment of the SOX Act of 2002 included the sizeable financial burden it put on businesses. Businesses were now required to increase internal controls and implement segregations of duties. These requirements changed how transactions were processed and ultimately led to additional costs (Chiu et al., 2014). A significant burden felt by many businesses was the requirement to provide audit documentation. The strict audit requirements of the SOX Act of 2002 meant that businesses would need to focus on human resources towards accomplishing audit readiness. This migration came at a cost for many businesses that did not commonly have to endure these types of strict audit requirements. The majority of the public and along with government officials, felt the SOX Act of 2002 was a necessary regulation and would ensure that businesses were disclosing accurate financial statements and protect stakeholders such as employees, communities, and investors (Brown & Nasuti, 2005).

The establishment of the SOX Act of 2002 emphasized the importance of internal controls and heightened the standard for public companies disclosing financial information. These changes were meant to reinstall confidence in the American public and investors about the accuracy and reliability of financial reports (Clements, Neill, & Wertheim, 2015). Internal controls encompass the processes and procedures that ensure compliance with GAAP, enable corporate governance, and mitigate risks (Jahmani & Dowling, 2015). The enactment of the SOX Act of 2002, specifically Section 404, has changed the way corporations, investors, and auditors defined internal controls (Jahmani et al., 2014).

Components of IT Controls

Appropriate levels of IT controls are vital to the successful performance of a business. IT controls are a valuable asset that businesses can use to avoid risks (Kuhn et al., 2013). Also, IT controls can be complicated, misunderstood, and inappropriately integrated (Kuhn et al., 2013). These errors can result in a business incurring a significant amount of financial losses (Kuhn et al., 2013). In order to better understand IT controls, it is crucial to have the ability to identify the various components of IT controls. General Controls and Application Controls are the two types of internal controls that are specific to IT (Rubino, Vitolla, & Garzoni, 2017).

General Controls. General controls govern all aspects of the IT function before the processing of transactions. General controls are the component of IT controls that are concerned with the relevant controls designed to manage a business's control environment (Rubino et al., 2017). The function of general controls is managing the mainframe, server, and end-user environments (Rubino et al., 2017). These functions can also include the appropriate controls that govern data centers, system access security, physical security, network operations, system software acquisition, system maintenance, and application acquisition (Rubino et al., 2017).

Overall, the primary function of general controls is the management of the control environment and the development of the IT infrastructure that is used by the business (Rubino et al., 2017). IT general controls can be categorized into six groups: administration of the IT function, separation of duties, system development, physical and online security, backup and contingency planning, and hardware controls (Rubino et al., 2017). Administration of the IT function encompasses the attitude and decisions made by senior managers and the board of directors to allocate resources in IT and assign authority (Rubino et al., 2017). Separation of duties is a general control that allows businesses to mitigate the risk of any potential conflicts of interest and the event of a single individual having too much power or the capability to cause serious harm to the business (Rubino et al., 2017). System development encompasses the acquisition or development of software that can assist the organization in meeting its objectives (Rubino et al., 2017). Physical security includes safeguarding computers, servers, and other IT hardware through the use of security guards, locks, and other types of physical barriers (Cook, 2015). Network security encompasses the use of librarians, network administrators, and computer operators to control individuals' access, the data that are accessed, and the granting of roles and permissions (Adnan, Just, Baillie, & Kayacik, 2015). Backup and contingency planning includes having fail-safes and policies in place in case of emergencies like natural disasters, inadvertent disasters, and deliberate attacks (Cook, 2015). Organizations often invest in resources such as backup generators, off-site storage, hot-sites, and cold-sites (Cook, 2015). Hardware controls are commonly included with the purchase of the IT equipment and come from the manufacturer. These types of general controls are intended to identify equipment failures or errors (Rubino et al., 2017).

Application Controls. Application controls are designed specifically for computer software applications and the governing of transactions (Kuhn et al., 2013). Application controls are needed to govern the control environment of software systems that support the most fundamental business processes and the financial reporting of a corporation (Kuhn et al., 2013). The majority of U.S. corporations use a variation of commercial-off-the-shelf (COTS) ERP systems that centralize and incorporates the primary business functions of any given organization (Al-Sabaawi, 2015). One of the leading providers of ERP systems in the industry is SAP. SAP-ERP has many application controls programmed within the enterprise software. These application controls allow roles and permissions to be both manually and automatically controlled to ensure the principle of segregation of duties and responsibilities is upheld and mitigate the risk of the occurrence of conflicts of interest (Kuhn & Morris, 2017). Application controls can be manual or automated and categorized as one of the following: input controls, processing controls, and output controls (Ragan, Puccio, & Talisesky, 2014).

Input Controls. Input controls are designed to ensure that the introduction of data into an information system is authorized, accurate, and complete (Ragan et al., 2014). Many input controls are specific to IT and are designed to ensure data quality (Ragan et al., 2014). A few examples of input controls include check digit, validity check, edit checks, limit tests, and the pull-down menu (Ragan et al., 2014).

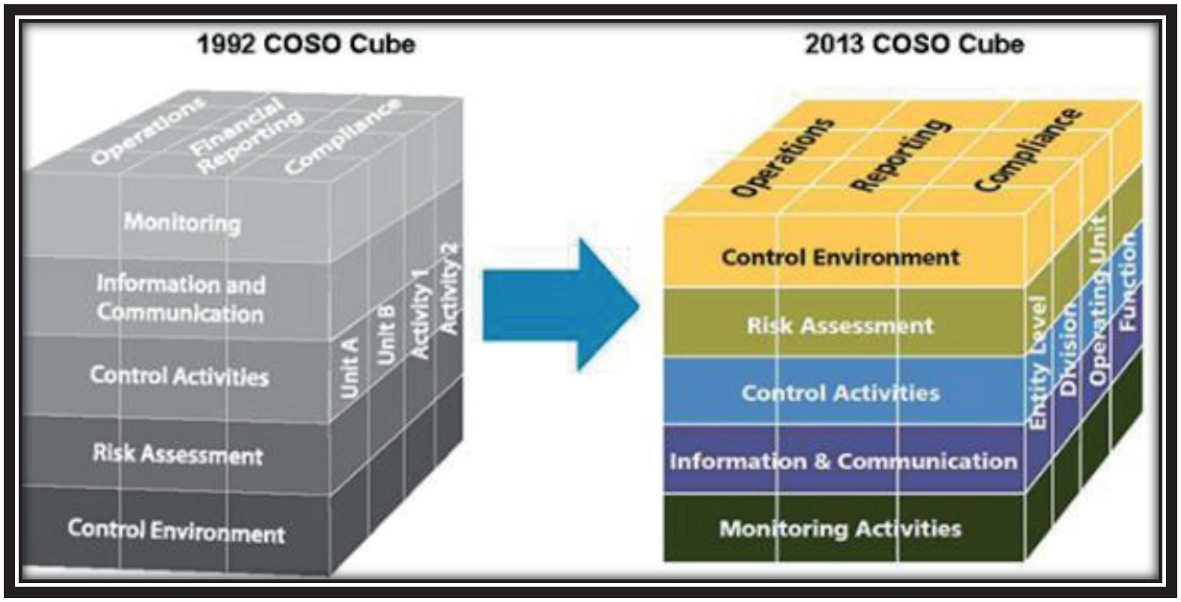
Processing Controls. Processing controls prevent and detect errors as transactional data is transferred and stored (Ragan et al., 2014). Processing controls are commonly programmed into the software in order to prevent, detect, and correct processing errors (Ragan et al., 2014). Examples of processing controls include validation tests, sequence tests, arithmetic accuracy tests, data reasonableness tests, and completeness tests (Ragan et al., 2014).

Output Controls. Output controls are used to detect errors once the processing of transactions is complete (Ragan et al., 2014). Output controls include examples such as the following: reconcile computer-produced output to manual control totals, comparison of processed units to submitted units, comparison of transaction output to input source documents, and verification of dates and times of processing in search of out of sequence processing (Ragan et al., 2014).

Internal Control Frameworks

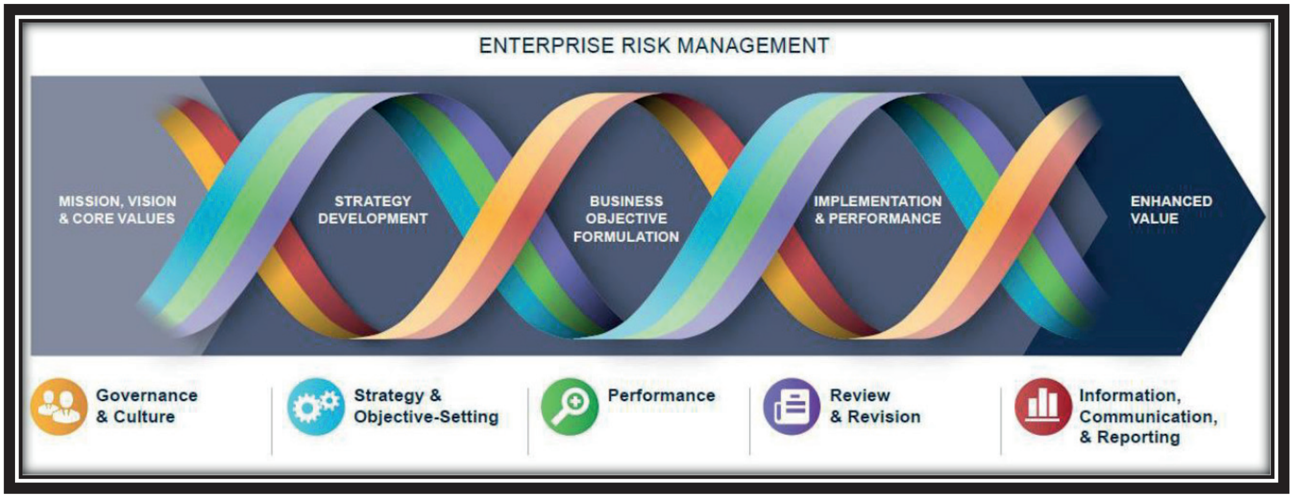
Committee of Sponsoring Organizations of the Treadway Commission (COSO). The COSO framework was initially published in 1992 and, more recently, updated in 2013 (Jahmani, Ansari, & Dowling, 2014). The majority of U.S. public businesses use the COSO framework as a means to meet the government standards of Section 404 of the SOX Act of 2002 (Kinkela & Harris, 2013). These businesses continue to choose the COSO framework even though the PCAOB has not made this a requirement (Rubino & Vitolla, 2014). The COSO framework classifies internal controls into five distinct categories (Rubino & Vitolla, 2014). These categories include the control environment, risk assessment, control activities, information/communication, and monitoring activities (Rubino & Vitolla, 2014). The COSO framework is useful in assisting businesses with improving governance over processes and internal controls for financial reporting (Jahmani et al., 2014).

2013 COSO Updates. The intent of the 2013 updates to the COSO framework was to assist management and the board of directors with improving IT governance (Kinkela & Harris, 2013). These changes enabled the internal controls processes to be implemented universally by different entities and at all levels and functions (Kinkela & Harris, 2013). Many businesses have a high level of success and satisfaction with the integration of the improved COSO framework (Samithisomboon & Chantatub, 2016). The basis for the changes to the COSO framework was rooted in the increased dependency of IT by businesses and advancements in IT. The updates were also intended to improve compliance and the quality of reporting by aligning current business practices and modern technology (Kimbell, 2017). According to D'Aquila & Houmes (2014), the 2013 updates to the COSO framework were explicitly intended as an internal control guide to be used by non-profit and governmental organizations. The following chart is a visual comparison of the 1992 COSO framework and the 2013 COSO framework.



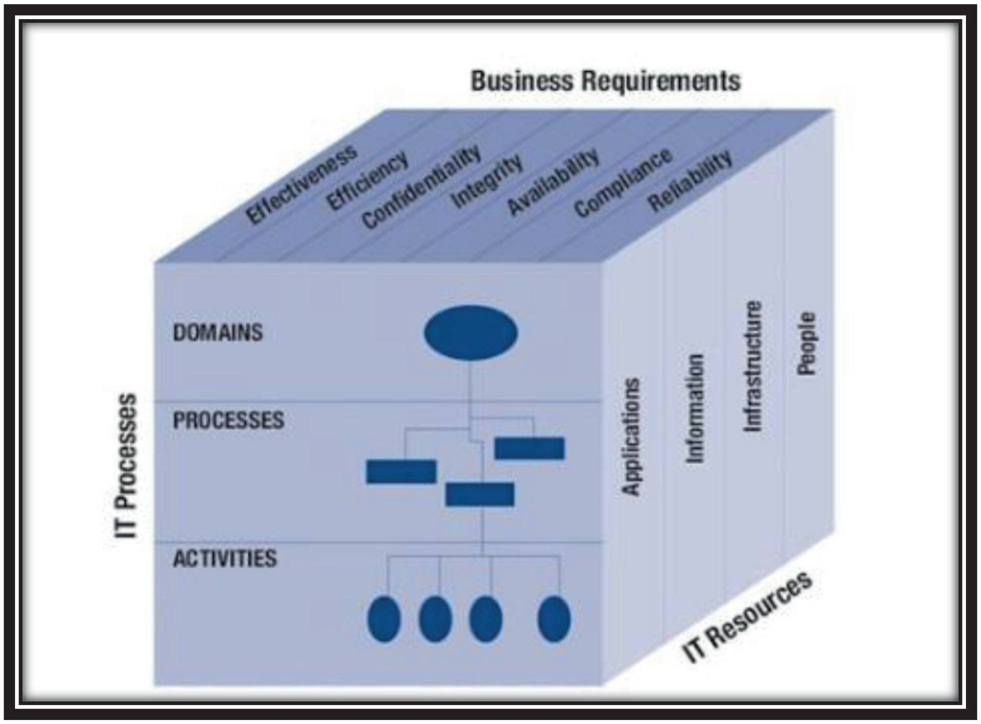
http://rsmus.com/content/dam/mcgladrey/images/figure/coso_cube_comparison.png
Figure 2. COSO Framework Comparison

2017 COSO Updates. In September 2017, the COSO Board published the Enterprise Risk Management (ERM)-Integrating with Strategy and Performance (COSO, n.d.). The purpose of the update is to assist organizations with managing uncertainty and determining an acceptable level of risk, meanwhile improving value (COSO, n.d.). The motivation for the updates was derived from the increased complexity of the business environment that many enterprises are faced with (COSO, n.d.). The increased complexity in the business environment is also associated with an increased level of uncertainty among businesses (COSO, n.d.). The updated framework allows organizations to improve their value through the improved application of ERM (COSO, n.d.). The updated ERM Framework is intended to complement and develop the COSO 2013 Internal Control-Integrated Framework further (COSO, n.d.). The 2017 COSO ERM Framework does not replace the COSO 2013 Internal Control-Integrated Framework (COSO, n.d.).


ENTERPRISE RISK MANAGEMENT
MISSION, VISION & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting

https://www.coso.org/Documents/COSO-ERM-Presentation-September-2017.pdf
Figure 3. 2017 COSO ERM Framework

Control Objectives for Information and Related Technology (COBIT). In 1996, the Information System Audit and Control Association (ISACA) created the COBIT framework to assist organizations with more efficiently managing their IT (Samithisomboon & Chantatub, 2016). The institution of the COBIT framework came during a time when large firms began to implement ERP and become more dependent on IT. An advantage of the COBIT framework is the ability to assist managers with balancing expected benefits and risks meanwhile supplementing the COSO framework (Samithisomboon & Chantatub, 2016). The progression of the COBIT framework has been from COBIT 1 to COBIT5, which begins with a primary focus as an audit tool and progresses to controls, management, IT governance, and the governance of enterprise/information systems (Rubino & Vitolla, 2014). The increased reliance on IT and the use of ERP have added higher value and importance to the application of the COBIT framework (Rubino & Vitolla, 2014).



http://www.bmc.com/guides/itil-cobit-introduction.html
Figure 4. COBIT5 Framework

Criteria of Control (CoCo). The CoCo framework is another popularly implemented approach towards internal controls (Babos, 2009). Canadian Institute of Chartered Accountants is responsible for the development of the CoCo framework (Babos, 2009). Also, CoCo identifies twenty factors that managers can use to improve efficiency and effectiveness (Babos, 2009). The structure of the CoCo framework is centered on four areas, which include purpose, commitment, capability, and monitoring and learning (Babos, 2009).

Information Technology (IT)

IT is a primary construct of IT controls and connects the constructs of security, ERP, and accounting. Taheri, Momeni, & Hashemi (2016) states there is a direct relationship between the useful application of IT and the reliability of accounting information. The primary function of IT in most organizations is a support role in many business and operational processes (Samithisomboon & Chantatub, 2016). In addition, the function of IT in most organizations is to engage in planning, networking, data management, and security (Kim et al., 2018). Due to globalization, the majorities of public businesses compete in international markets and have become dependent on IT to the point that any network interruptions have devastating financial effects (Dogaru, 2015). Business's inabilities to function due to network interference reflect the presence of internal weaknesses that can be exploited by cybercriminals (Dogaru, 2015). Cyber-criminals look for opportunities that can present themselves in the form of weaknesses in internal processes, infrastructure, or networks (Dogaru, 2015). Cybercriminals exploit these types of weaknesses for personal gains. Businesses have no choice but to invest in a sufficient level of IT controls to ensure they protect themselves against security threats (Dogaru, 2015).

IT Investment. The function of IT is incredibly critical to the financial reporting of a firm (Kim et al., 2018). On average, businesses invest 2.5 percent of their annual revenue in IT (Kim et al., 2018). A primary reason for these investments that total over $3 trillion globally stems from the need to mitigate the risk of IT control weaknesses (Kim et al., 2018). The SOX Act of 2002 has solely accounted for raising IT costs among all U.S. public companies to $1.4

billion (Jory, Peng, & Ford. 2010). Investing in IT enables businesses to replace manual controls with automated controls and reduce the risk of material misstatements of financial statements (Kim et al., 2018). In a study by Jory et al. (2010), there is a significant relationship between the positive reactions among the stock market and firms that have invested in IT in order to achieve compliance with the SOX Act of 2002. Also, the Jory et al. (2010) study shows firms that invest in IT for the expressed purpose of improving compliance with the SOX Act of 2002 fail to incur a positive market reaction when they report an internal control material weakness. These findings align with the correlational study of Kuhn & Morris (2017), which describes the significant relationship between reported internal control material weaknesses and stock returns. In order to comply with Section 404 of the SOX Act of 2002, businesses must strategically invest in IT in order to ensure they institute proper IT controls (Kim et al., 2018). The increased complexity and vulnerability that occurs with the automation of internal controls is a standard error made by businesses haphazardly spending money on IT without a critical plan to develop an effective financial reporting system (Kim et al., 2018).

IT Integration. The majority of large public corporations throughout the world use ERP systems to integrate the more significant part of their financial and business processes (Al-Sabaawi, 2015). The success of a business' ERP is depended upon the IT infrastructure and IT resources that are at their disposal (Kim et al., 2018). IT support must be available for regular maintenance, providing uninterrupted network connectivity, and providing dependable security (Bernroider, 2013). ERP and IT generally improve a business's computation power and the quality of reported financial information (Naveed, Ahmad, & Ahmad, 2016). The use of IT that is compatible with ERP allows firms to capture more data and information fields (Naveed et al., 2016). The main benefit of capturing more data and information fields is that it leads to an increase in performance measures, along with an increase in efficiency among management accounting activities (Naveed et al., 2016). Research is needed to understand the converging roles of IT specialists and accountants. This type of research would allow for a connection between the constructs of accounting, IT, and ERP. The majority of the literature describes the need for accountants to understand IT better as opposed to the need for IT specialists to better understand accounting (Strong & Portz, 2015).

IT Governance. IT governance was first termed in 1992 in order to describe the necessary IT components required to ensure organizational success (Rubino & Vitolla, 2014). IT governance is the subset discipline of corporate governance that management can use to focus on controlling the IT assets and the associated processes and procedures of the organization (Ettish, El-Gazzar, & Jacob, 2017). In the late 1990s and on into the 2000s, IT governance became a more commonly used term within academic literature due to the increased dependency and advancements in IT throughout the world (Rubino & Vitolla, 2014). Businesses use IT governance to reinforce many of their objectives that impact ERM and other associated processes (Samithisomboon & Chantatub, 2016).

In today's modern business world, many businesses have begun integrating the previously mentioned COSO ERM (2013) framework in order to ensure a sufficient level of IT governance (Ettish et al., 2017). IT governance is used to ensure that IT systems are controlled and managed in a manner that maximizes expected benefits and supports the long-term success of the organization (Ettish et al., 2017). According to Rubino & Vitolla (2014), the COBIT5 framework has an advantage compared to the COSO ERM (2013) framework in the categories of both ERM and internal control systems. A common practice to fill the gaps or deficiencies in the capabilities of ERM frameworks, many businesses use a combination of frameworks such as the

2013 COSO Internal Control Framework and the COBIT5 framework in order to maximize IT governance (Rubino & Vitolla, 2014; Ettish et al., 2017). Rubino & Vitolla (2014) use an analytical comparison study to describe the integration of the COSO ERM (2013) framework and the COBIT5 framework. The authors find that the COBIT5 framework is a viable solution for assisting organizations with reaching their internal control and ERM objectives (Rubino & Vitolla, 2014).

Ettish, El-Gazzar, & Jacob (2017) use a deductive approach to describe several integrated frameworks used by businesses to manage internal controls. The focus of the study is on examining the relationship between IT governance and internal control frameworks. The researchers describe the issue of the need for businesses to use multiple IT governance frameworks to have a sufficient level of ERM and IT controls (Ettish et al., 2017). The researchers' findings are based on the fundamental need for the corporation to obtain successful IT governance and operational control through five distinct corporate domains (e.g., strategic alignment, value delivery, resource management, risk management, and performance) (Ettish et al., 2017). In order for businesses to successfully meet the requirements established by each of these domains, businesses will likely integrate the following three frameworks; ERM, COSO, and COBIT5 (Ettish et al., 2017).

As described in previous sections, the COSO ERM (2013) framework was updated and is now known as the 2017 COSO ERM Framework (COSO, n.d.). Future research, similar to the work of Rubino & Vitolla (2014), is needed to compare the relational impact between IT governance, ERM, and internal control systems as a result of the integration of the COBIT5 framework and newly updated 2017 COSO ERM Framework. COSO states the 2017 COSO ERM Framework requires the support of the 2013 COSO Internal Control Framework (COSO, n.d.). The increased computerization of company data and the extensive use of ERP systems among businesses within the U.S. and internationally is the primary reason for managers to invest time and resources in IT governance (Rubino & Vitolla, 2014).

IT Responsibilities. IT has the responsibility to design, implement, and maintain the controls that govern an organization's business processes (Bharaditya, Sukarsa, & Buana, 2017). Public businesses are expected to integrate IT systems that are well-equipped with sufficient operational controls (Bharaditya et al., 2017). IT is accountable for supporting opportunities for businesses to gain competitive advantages through the improved accuracy of financial data, cost savings, added value to stakeholders, and increased operational efficiency (Ettish et al., 2017). The inability of a business to maintain a sufficient level of IT governance can cause an increase in IT controls weaknesses, a reduction in overall firm performance, and a decrease in market value (Kuhn & Morris, 2017).

According to Kim, Richardson, & Watson (2018), a primary concern of managers is the capabilities of the IT they are using and the IT control weaknesses they are experiencing. An interesting finding of the study shows that IT control weaknesses have more significant adverse impacts on executives than non-IT control weaknesses. Companies with a reported IT control material weakness were 24.9 percent more likely to terminate the Chief Financial Officer (CFO) (Kim et al., 2018). Managers have the responsibility to ensure the IT of a business must support an accurate and efficient financial reporting system. This requirement makes IT, and various types of IT control weaknesses a primary concern of managers for several reasons (Kim et al., 2018). First, IT can be costly, require a substantial upfront investment, and commonly associated with recurring maintenance fees (Kim et al., 2018). Second, managers face time constraints, and IT control weaknesses could be time-consuming to identify the specific problem (Kim et al., 2018). Third, there is a certain level of risk and vulnerability when investing in the capabilities of IT (Kim et al., 2018). The manager's investment may not fix the IT issue allowing the IT control weakness or may create other issues in the process (Kim et al., 2018). Fourth, the introduction of cloud computing technologies creates a more significant concern of cyber-threats and IT that is vulnerable to these types of IT control weaknesses (Kim et al., 2018). The research of Stanciu & Bran (2015) states that cybersecurity increasingly becomes a primary concern along with the investment in business tools such as ERP, complicated integrated accounting software, and IT. In a 2014 survey issued by Deloitte, 74 percent of CFOs identify cybersecurity as a top priority due to the high risks associated with the automated processing and storage of accounting data (Stanciu & Bran, 2015).

Enterprise Resource Planning (ERP)

ERP is a business software management tool that is often used to improve the way that businesses and organizations operate (Konthong, Suwan-natada, & Sompong, 2016). The increased integration of ERP is primarily due to advancements in IT and the increase in international business (Grabski, Leech, & Schmidt, 2011). Businesses use ERP to consolidate and refine many business processes such as accounting, human resources, and budgeting. In today's complex business world, businesses require complex business processes to operate efficiently (Sularto, 2016). These complex business processes can be complicated for managers and other stakeholders to understand. ERP streamlines and simplifies the complex processes of mainly medium to large-sized businesses (Hart & Snaddon, 2014). ERP using businesses can improve their profitability and capital strength when compared to businesses that do not use ERP (Ljutic, Marjanovic, & Djordjevic, 2014). ERP allows businesses to remain relevant and competitive, meanwhile achieving the standards of government regulations such as those instituted by Section 404 of the SOX Act of 2002 (Debreceny et al., 2005). ERP systems are easily integrated with Embedded Audit Modules (EAMs) and Computer Assisted Audit Tools and Techniques (CAATTs) (Debreceny et al., 2005). These types of ERP accessory applications allow businesses to monitor internal controls continuously and reduce the chance of suffering the adverse effects of IT control weaknesses (Debreceny et al., 2005; Kim et al., 2018).

Integration of ERP. Management is the determining factor within an organization that decides to invest and implement ERP (Lipaj & Davidaviciene, 2013). Management also decides and sets the level of integration. Businesses can have varying levels of integration that will impact their dependency on ERP (Sularto, 2016). Management must also analyze the impact of ERP on their accounting, financial aspects of their business, and human resources (Lodhi, Aftab, Mahmood, & Cheema, 2014). Managers must consider the theory of absorptive capacity when managing human resources and drastically changing business processes. Absorptive capacity is the business's ability and willingness to accept, adapt, and apply knowledge and methods. Implementing ERP requires employees with specific and unique skill sets with a willingness to change and learn new information (Debreceny et al., 2005). Companies with skilled employees who are willing and able to learn to use ERP will often find success with integration (Lodhi et al., 2014).

Impact of ERP. ERP is perhaps the most dominant tool used by businesses to manage day-to-day processes in today's business environment. ERP is a commonly used enterprise solution and used by businesses to improve efficiency in many operational areas. However, several negative impacts are a result of the use of ERP, such as the increased dependency on IT and the increased risk of IT control weaknesses. Firms that integrate ERP must also be concerned about proper training of employees, cyber threats, data storage, software compatibility, and a long list of costs to maintain the enterprise system (Lipaj & Davidaviciene, 2013; Lodhi, Aftab et al., 2014). According to the study by Kim, Richardson, & Watson (2018), only 14 percent of businesses are using manual systems; meanwhile, most businesses have turned to use ERP. In 2015, 21 percent of ERP using businesses reported their ERP integration process had become a complete failure, and 52 percent stated they were behind the anticipated "go-live" (Kim et al., 2018). Also, 60 percent out of the businesses that integrated ERP successfully reported they did not experience any gained benefit from the investment (Kim et al., 2018). The increased use and dependency on ERP, AIS, and IT increase the risk of incurring IT control weaknesses. Management must understand and account for the complexity and challenges associated with the integration of ERP systems (Debreceny et al., 2005).

Continuous Assurance. In response to the numerous landmark cases of corporate fraud, such as Enron, WorldCom, and Tyco, there has been a greater emphasis on the importance of continuous assurance, continuous auditing, and continuous monitoring of public companies' financial processes and frameworks (Kuhn & Sutton, 2006). According to the study conducted by Kuhn & Sutton (2006), ERP integrated with continuous assurance procedures enables businesses to monitor and report the status of their financial condition more readily and accurately than traditional methods. The two most prominent architectural systems that provide continuous assurance capabilities are Monitoring and Control Layer (MCL) and Embedded Audit Modules (EAM) (Kuhn & Sutton, 2006). Accounting theory explains the use and application of MCL and EAM that assist auditors and clients with the continuous assurance of the financial information within an ERP system.

Monitoring and Control Layer (MCL). MCL is often off-site and externally controlled by an independent auditor (Kuhn & Sutton, 2006). The use of independent servers allows the auditor to monitor the ERP system of clients continuously (Kuhn & Sutton, 2006). In comparison to EAM, a disadvantage of MCL is that it does not monitor the financial data of the client in real-time. MCL provides several advantages to EAM, such as reduced costs to the client created from the implementation and maintenance of continuous assurance systems (Kuhn & Sutton, 2006). MCL also operates externally and does not impact the performance of the client's enterprise system (Kuhn & Sutton, 2006). Also, MCL requires fewer human resources from the client to execute continuous assurance procedures (Kuhn & Sutton, 2006). The research of Kuhn & Sutton (2006) states the use of continuous assurance applications such as MCL is a viable solution that could have been used to detect irregularities in financial data at WorldCom.

Embedded Audit Modules (EAM). The goal and function of EAM are to improve the auditability of the user's organization. EAM allows businesses to provide more accurate and relevant financial information in real-time (Kuhn & Sutton, 2010). Also, EAM allows businesses to continuously monitor and test their internal controls for material weaknesses through the use of continuous sampling procedures (CSP) (Debreceny et al., 2005; Kuhn & Sutton, 2010). EAM allows internal and external auditors to more easily verify compliance and run substantive audit tests (Debreceny et al., 2005). Auditors must possess the skills necessary to efficiently and accurately conduct audits of financial data within an ERP system (Debreceny et al., 2005). The auditors must be experienced and knowledgeable about the internal functions of ERP, along with the financial processes of the business (Debreceny et al., 2005). The capabilities that EAM has to offer is a big marketing promotion for ERP providers and a favorable investment of ERP users (Debreceny et al., 2005). The research conducted by Jory et al. (2010) states that there is a favorable market reaction to firms that have invested and implemented ERP. EAM and improved continuous assurance are features that allow ERP to better assist businesses with improving auditability and compliance with the SOX Act of 2002 (Debreceny et al., 2005; Kuhn & Sutton, 2010).

Corporate Governance

Management. Management is a construct of corporate governance and connects many of the other primary theories found in IT control literature. A relationship under the theme of management can be drawn between the constructs of decision quality, streamlining business processes, product quality, productivity, and organizational performance (Kuo, 2014). The integration of ERP aligns with managements' desire to improve business processes, product quality, and decision-making capabilities (Kuo, 2014). The next most influential factors included free usage and distribution, compatibility with other solutions, technical and online support, global access to information, and the organization of knowledge. According to users of the Koha ERP systems, the three highest-ranked benefits were an integral solution, economic opportunities, and a reliable customer base (Makori & Mauti, 2016). Organizations that can improve these primary components of the business can improve their organizational performance. Managers that are implementing ERP should understand that ERP is the moderating construct, and there are many mediating constructs such as the level of ERP integration, flexibility, and the size of the company (Kuo, 2014).

Control Environment. Many managers perceive the control environment as the most critical component of an internal control framework (Rubino et al., 2017). The control environment is the cultural representation of the organization's overall attitude and behavior toward internal controls (Rubino et al., 2017). The control environment is partly defined by the organizational principles and values that are conveyed by management, expressed in the form of policies and procedures, and intended to reinforce competent and positive behavior (Rubino et al., 2017). An example of a healthy control environment for a public corporation is one that enables highly performing IT controls that produce financial records in compliance with Section 404 of the SOX Act of 2002 (Kinkela & Harris, 2013).

Corporate Social Responsibility (CSR). Cases of corporate fraud have shown the public how devastating they can be to families, communities, industries, and markets (Miller et al., 2016). In order for businesses to maintain a competitive advantage, they must display a genuine interest in CSR due to the high demand from the public (Pirrone & Trainor, 2015). Section 406 of SOX is titled code of ethics for senior financial officers (Kinkela & Harris, 2013). Companies must disclose their code of ethics to the public and describe how management actively promotes honesty and ethical conduct (Kinkela & Harris, 2013). Stakeholders such as society should be afforded the opportunity to read the intent of business and gain an understanding of how they plan or envision how conflicts of interests should be mitigated or resolved and how financial reports should be disclosed in general (Miller et al., 2016). These actions allow businesses to promote a positive culture throughout their organization as well as improve their trust with the public (Pirrone & Trainor, 2015).

Risk Management

Risk management encompasses the strategic methods used by a business to reduce the chance of financial loss (Derenyielo & Joseph, 2018). The primary tool of risk management is the application of internal controls. Executives, middle managers, and supervisors must have a thorough understanding of their organization’s internal controls along with the ability to test their functionality. The inability of businesses to adequately test and assess their internal controls can result in misidentifying material internal control weaknesses. The early recognition of internal controls weaknesses can save businesses from incurring significant financial losses. IT controls weaknesses can be extremely costly and challenging to identify. There are two significant processes companies use to maintain the integrity of their internal controls and manage their risk more effectively. These processes include the periodic testing of internal controls and the assessment of control risk.

Risk management encompasses the process of identifying, analyzing, assessing, controlling, and avoiding risks that could be incurred by an organization (Lackovic, 2017). Companies have many different strategies at their disposal when it comes to managing their risks. According to Bogodistov & Wohlgemuth (2017), the framework of risk management theory is the risk management cycle, risk assessment, and the four types of risk management (i.e., risk retention, risk reduction, risk avoidance or risk transfer in order to manage risks). These methods have a unique purpose and can be applied strategically to assist businesses with growth and stability (Derenyielo & Joseph, 2018). Risks can create many financial and operational constraints for a business. Engaging in risk management and implementing effective internal controls can assist a business by creating financial flexibility and avoiding financial distress (Lackovic, 2017). Management should understand each method and be able to determine when to implement each one of them.

Risk Assumption & Retention. Risk assumption and retention is a method used when an organization identifies what level of risk, they are willing to sustain or willing to absorb (Derenyielo & Joseph, 2018). A business may feel the method of risk assumption and retention is best after calculating the cost-benefit analyses of a business process and the risk involved (Derenyielo & Joseph, 2018). In some instances, the business may find it will cost more to mitigate the risk then if they were to absorb the costs. If the business process involves a large profit or increase in efficiency, then a business may choose to absorb the risks that are involved with that process. The business typically identifies an acceptable limit of risk that is involved with each process. Once the risk passes the specified limit, they must change their method in order to reduce the risk back to an acceptable level. An example of a business that uses the method of risk absorption and retention can pertain to pilferage, fraud, or embezzlement (Eaton & Korach, 2016). The Association of Certified Fraud Examiners' (ACFE) has reported that companies lose 5 percent of revenues due to fraud with a median loss of $145,000 per single case (ACFE, n.d.).

Risk Reduction. Risk reduction is also known as optimization and involves the process of reducing the severity of the risks that are involved with the business activity (Derenyielo & Joseph, 2018). Risk reduction is perhaps the most vastly used method of risk management (Derenyielo & Joseph, 2018). Many businesses begin with an understanding of the common risks that are involved with running that type of business (Derenyielo & Joseph, 2018). Risk identification is one of the most critical stages of risk management. Managers that can identify risks provide their company with an edge over their competitors (Derenyielo & Joseph, 2018). Managers can reduce the negative impacts of economic threats if they can identify and reduce potential risks (Lackovic, 2017).

Risk Avoidance. Risk avoidance is a method of risk management that enables a business to completely remove the risk from their business processes (Derenyielo & Joseph, 2018). A business may be able to avoid risk by engaging in alternative business processes or activities (Derenyielo & Joseph, 2018). Risk avoidance can be the most assuring method of decreasing risk, but it restricts the business from engaging in specific activities if they choose to avoid taking certain risks (Derenyielo & Joseph, 2018). Many companies may not have the luxury of withdrawing from particular processes or activities and may find that the method of risk avoidance is too restrictive and inapplicable. In many circumstances, risk avoidance can be advantageous to a business. Companies can be forced to adapt and evolve new and improved methods of internal controls in order to avoid risks (Derenyielo & Joseph, 2018). A business may identify a process that involves too much unavoidable risk, and in order to avoid the risk, they must reorganize the company and their business processes (Eaton & Korach, 2016).

Risk Transfer. The last method of risk management is risk transfer, which is also known as risk-sharing. Risk transfer or sharing is the process of allowing multiple parties or processes to assume liability and risk (Bogodistov & Wohlgemuth, 2017). Many companies recognize that certain risks are unavoidable and will inevitably occur. The business might not be able to reduce or avoid the risk due to the fact it could be detrimental to the organization if they did not participate in particular business activity (Derenyielo & Joseph, 2018). In these types of situations, management has the option to use the method of risk transfer. The most common example of risk transfer is insurance (Derenyielo & Joseph, 2018). The business is not avoiding risk through the use of insurance (Derenyielo & Joseph, 2018). The business remains liable and experiences the same amount of risk, but rather, the insurance compensates the business for losses incurred (Derenyielo & Joseph, 2018). The company absorbs the risk, but compensation does not sustain the negative impact (Derenyielo & Joseph, 2018). Risk transfer allows companies to continue with the same business process (Derenyielo & Joseph, 2018). Management can also transfer or share the risk internally by departments or processes, absorbing parts of the risk together (Bogodistov & Wohlgemuth, 2017; Derenyielo & Joseph, 2018). Sharing risk allows for individual departments or processes of a business to continue operating without completely being destroyed from the negative impacts (Bogodistov & Wohlgemuth, 2017).

Risk Management & IT Controls. Businesses engage in risk management in a variety of ways, depending on their strategy and objectives (Derenyielo & Joseph, 2018). The implementation of internal controls allows managers to reinforce the policies and guidelines of the organization. IT controls enable managers to manage risk through automation and the increase in efficiency (Derenyielo & Joseph, 2018). The increased efficiency and reduction of risk from implementing IT controls can be costly. Managers may also find an underlying disadvantage to managing risk through an increase in the use of IT controls, which adds to the complexity of business processes and the execution of transactions (Derenyielo & Joseph, 2018). The increased complexity of IT controls creates a demand for accountants, IT specialists, and managers with the skills and knowledge to understand the IT controls (Strong & Portz, 2015; Debreceny et al., 2005). The majority of businesses recognize the need and benefits of utilizing risk management as a means to avoid or mitigate the known or unknown risks of daily business operations (Derenyielo & Joseph, 2018). Management plays a crucial role in implementing, applying, and identifying the management of risk within their organization (Lackovic, 2017).

The concept of risk management is not to eliminate all risk but rather to assist businesses with making better decisions (Derenyielo & Joseph, 2018). Businesses can protect their interests from threats by decreasing the negative impact that may potentially be avoided or mitigated through risk management. The application of risk management has taken many forms and is a variety of businesses and industries use it in different manners (Lackovic, 2017). In the financial world today, risk management has been developed into ERM (Lackovic, 2017). Management can enable the success of the business by accurately identifying potential risks before they occur (Lackovic, 2017).

Enterprise Risk Management (ERM)

Risk management has evolved into a complex framework that incorporates all the business processes of an organization (Lackovic, 2017). In today's corporate world, one of the widely used risk management frameworks is ERM. ERM has developed from the traditional framework of risk management and evolved in order to accommodate the growing complexity of business processes and advancements in technology. Modern ERM can be set apart from traditional risk management through the presence of three distinct features (Lackovic, 2017). The first feature of ERM is that it accounts for risks from all possible sources and potential interactions (Lackovic, 2017). The second feature of ERM is to maximize the goals of the business rather than solely minimizing the losses from risks (Lackovic, 2017). The third feature of ERM is that it allows companies to take a proactive approach towards risks rather than a reactive approach when dealing with risks (Lackovic, 2017).

Benefits of ERM. Many businesses have recognized the need for ERM and realized the internal and external benefits that can be yielded from such an application (Lackovic, 2017). Businesses that emphasize values in ERM gain more trust with insurance entities, stakeholders, regulators, customers, creditors, and employees (Lackovic, 2017). ERM helps reduce risks that deal with strategic planning, marketing, compliance and ethics, accounting, legal, insurance, treasury, quality assurance, operational management, credit, customer service, and internal audit (Lackovic, 2017). ERM encompasses many types of internal controls, such as IT controls, to mitigate risks of material weaknesses (Lackovic, 2017).

Leadership and Support. ERM requires the dedication of management to ensure a smooth transition and accurate implementation (Lackovic, 2017). An organization must identify its values in order to establish the goals they wish to accomplish with the implementation of

ERM. Once a business has identified their goals, they can establish the standards that their ERM needs to meet and research what framework meets those standards. There are many different frameworks, and many have the misperception that there is only one way of executing ERM. The Risk Management Society (RIMS) is dedicated to providing guidance, leadership, and advancing all aspects of risk management (RIMS, n.d.). Through the RIMS web marketplace, companies can shop for leading professionals that provide expertise in risk management (RIMS, n.d.). RIMS enable businesses to find professionals with the knowledge, tools, and resources that can assist with implementing ERM (RIMS, n.d.). Once a company understands the desired framework, they can easily find a provider of ERM (RIMS, n.d.).

Implementation of ERM. Businesses do not have to reorganize or redevelop their processes and procedures when implementing ERM. Most companies have already established a basic foundation of risk management. ERM is meant to build and improve on a business's current risk management framework, along with its current internal control framework (COSO, n.d.). Updating a business' traditional risk management framework to ERM does not mean a company needs to throw out what has worked for them in the past (COSO, n.d.). ERM is a tool that allows businesses to reach goals and convey the current values and objectives of management (Lackovic, 2017). ERM is an investment that can have significant returns and find favor among investors (Lackovic, 2017). Implementing ERM should be strategic and carefully analyzed to ensure accuracy and a smooth transition.

Challenges of ERM. A business may face many challenges when implementing ERM. The significant challenges are the initial investment in ERM. Businesses must initially take the investment risk of choosing a framework that is suitable to them. Many companies commonly face the challenge of risk appetite. Risk appetite is defined as a company's willingness to take risks to achieve strategic goals. It can be difficult for a company to develop and agree upon acceptable risk or limit of risk with topics like liquidity, reputation and brand, supply chain management, acquisitions, environment, human resources, and corporate governance (Lackovic, 2017). In some instances, a company that has implemented ERM may feel their framework has become inflexible and too controlled.

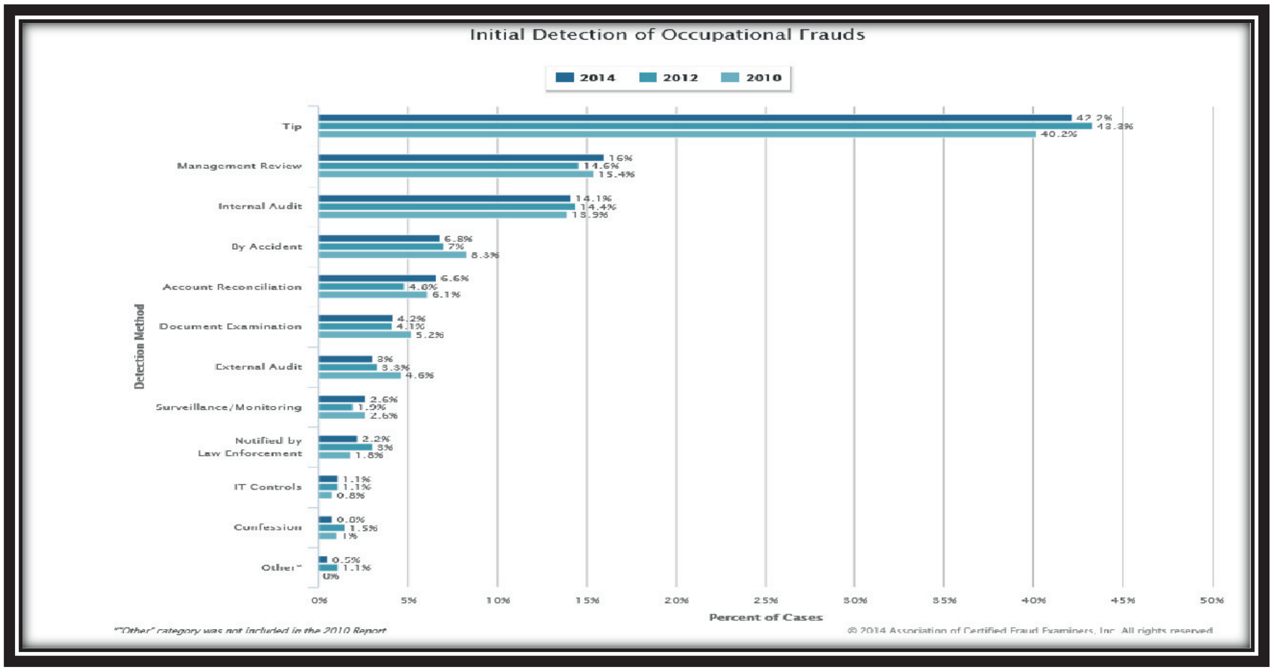
Application of ERM Framework. Many companies have been affected by Section 404 of the Sarbanes-Oxley Act of 2002. Section 404 requires corporations to implement a framework of internal controls and assessments. The majority of companies have turned to the COSO internal control framework in order to meet the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 (COSO, n.d.). Many companies have implemented the 2013 updates to the COSO internal control framework in order to keep up with the more sophisticated technology and business processes (COSO, n.d.). The COSO ERM framework was updated in 2017 to guide corporations on how to strategically and more effectively implement ERM (COSO, n.d.). A highly polarized political environment will often lead to changes in government regulation that impacts the methods used by businesses to manage risks and implement internal controls.

Security

IT control weaknesses leave businesses susceptible to risks such as security breaches, violations of segregation of duties, and fraud. These types of security risks have devastating effects on businesses and can result in the loss of confidentiality, integrity, and availability of IT assets (Kuhn & Morris, 2017). Businesses that incur IT control weaknesses will commonly have shortfalls such as: failing to manage IT security, failing to maintain their ERP correctly, and failing to implement IT governance (Kuhn & Morris, 2017). According to the study by Kuhn & Morris (2017), there is an apparent negative investor reaction to the reporting of an IT control weakness by a corporation. This type of market reaction stems from the theory of a correlation between IT control weakness and adverse events such as financial statement errors, earnings manipulation, and financial losses due to IT-related security breaches (Kuhn & Morris, 2017). A high level of security is a common objective of every business and requires overlapping areas of responsibilities from many different components. The ability to achieve these milestones relies heavily on a sufficient level and proper management of IT controls. The concept of security described within the IT controls literature directly connected to IT, risk management, and ERP. Management must meet the high demands of many internal and external stakeholders in order to remain relevant and competitive. He et al. (2013) describes the need for businesses to use ERP as a means to meet the demands of stakeholders and the standards instituted through government regulation. Management has a responsibility to ensure their organization's data is protected against security threats and mitigate the risk of having to report IT control weaknesses (Taheri et al., 2016).

Physical vs. Network Security. Security encompasses both virtual security (i.e., cybersecurity) and the physical security of their networks and infrastructure (Wang, 2014). Physical security includes safeguarding computers, servers, and other IT hardware through the use of security guards, locks, and other types of physical barriers (Cook, 2015). Organizations often invest in resources such as backup generators, off-site storage, hot-sites, and cold-sites (Cook, 2015). Network security encompasses the use system librarians, network administrators, and computer operators to control individuals' access, the data that are accessed, and the granting of roles and permissions (Adnan, Just, Baillie, & Kayacik, 2015). Backup and contingency planning includes having fail-safes and policies in place in case of emergencies such as fires, flooding, and power outages (Cook, 2015). According to Cook (2015), 75% of businesses will fail within three years after they experience a disaster. Businesses that invest and value security display a high sense of corporate governance and corporate social responsibility (Bawaneh, 2014). Businesses that fail to protect the data of customers and other stakeholders can find themselves faced with lawsuits and other financial setbacks. Maintaining the security of data allows management and investors to trust the financial information that is provided and make accurate decisions (Grabski et al., 2011). A sufficient level of working IT controls improves the security ERP and allows businesses to reduce the risk of cyber-attacks, which continues to plague nearly every industry (He et al., 2013). The increase in the security of enterprise systems ultimately improves the reliability of financial reports and the trust between organizations and stakeholders.

Corporate Fraud. Sherif, Pitre, & Kamara (2016) use a case study approach to describe the effectiveness of the IT controls that within ERP. IT controls are believed to be a leading deterrent against unethical behavior, such as corporate fraud (Morris, 2011). The qualitative research of Sherif, Pitre, & Kamara (2016) shows the primary deterrence against fraudulent activities are positive cultural values built on a strict code of ethics and reinforced by the support of top management. In a 2014 study conducted by the ACFE, the researchers find that IT controls only accounted for the detection of 1.1 percent of fraudulent activities; meanwhile, whistleblowers accounted for 42.2 percent of fraudulent activity detection (AFCE, n.d.).



https://www.acfe.com/rttn-detection.aspx

Figure 5. Initial Detection of Occupational Frauds

The data found in the bar chart above titled "Initial Detection of Occupational Frauds" reflect the ACFE report on the Initial Detection of Occupational Frauds for the years 2010, 2012, and 2014. Consistently, the ACFE finds IT controls are on the lower end of the spectrum when compared to Tips/Whistleblowers as the primary method of fraud detection. The ACFE also finds that management and internal audits play a crucial role in detecting fraud. The assumption that management has a more exceptional ability to reduce fraud than IT controls aligns with the case study conducted by Sherif, Pitre, & Kamara (2016). Research is still needed to understand the effects of specific IT control weaknesses on the financial performance of public businesses. IT controls have a relatively lower score when it comes to the ability to detect fraud, but internal controls score high when rated on their ability to be used to mitigate the risk of fraud.

Ethics and Responsibilities

AICPA Code of Professional Conduct. The AICPA Code of Professional Conduct describes the fundamental guidelines for accountants. These six principles include responsibilities, public interest, integrity, objectivity and independence, due care, and the nature of services. The basic principles that are foundational to the AICPA Code of Professional Conduct align with all accounting standards and along with the SOX Act of 2002. These ethical principles assist accountants with identifying and developing the financial information to include in the disclosures and footnotes of financial reports. Overall, AICPA's Code of Professional Conduct assists executives, accountants, and auditors with conducting themselves professionally and ethically. These principles act as a general foundation for the profession of accounting and assist businesses with making better ethical decisions (AICPA, n.d.). The PCAOB and the SEC both recognize the AICPA Code of Professional Conduct as a viable approach towards ethical professionalism (Sorensen, Miller, & Cabe, 2017).

Responsibilities. The principle of responsibilities, as described in the AICPA Code of Professional Conduct, states that Accountants have a responsibility to uphold the public's confidence and protect the sanctity of the accounting profession (AICPA, n.d.). The principle of responsibilities applies to disclosures since accountants commonly identify the financial information to report. Accountants must ensure that they identify the proper financial information and disclose it in a coherent manner that is understandable to all users of financial information. The business disclosures must align with the standard practices of other businesses within the industry (Sorensen et al., 2017).

Public Interest. In addition to the first principle, the principle of public interest part of the AICPA Code of Professional Conduct. Accountants must ensure they maintain the trust of the public, which encompasses serving the public interest and maintaining a high standard of professionalism (AICPA, n.d.). An essential aspect of serving the public is producing financial statements that include financial information that is accurate, timely, and reliable. Also, providing disclosures and footnotes that assist users with understanding financial information is an essential part of serving the public. The increased transparency allows businesses and the field of accounting to maintain public trust and better serve their interests (Sorensen et al., 2017).

Integrity. The principle of integrity is another pillar of the AICPA Code of Professional Conduct. Integrity is the measure between right and wrong and is a necessary element of accounting. Identifying or establishing rules for every scenario is impossible for governing bodies. Accountants must have the ability to identify a solution that is justifiable and ethical in the absence of clear rules or regulations. Accountants must focus on maintaining their integrity, along with the integrity of the accounting profession (AICPA, n.d.). Accountants can use disclosure and footnotes to provide information that is pertinent to stakeholders, even in the absence of clear rules stating the information must be disclosed (Sorensen et al., 2017).

Objectivity and Independence. Objectivity and independence are a principle that is part of the AICPA Code of Professional Conduct. Objectivity and independence encompass focusing on carrying out professional responsibilities, meanwhile avoiding conflicts of interest. Accountants must remain impartial and honest while executing their duties (AICPA, n.d.). During the preparation of financial disclosures, accountants must remain impartial and disclose the necessary information that will protect the public and the accounting profession (Sorensen et al., 2017).

Due Care. Due care is a principle that is a component of the AICPA Code of Professional Conduct. Due care describes how an accountant must carry out their duties. Accountants must be competent and provide a high standard of quality services. They must execute accounting services with a high level of technical proficiency and ethical standards. Accountants can express the principle of due care by striving for excellence and ensuring they are consistently serving the public interest (AICPA, n.d.). Accountants must display due care when they are developing and issuing disclosures and footnotes. The disclosures and footnotes provided in their company's financial statements must be within compliance of the rules and regulations, such as the Securities Act of 1933, the Securities Exchange Act of 1934, the Foreign Corrupt Practices Act of 1977, and SOX (Sorensen et al., 2017).

Scope and Nature of Services. The scope and nature of services is the last principle that is part of the AICPA Code of Professional Conduct. Scope and nature of services encompass the concept that an accountant must express consistency when it comes to professional services (Sorensen et al., 2017). Scope and nature of services tie together the concepts of integrity, independence, objectivity, and due care. Accountants must perform services that align with typical behaviors and practices within the accounting field (AICPA, n.d.). Disclosures and footnotes must be developed and presented in a manner that is consistent with businesses within the industry. Accountants must disclose financial information that is relevant and creates a sense of fairness across competitors and industries (Sorensen et al., 2017).

GAAP. ERP is intended to reinforce GAAP and allow organizations to remain compliant with government regulations (Grabski et al., 2011). The reoccurring concepts throughout the IT control literature are the need for producing accurate financial reports and the need to engage in risk management successfully. ERP uses the foundation of a general ledger-based accounting information systems (AIS) to improve the accounting and financial processes of a business (Grabski et al., 2011). Businesses commonly invest in ERP intending to improve transparency and improve the accuracy of their financial statements (Kim et al., 2018). The necessary financial disclosures and footnotes are described by Statement of Financial Accounting Concepts (SFAC) No. 5. SFAC No. 5 provides businesses with guidance about the proper methods for measuring and recognizing the figures found on financial statements. SFAC No. 5 offered guidance to businesses about the necessary steps to take in order to develop disclosures and footnotes that are accurately and qualitatively support the figures in the business's financial statements. These financial figures include those found on the income statement, the statement of retained earnings, balance sheet, and statement of cash flows (Fajardo, 2016). Businesses will commonly submit financial reports that do not capture all the necessary financial and non-financial information that is necessary to convey the current financial status of their business. Supplementary schedules, footnotes, and other parenthetical disclosures are commonly used by companies to improve their business's transparency and convey additional and necessary financial and non-financial information. Footnotes are among the most commonly used type of disclosure and come in four major formats. These formats include accounting policies, schedules and exhibits, explanations of financial statement items, and general information about a company (Dhanani & Connolly, 2015).

IFRS. Globalization has led to the need for an International Financial Reporting System (IFRS). The concepts of GAAP and IFRS run parallel to one another with slight differences (Kao & Wei, 2014). Principles gathered from both GAAP and IFRS are used in the development of ERP in order to improve compliance and allow businesses to operate in many countries. ERP is described as a viable solution to reinforcing ethical behavior and enabling firms to achieve regulatory compliance with multiple governments (Grabski et al., 2011). Research needs to be conducted to further understand the future role of GAAP, IFRS, ERP, and ethics. Additional research is also required to describe the relationship between ERP and government regulation, such as SOX and the Dodd-Frank Act of 2010 (Kao & Wei, 2014).

Accounting

Accounting theory is present in the theoretical framework of IT controls literature. Accounting theory encompasses the recording and reporting of the financial transactions of a business entity (Jabłoński et al., 2018). A significant benefit of ERP is the ability to apply the concepts and principles surrounding accounting theory and allow businesses to execute the many functions of accounting more easily. ERP is coded synonymously with IT controls intending to reinforce GAAP and improve compliance with government regulation (Kao & Wei, 2014). Businesses often view ERP as a viable means to improve reporting by providing financial information that is more accurate, reliable, and timely (Jabłoński et al., 2018). The ability of ERP to improve the quality and integrity of financial data is rooted in the application of IT controls (Rubino et al., 2017).

The Function of Accounting. Accounting is a primary construct of IT controls that link many of the other constructs within the IT controls literature. The reoccurring construct of accounting establishes the fundamental goal of all accounting software, information systems, and internal control systems are to record accurate, relevant, and timely financial data (Rubino et al., 2017). Kanellou & Spathis (2011) describes that accounting encompasses financial reporting, general ledger, auditability, reconciliation, and analysis of financial transactions within a business. The integration of the concepts of accounting and IT establishes a basic framework of ERP (Kanellou & Spathis, 2011). Advancements in accounting or IT can significantly affect the development and function of ERP (Rubino et al., 2017). A primary accounting function of ERP in today's business world is the ability to automate incessant accounting tasks such as activity-based costing (ABC) (Bhumgara & Sayyed, 2017). Businesses in the restaurant industry, like many other industries, have found success with the use of ERP in streamlining essential accounting functions that allow businesses to gain a competitive advantage through cost reduction (Sularto, 2016).

Auditability. Auditing Standard No. 5 describes the essential elements and capabilities of application controls (Morris, 2011). Auditing Standard No. 5 creates an important relational link between auditing and the inherent ability of IT to maintain the integrity of internal controls more effectively than manual internal controls (Morris, 2011). The theory suggests that the application controls that integrated with IT are less likely to have weaknesses because they are not subject to human error (Morris, 2011). The research conducted by Johari & Hussin (2016) reflects the ties between the concepts of auditability, internal controls, and corporate governance. Auditability is the foundation of financial reporting and is achieved when a business can maintain the integrity of control processes and provide accurate and adequate information about financial transactions (Johari & Hussin, 2016). The existence of an IT control weakness reflects a message there has been a breakdown in the auditability triangle (Johari & Hussin, 2016).

The auditability triangle is a three-pillar corporate governance model composed of effective internal controls, capable processes, and competent personnel (Johari & Hussin, 2016). The first pillar of the auditability triangle is effective internal controls, which describes the unbias forces that ensure the proper execution of the processes and procedures that are per organizational policies and guidelines (Johari & Hussin, 2016). The second pillar is the capable processes that refer to the accurate recording of transactions and preparations of financial statements (Johari & Hussin, 2016). The third pillar describes competent workers that have proper authorization, training, and experience to manage financial transactions and prepare financial statements (Johari & Hussin, 2016).

Test of Internal Controls. Managers, IT Specialists, and Accounting professionals must have the ability to test internal controls effectively. These necessary skills and abilities extend to IT controls that can be more complex and difficult to test. In many cases, IT controls require IT Specialists that understand the concepts of accounting, vice versa, or a combined effort in order to test an IT control properly. Testing internal control encompasses several processes. The auditor should assess the audit risk through inquiry, inspection, and observation (Mentz, Barac, & Odendaal, 2018). Auditors should also design substantive procedures if they find the testing of the internal controls to be ineffective or inefficient (Mentz et al., 2018).

The Changing Role of Accountants. The development of ERP has dramatically impacted the identity and role of accountants (Grabski et al., 2011). The skills and abilities needed to be an effective and efficient accountant have drastically changed when compared to those of traditional accountants (Grabski et al., 2011). The application of social identity theory and the framework of the Professional Accountants' Identities Chart can be used to explain the identity formation of accountants (Brouard et al., 2017). The role of accountants is defined through various societal demands, professional associations, employers, and accounting firms (Brouard et al., 2017). Advancements in IT and the use of ERP systems can impact each of these factors and the defined role of accountants (Chen et al., 2012).

The concepts of accounting, ERP, IT, and internal control frameworks are the primary focus of the study conducted by Monk & Lycett (2016). This study focuses on students of accounting and their lack of familiarity and interest in understanding ERP and IT. The traditional role of accountants is evolving into a hybrid role that emphasizes an equal need for both accounting and IT skills (Strong & Portz, 2015). Traditionally, managerial accountants collect, analyze, and prepare financial data that are then useful for decision-makers (El-Sayed &

Youssef, 2015). In more recent years, literature and events reflect a changing role of managerial accountants. These changes include taking on an advisory role and acting as managerial decision-makers (El-Sayed & Youssef, 2015). The changing role of accountants, like many professions, will be a catalyst for a change in the accounting curriculum (El-Sayed & Youssef, 2015). There is a need for further research about higher learning institutes and their approach towards assimilating accounting and IT curriculum.

Strong & Portz (2015) provide research which supports a lack of emphasis on IT for many accounting majors throughout universities. ERP relies heavily on the skills of IT specialists and drastically impacts the daily functions of accountants. Accountants, in today's business environment, require education and experience with IT, ERP systems, and AIS (Strong & Portz, 2015). Professional identity changes, along with the changes within society demands, have created a gap between the expectations of accountants and the accounting education that students receive at higher learning institutions (Strong & Portz, 2015). The accounting profession, along with the accounting curriculum, continuously changes due to factors such as globalization, advancement in technology, and government regulation (Brouard, Bujaki, Durocher, & Neilson, 2017).

Summary

IT controls encompass the policies, processes, procedures that businesses implement to ensure their financial data is accurate and in alignment with organizational goals and objectives (Erickson et al., 2014). The Sarbanes-Oxley (SOX) Act of 2002 significantly impacted the way businesses in the United States viewed and defined IT controls (Deis & Byus, 2016). Section 404 and Section 409 of the SOX Act of 2002 significantly increased the requirements of public business' annual financial statements. The requirement of businesses to provide an assessment of any internal control material weaknesses to include an account for all IT control weaknesses protected investors and instilled trust in the U.S. market (Deng et al., 2017). IT controls have become more critical to our society through the increased use of IT. Advanced systems such as ERP have allowed U.S. businesses to expand operations and compete in markets globally. ERP has allowed businesses to improve IT governance, competitive positioning, and overall performance (Deng et al., 2017). The extensive use of ERP offers businesses the additional ability to comply with the SOX Act of 2002 and many other business regulations of foreign governments. The advancement in IT has assisted businesses with the integration of frameworks such as COSO, COBIT5, and COCO (Samithisomboon & Chantatub, 2016; Kinkela & Harris, 2013; Babos, 2009). The increased complexity of business processes and IT controls requires managers to engage in methods such as corporate governance, IT governance, and risk management (Rubino & Vitolla, 2014; Ettish et al., 2017). Managers also find it necessary to integrate more advanced and updated systems like ERM in order to maintain the integrity of their business's financial records. IT controls are an essential security measure to ensure businesses can mitigate threats such as fraud or material misstatements (Sherif et al., 2016). Businesses must comply with GAAP in order to be considered acting ethically and responsibly and IFRS when engaging internationally (Grabski et al., 2011). Also, executives and accounting professionals must understand the principles of the AICPA Code of Professional Conduct in order to fulfill their responsibilities and improve internal controls.

The purpose of this brief literature review was to describe the theories and constructs associated with IT controls to assist in researching the effects of various types of IT control weaknesses on the financial performance of publicly traded U.S. corporations. The framework of this study was built from the research of Kuhn et al. (2013), which states; companies that report both material IT and Non-IT control material weaknesses will consistently experience lower levels of financial performance. This proposed research is intended to fill the gap IT controls literature through gaining a deeper understanding of the impact of various types of reported IT control material weaknesses (i.e., independent variables) on the Tobin's Q and Open Market Value (OMV) (i.e., dependent variables) of U.S. publicly traded businesses (Ragothaman & Cornelsen, 2017). A description of these variables in further detail, along with other elements of the research method and design are in the subsequent Chapter.

Chapter 3: Research Method

The purpose of this quantitative causal-comparative research study was to identify the differences that possibly exist in the effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses. The basis for conducting this research stems from the research conducted by Kuhn et al. (2013), which shows that companies that report both IT control material weaknesses and Non-IT control material weaknesses experience lower levels of financial performance. Also, this research was intended to build on the work of Ragothaman & Cornelsen (2017), which describes the negative relationship between internal controls material weaknesses and gross margin. These previous studies have both shown evidence of the negative impact that reported IT control material weaknesses have on the financial performance of publicly traded U.S. corporations. This study is used to describe in further detail the extent of the adverse effects on the financial performance of publicly traded corporations that are possibly caused by individual types of IT control material weaknesses. In this chapter, the research methodology and design of this study are described along with an examination of the population, sample, instrumentation, variables, procedures, data collection, data analysis, assumptions, limitations, delimitations, and ethical assurances. The research method described in Chapter 3 will be used to answer and test the following research questions and hypotheses.

Research Questions

Q1: What are the differences in financial performance between U.S. publicly traded businesses that report various types of IT control material weaknesses and U.S. publicly traded businesses that do not report IT control material weaknesses?

Q2: What are the differences in market valuation between U.S. publicly traded businesses that report various types of IT control material weaknesses and U.S. publicly traded businesses that do not report IT control material weaknesses?

Q3: What are the differences in financial performance between U.S. publicly traded business that resolved a various type of IT control material weakness in a given year and did not report any in the following year and U.S. publicly traded business that did not report an IT control material weakness in the same given year or the following year?

Hypotheses

H1: There is no significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded businesses that report various types of IT control material weaknesses (*x*) and U.S. publicly traded businesses that do not report IT control material weaknesses (*x*).

$H1_0$: $\mu_1 = \mu_2$

$H1_a$: There is a significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded businesses that report various types of IT control material weaknesses (*x*) and U.S. publicly traded businesses that do not report IT control material weaknesses (*x*).

$H1_a$: $\mu_1 \neq \mu_2$

H2: There is no significant difference in the Open Market Value (OMV) (*y*) between U.S. publicly traded businesses that report various types of IT control material weaknesses (*x*) and U.S. publicly traded businesses that do not report various types of IT control material weaknesses (*x*). $H2_0$: $\mu_1 = \mu_2$

$H2_a$: There is a significant difference in the Open Market Value (OMV) (*y*) between U.S. publicly traded businesses that report various types of IT control material weaknesses (*x*) and U.S. publicly traded businesses that do not report various types of IT control material weaknesses (*x*). ***$H2_a$*: $\mu_1 \neq \mu_2$**

H3: There is no significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded business that resolved a various type of IT control material weakness (*x*) in a given year (t) and did not report any in the following year (t+1) and U.S. publicly traded business that did not report a various type of IT control material weakness (*x*) in the same given year (t) or the following year (t+1). ***$H3_0$*: $\mu_1 = \mu_2$**

$H3_a$: There is a significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded business that resolved a various type of IT control material weakness (*x*) in a given year (t) and did not report any in the following year (t+1) and U.S. publicly traded business that did not report a various type of IT control material weakness (*x*) in the same given year (t) or the following year (t+1). ***$H3_0$*: $\mu_1 \neq \mu_2$**

Research Methodology and Design

A quantitative quasi-experimental or causal-comparative research methodology is an appropriate strategy that will enable a deeper understanding of the differences that exist between businesses that incur various types of reported IT control material weaknesses (Ragothaman & Cornelsen, 2017). The intent of conducting this study was to measure the effects that may exist among various types of IT control material weaknesses and the financial performance of the U.S. public corporations who reported them to the SEC. Public registrants of the SEC are mandated by Section 404 of the SOX Act of 2002 to disclose an assessment of all internal control weaknesses that are deemed material in nature (Erickson et al., 2014).

Retrospective Causal-Comparative Research Design. A retrospective causal-comparative research methodology is more favorable than other research methods due to the nature of the research problem and the stated purpose for conducting this study (Apuke, 2017). This research is considered quasi-experimental and “ex post facto” because the independent variable cannot be manipulated, and the participants have been introduced to the variables prior to the start of the study (Apuke, 2017). Matched-pairs *t*-tests are used in this study to better understand the target population (i.e., U.S. public corporations). The comparison of two near homogeneous groups that are distinct from one another based on the independent variable of various types of reported IT control material weaknesses will assist in measuring the differences in financial performance using the dependent variables of Tobin’s Q and OMV.

Quasi-Experimental vs. Experimental Design. A quasi-experimental research design, such as a retrospective causal-comparative design, was selected over an experimental design due to the inability to meet the feasibility standards necessary to be considered an actual experiment. The variables in this study occur due to the natural order of businesses engaging in relatively fair and competitive markets. The manipulation or disruption of the identified variables would not be feasible or meet the standards of ethical research (Apuke, 2017). The inability to manipulate the variables or randomly assign participants to groups removes any experimental design as a viable research strategy (Apuke, 2017).

Causal-Comparative vs. Descriptive and Correlational Design. A retrospective causal-comparative design was selected over a descriptive or correlational research design due to the purpose of the study. A descriptive or a correlational design is considered a practical research methodology for similar studies about IT control material weaknesses. In contrast to descriptive or correlational designs, causal-comparative designs allow for an inference to be made about a cause and effect relationship between variables along with predictions of causality. The ability to predict the probability of outcomes based on the findings of correlational studies allows stakeholders to make less risky decisions.

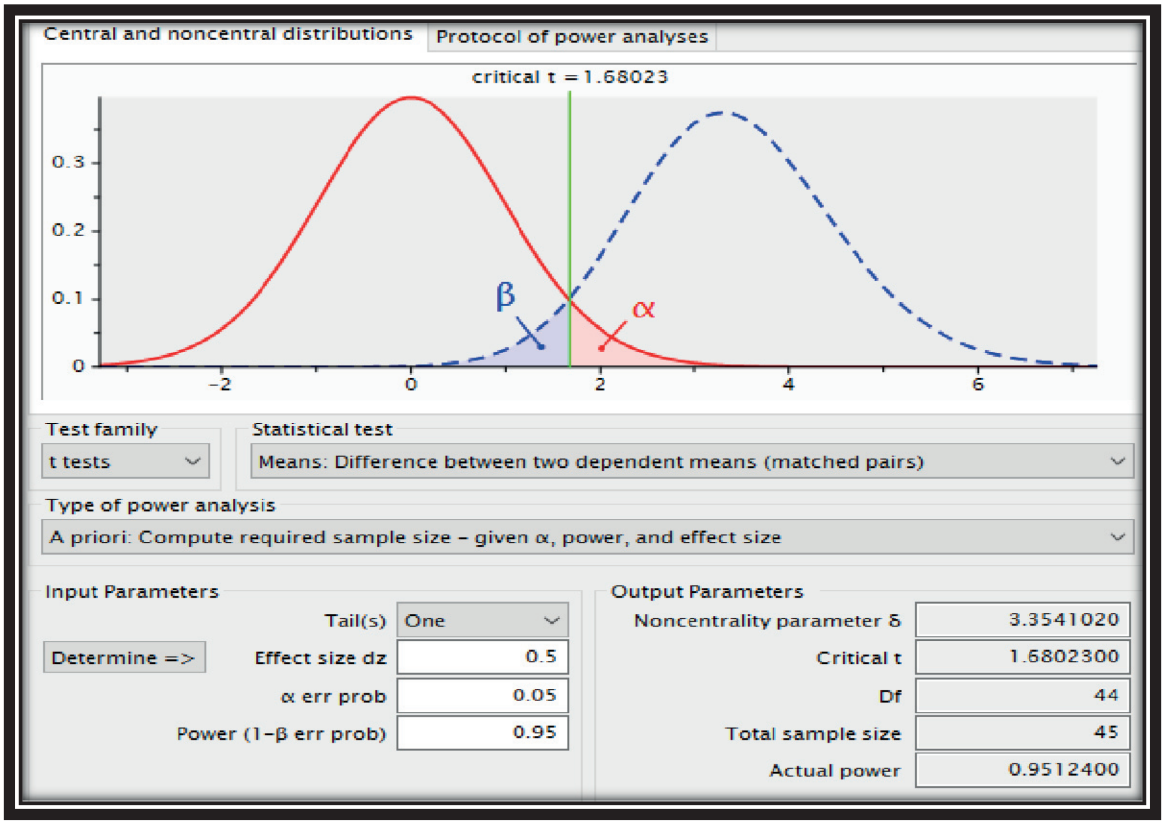
Meanwhile, the ability to make propositions of causation based on the findings of causal-comparative studies allows stakeholders to take programmed action. Descriptive and correlational research studies about IT control material weaknesses have been published throughout the literature and identified the negative relationship which exists between IT control material weaknesses and financial performance (Ragothaman & Cornelsen, 2017; Kuhn et al., 2013). A retrospective causal-comparative research design has been selected for this study with the intent to build from previous studies and gain a deeper understanding of the differences that may exist in the effects of different types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses.

Population and Sample

Population Characteristics. The target population of this study includes all U.S. corporations that fit the following criteria: they are registered with the SEC, they trade publicly on the U.S. stock exchange, and they fall subject to the requirements of the SOX Act of 2002. This population of public businesses is required by Section 404 of the SOX Act of 2002 to disclose an assessment of all internal control weaknesses that are deemed material in nature (Erickson et al., 2014). This information is archival data made available to the public and can be retrieved through several databases. The database maintained by the SEC is known as the Electronic Data Gathering, Analysis, and Retrieval System (EDGAR).

Sample Characteristics. The sample consisted of businesses selected from a population through the use of the quota sampling method. The sample size was determined based on the total number of reported IT control material weaknesses during the years of 2013-2018. This group of businesses with IT control material weaknesses (i.e., Group 2) were matched with a comparable business that did not report an internal control material weakness (i.e., Group 1). The businesses were matched together based on two primary criteria: industry type and annual earnings.

Sampling Method. The sampling method is non-random and consists of a minimum of 46 participating businesses. Group 2 must include 23 businesses that have reported an IT control material weakness and 23 businesses in Group 1 that have not reported an internal control material weakness. The method of sampling will be a quota sample that is based on the sample size of 46, which is required to maintain a sufficient effect size and power (Sprouse & Almeida, 2017). Quota sampling entails finding businesses that describe the following characteristics and represent the population. The ability to find participants is based solely on convenience and a set of strict characteristics. This method of matched-pair sets has been used successfully in the foundational studies for this research, which include the research of Kuhn et al. (2013) and the research of Ragothaman & Cornelsen (2017). The sample is appropriate for this study and will ensure the stated purpose is achieved, which is to measure the differences in the possible effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses. The use of matched-pair samples will enable comparisons to be made between the financial performance of businesses with various IT control material weaknesses and businesses without IT control material weaknesses.


Central and noncentral distributions
Protocol of power analyses
critical t = 1.68023
0.3
0.2
0.1
0
−2
0
2
4
6
β
α
Determine =>

Test family: t tests

Statistical test: Means: Difference between two dependent means (matched pairs)

Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters

Tail(s)	One
Effect size dz	0.5
α err prob	0.05
Power (1−β err prob)	0.95

Output Parameters

Noncentrality parameter δ	3.3541020
Critical t	1.6802300
Df	44
Total sample size	45
Actual power	0.9512400

Figure 6. G*Power Analysis

Power Analysis. The G*Power output in Graph 1 (Appendix A) provides a measurement of a sufficient sample size for this study. The statistical *t*-test would measure the differences between the means of two dependent groups (matched pairs). The statistical analysis would use an input parameter with an effect size (d) of .5, the α error probability of .05, β of .5, and Power (1- β error probability) of .95. A study based on a priori (before the fact) with a given α, power, and effect size would require an estimated minimum sample size of 46. The study would use two groups; Group 1 with a minimum of 23 comparable businesses that did not report an IT control material weakness and Group 2 with a minimum of 23 businesses that did report an IT control material weakness. The critical *t* factor would be 1.68023, and the non-centrality parameter λ would be 3.3541020. The Df value would be 44 with a large effect size (d) of .5. The β represents the probability of making a Type II error or accepting the null hypothesis when it is false. A Type I error is represented by α and is the probability of rejecting the null hypothesis when, in fact, it is true. The predetermined Type I error rate for hypothesis testing is 0.05 for each of the three hypotheses stated in this study. Based on the power analysis, the required sample size is exceptionally feasible when compared to prior studies with similar research designs such as Kuhn et al. (2013) and Ragothaman & Cornelsen (2017).

Materials/Instrumentation

The instrumentation method employed in this study has been used successfully in prior studies such as Kuhn et al. (2013) and Ragothaman & Cornelsen (2017). This study will use the most commonly used instrument, Microsoft Excel. Microsoft Excel will be used to create tables to display comparisons of various IT control weaknesses and Tobin's Q values between matched pairs within Group 1 and Group 2. The use of research tools such as Audit Analytics and EDGAR are well known and widely accepted resources that offer detailed and accurate data that can be cross-referenced for validity. The collected data will be analyzed through the use of the IBM SPSS Statistics (SPSS) application. SPSS will be used to produce descriptive statistics and charts. Also, SPSS will be used to conduct matched-pair *t*-tests in order to measure the differences in the possible effects of different types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses.

Internal Validity. Several concerns threaten the internal validity of this study. The design of a causal-comparative study reduces internal validity based on two primary factors. The first factor is the inability to select samples and assign businesses to a particular group randomly. The lack of randomization and subject selection bias increases the possibility the groups are inequivalent, which is a threat to the internal validity of this study. The second factor that threatens the internal validity of this study was the inability to manipulate an independent variable. The design of this study uses historical financial data about businesses that have already been impacted or introduced to an independent variable (i.e., various types of IT control material weaknesses).

External Validity. The external validity of the study is less concerning due to the large sample size and amount of datum that is available for public use. The sampling method identifies participants that share the same characteristics and are more generalizable to their populations. The study can be replicated using exact replication, conceptual replication, or systematic replication. These methods can all provide further evidence for external validity. External validity is reduced due to an inability to select and assign participants to a particular group randomly.

Operational Definitions of Variables

This study is used to measure the differences between the variables using matched-pair *t*-tests with the intent to gain a deeper understanding of the impact that various types of IT control material weaknesses have on the financial performance of publicly traded U.S. corporations (Weng, Chi, & Chen, 2015). The dependent variable of Tobin’s Q or Q-ratio is a measure of a firm’s valuation and financial performance (Ragothaman & Cornelsen, 2017). The calculation for the Tobin’s Q is a firm’s market value of physical assets divided by the replacement cost of assets (Ragothaman & Cornelsen, 2017). The dependent variable of OMV or market value is the price at which an asset would sell in a competitive and fair marketplace (Rognlie, 2015). OMV is a useful indicator of how investors perceive the financial performance of a business (Rognlie, 2015). OMV is calculated by multiplying the number of outstanding shares by the current share price (Rognlie, 2015). The independent variables are explained in detail by the research of Rubino & Vitolla (2014), which describe the COSO classification of internal controls into five categories, including the control environment, risk assessment, control activities, information/communication, and monitoring activities. The study of Rubino & Vitolla (2014) also describes the COBIT5 framework, which begins as an audit tool and progresses to controls, management, IT governance, and the governance of enterprise/information systems. The COSO and COBIT5 frameworks are widely accepted and commonly used to define and categorize the type of internal control weaknesses, such as different types of IT control weaknesses (Kuhn et al., 2013; Rubino & Vitolla, 2014). These frameworks are necessary for this research in order to define and categorize the various types of IT control material weaknesses that are reported to the SEC.

Study Procedures

The procedures used to conduct this study began with the approval from the Northcentral University Internal Review Board (NCU-IRB). The data collection method of this study was centered on the use of archived public data. Several methods can be used to collect the required data, which improves the feasibility of the study. The second procedure is to gain access to the data. The datum that is required is found on the audit reports and annual financial statements reported to the SEC by businesses. The third procedure is retrieving all data about publicly registered U.S. corporations for the years 2013-2018. This data is available through the Audit Analytics public company intelligence database. Information about subscribing to Audit Analytics can be found at the website https://www.auditanalytics.com by calling (508) 476-7007 or via email at info@auditanalytics.com. A download of the data can be exported in Microsoft Excel format. The fourth procedure is to conduct statistical tests by uploading the data into IBM SPSS Statistics. The statistical tests will include descriptive statistics and matched-pair *t*-tests. The fifth procedure is to analyze the data and interpret the findings.

Data Collection and Analysis

Data Collection Method. The archival data collection method will be used in the study to retrieve financial and non-financial data about public businesses in the U.S. The Audit Analytics database will be the primary source of data. The data from this database will be cross-referenced with the SEC's official database, EDGAR, for public disclosures made by SEC registrants. The data collected from the Audit Analytics database can also be verified through the analysis of 10K annual financial reports that have been reported to the SEC (AICPA, n.d.). The data collected from audit reports are verified by multiple layers of accounting professionals, including the endorsement of a certified public accountant (CPA) (Schaltegger & Zvezdov, 2015). The Chief Financial Officer (CFO) or a similar ranking official in the company will often scrutinize and investigate the findings during an audit. The additional levels of inspections mitigate the risk that the data included in the audit reports contain errors. The Audit Analytics database will identify demographic information to categorize businesses into two groups of businesses; one with IT control material weaknesses (i.e., Group 2) and one that did not report an internal control material weakness (i.e., Group 1). The Audit Analytics database will also identify the industry and earnings required to establish a sample of matched pairs.

Data Analysis. The descriptive statistical analysis will primarily include a comparison of the mean of each group and the standard deviation in order to determine whether the scores are homogeneous or heterogeneous about the mean. The dependent or matched-pair *t*-test will be used for inferential statistical analysis of the data. The test will be one-tailed and use a sample size (N) of 46 with 23 in Group 1 and 23 in Group 2. The matched-pair *t*-test will be used to compare the mean of Group 1 (μ_1) with the mean of Group 2 (μ_2). Group 1 is comprised of U.S. publicly traded businesses that do not report IT control material weaknesses. Group 2 is comprised of U.S. publicly traded businesses that have reported various types of IT control material weaknesses (*x*). The mean of the difference ($T_{\bar{D}}$) found among the mean of each set of pairs ($\bar{x}$) from both groups and will be compared to the outcome predicted by the null hypotheses. The skewness, kurtosis, mean, median, mode, range, and significance values will be included in the descriptive statistics. Also, cumulative frequency polygons will be used to provide a visual representation of the distribution of the data collected from each of the two groups. The matched-pair *t*-test will be used to measure the differences between publicly traded U.S. businesses that report (*x*) types of IT control material weaknesses and publicly traded U.S. businesses that do not report IT control material weaknesses The results of these tests will be used to test each hypothesis and answer each research questions.

H1 Data Analysis. The first research question (Q1) aligns with the first hypothesis (H1) and requires a compiled list of independent variables gathered from the Audit Analytics database to identify various types of IT control material weaknesses (*x*) that have been reported by the sample. Public data about the industry and size of the businesses being samples are used to develop matched-pairs. Matched-pair *t*-tests are used for comparing differences between the mean Tobin's Q (*y*) of U.S. publicly traded businesses that do not report IT control material weaknesses (*x*) (i.e., Group 1) and U.S. publicly traded businesses that report various types of IT control material weaknesses (*x*) (i.e., Group 2). The predetermined Type I error rate for hypothesis testing is 0.05.

H2 Data Analysis. The second research question (Q2) aligns with the third hypothesis (H2) and uses matched-pair *t*-tests to determine if Group 1 and Group 2 are statistically different. An answer to Q is necessary to gain a better understanding of the differences in the possible effects of various types of IT control material weaknesses (*x*) on the OMV (*y*) of U.S. publicly traded businesses. Matched-pairs or dependent *t*-tests are used to measure the differences between the mean OMV (*y*) of Group 1 and Group 2. The predetermined Type I error rate for hypothesis testing is 0.05.

H3 Data Analysis. The third research question (Q3) aligns with the third hypothesis (H3) and requires an inferential statistical analysis of the dependent variable between Group 1 and Group 2. The dependent variable used in H3 is the mean of Tobin's Q (*y*) as a measure of financial performance. Matched-pair *t*-tests are used to measure the differences between the mean ($t_{\bar{D}}$) Tobin's Q (*y*) of Group 1and Group 2. The subgroup used to answer Q3 applies the element of time to compare the practical differences in financial performance between consecutive fiscal years. The criteria used to establish a Group 2 subgroup includes U.S. publicly traded business that resolved a various type of IT control material weakness in a given year and did not report any in the following year. The criteria used to establish the control subgroup includes U.S. publicly traded business that did not report a various type of IT control material weakness (*x*) in the same given year (t) or the following year (t+1). The predetermined Type I error rate for hypothesis testing is 0.05.

Assumptions

Data Comparison. An assumption that may exist with the design of this study was the accuracy of the data from the Audit Analytics database. The datum is expected to match when cross-referenced with the data with the EDGAR database, which is maintained SEC. The data should also match the information provided from the 10K reports retrieved from businesses' official webpages.

Data Compatibility. The design of this study also includes the assumption that the data is compatible with Audit Analytics, Microsoft Excel, and IBM SPSS Statistics. Data compatibility issues may require additional time to manually research and input data. The manual processing of data increases the possibility of human error and bias.

Accurate Reporting. An important assumption is that publicly registered businesses and external auditors are accurately assessing and defining IT control material weaknesses uniformly with the COBIT5 and COSO frameworks. An assumption is made that the IT control material weaknesses are reported accurately when in fact they may be inconsistently categorized or incorrectly reported. The research is conducted under the assumption that the audit reports and financial statements are accurately assessed and reported.

Limitations

A potential limitation with the causal-comparative research design of this study was the inability to manipulate the independent variables. The independent variables occurred in the natural progression of business activity and are considered “ex post facto.” The inability to manipulate the independent variables will only allow suggestive inferences to be made about causation with less than perfect correlation. The inability to select and assign participants randomly reduces the level of external validity due to the increased possibility of selection bias (Weng, Chi, & Chen, 2015).

Delimitations

This research methodology and design are used in support of a deeper understanding of various types of IT control weaknesses that negatively impact the financial performance of public firms in the United States. There is little research that explains the extent to which various types of IT control material weaknesses negatively impact the financial performance of public firms in the United States. This causal-comparative study is intended to identify the differences that may exist in the effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses. This study was used to describe in further detail the extent of the adverse effects on the financial performance of publicly traded corporations that are possibly caused by individual types of IT control material weaknesses. This research is not intended to recreate prior studies reflecting the holistic negative impact of IT controls material weaknesses on the financial performance of public businesses. Instead, this research measures the extent of the negative impacts that individual types of IT control material weaknesses have on the financial performance of public businesses.

The theoretical framework of this study was developed through the application of IT Governance Theory, Accounting Theory, Audit Theory, and Internal Control Theory. In the center of this theoretical framework, IT control material weaknesses are found to be one of the most critical variables in need of research. One reason IT control material weaknesses were selected to be studied over other types of internal control material weaknesses is due to the substantial dependent relationship that exists between businesses and IT in recent history (Dogaru, 2015). A second reason IT control material weaknesses were selected to be studied over other types of internal control material weaknesses is the devastating financial impacts that IT control material weaknesses have over non-IT control material weaknesses (Kuhn et al., 2013). Since firm performance is not solely measured by internal determinants and requires the input of external factors, the Tobin’s Q variable is used as a measure of firm performance over return on assets (ROA). The study is also used to analyze the OMV of public businesses in order to isolate the external valuation factor that determines firm performance (Rognlie, 2015). An analysis of the differences in OMV is used to gain a perspective understanding of investors’ reactions to IT control material weaknesses (Rognlie, 2015). A delimitating factor for choosing these variables was the historical record and public availability of the required data and the potentially high relatability and utility of the findings.

Ethical Assurances

The study is focused on collecting data from solely businesses and does not include human participants. Archival data and public information provided from individual businesses to the SEC for public disclosure are used in this research. This study does require the approval of the Northcentral University Institutional Review Board (NCU- IRB) (The Institutional Review Board (IRB) Process, n.d.). The archival data will be collected and cross-referenced through databases such as EDGAR and Audit Analytics. This method has no ethical concerns about full-disclosure, confidentiality, and consent since the archival data is disclosed publicly (The Institutional Review Board (IRB) Process, n.d.). There are ethical concerns about the accuracy of results and the impact erroneous findings can have on the businesses, markets, investors, and other stakeholders. This study also required the foundation of the study to include the ethical principles of respect for persons, beneficence, and justice.

Full-Disclosure, Confidentiality, & Consent. There were no individual participants used in this study, but it is important to note that subjects must be given full disclosure about the intent of the study and how the data will be used (The Belmont, 1979). Personally identifiable information (PII) must be kept safe and secure from public view along with audit and financial information that may be collected from businesses. This type of information can be detrimental to the career and livelihood of participants (Packenham, Rosselli, Ramsey, Taylor, Fothergill, Slutsman, & Miller, 2017). Participants must provide their consent before a researcher can include them in a study (The Institutional Review Board (IRB) Process, n.d.). Consent means the participant has been given an adequate amount of information before engaging in the study (The

Belmont, 1979). This agreement also requires that the participant can understand the terms of the agreement. Consent is a sign that the principle of respect for persons is part of the foundation of the study (The Belmont, 1979).

Institutional Review Board (IRB). The primary standards and guidelines of the NCU-IRB include laws and regulations such as the Code of Federal Regulation Title 45 Public Welfare and The Belmont Report (1979). The purpose of the NCU-IRB is to protect participants and other stakeholders from experiencing undue hardship or unnecessary risk caused by research. The secondary purpose of the IRB is to promote and assist researchers in conducting ethical research. All researchers conducting research that includes the human subject on behalf of NCU are required to apply for approval to the IRB before any engagement. An approved IRB application is also necessary after the approval of a dissertation proposal and before the researcher engages in any data collection. The approval from the IRB is valid for one calendar year before an extension request is required (The Institutional Review Board (IRB) Process, n.d.).

Summary

This quantitative study is intended to identify the differences in the impact of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses using a retrospective causal-comparative research design (Apuke, 2017). This research builds on research conducted by Kuhn et al. (2013) and Ragothaman & Cornelsen (2017). These previous studies have both shown evidence of the negative impact that IT control weaknesses have on the financial performance of publicly traded U.S. corporations. A causal-comparative research design is used to gain a better understating of the differences between the independent variables of various types of reported IT control weaknesses and the operational efficiency and effectiveness of corporations using Tobin’s Q and OMV (Ragothaman & Cornelsen, 2017). Public registrants of the SEC are mandated by Section 404 of the SOX Act of 2002 to publicly disclose an assessment of all internal control material weaknesses (Erickson et al., 2014). The archival data collection method is used to retrieve public data about U.S. corporations registered with the SEC. The Audit Analytics database is used to collect data that can be cross-referenced for accuracy with the SEC’s EDGAR database. Matched-pair *t*-tests and descriptive statistics are used in this study to analyze the differences in the financial performance of U.S. public corporations that report various types of IT control weaknesses.

Chapter 4: Findings

The purpose of this quantitative causal-comparative research study was to identify the differences that may exist in the effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses. The basis for conducting this research stems from the research conducted by Kuhn et al. (2013), which shows that companies that report both IT control material weaknesses and Non-IT control material weaknesses experience lower levels of financial performance. Also, this research was intended to build on the work of Ragothaman & Cornelsen (2017), which describes the negative relationship between internal controls material weaknesses and gross margin. These previous studies have both shown evidence of a negative impact that IT control material weaknesses may have on the financial performance of publicly traded U.S. corporations. This study is used to describe in further detail the extent of the adverse effects on the financial performance of publicly traded corporations that are possibly caused by different types of IT control material weaknesses. In this chapter, a description of the findings and an analysis of the results are presented. The findings of this study are a direct result of the application of the research methodology and design identified in Chapter 3. The following sections provide an examination of the data validity, matched pair statistical tests, sub-samples, dependent/independent variables, procedures used in data collection, and analysis. The application of the previously described research design enabled the statistical testing of the hypotheses and the evidence necessary to answer each research question.

Validity and Reliability of the Data

The AuditAnalytics datasets serviced by Ives Group, Inc are commercially available as individual and customizable data feeds. The subscription and licenses provided through Ives Group, Inc. allow data feed integration of the AuditAnalytics data with several internal information systems such as CRM. Additionally, the AuditAnalytics data feeds are designed for individual users to easily compare different data streams through the use of custom applications and dynamic reports. The source of the SEC Registrant's information for all the data feeds come directly from the official SEC EDGAR database (https://www.sec.gov/Archives/edgar/data), which provided a retrieval date within a mean of 73.99 days from the reported financials date. The reporting SEC registrant was the origin of the data and provided the electronic 10K financial report. The submitted 10K report was endorsed by corporate management and inspected through external audits.

Preliminary Data Analysis. The AuditAnalytics database allowed the pertinent data to be retrieved to accurately test and measure each hypothesis through the use of search parameters. The first search criterion used to identify companies with IT control material weaknesses was the filing date range of >January 1st, 2013, and <January 1st, 2019. The second search criterion was the specific internal control weakness identified as IC – Information technology, software, security, & access issues. The third search criterion isolated the data explicitly to Unites States Registrants. The fourth search criterion filtered the search to include data originating from 10K filings of SEC Registrants. The remaining search features, such as the company name and the Standard Industrial Code (SIC) was intentionally left unfiltered in order to capture data from all SEC Registrants that met the previously described criteria. The search returned 307 SEC Registrants that fit the criteria to be assigned to Group 2 (see Table 2). The data for Group 1 was collected using the same method, except for finding SEC Registrants with the feature 'internal control weakness' being selected. Table 2 is a reflection of the sample broken down by the initial count by the fiscal year. Group 1 was initially comprised of data collected on 28,275 SEC Registrants without a reported internal control material weakness.

<table>
<tr><th colspan="3">PRELIMINARY GROUP ASSIGNMENT of SAMPLE
(count by fiscal year)</th></tr>
<tr><th>Fiscal Year</th><th>Group 1</th><th>Group 2</th></tr>
<tr><td>2013</td><td>5,166</td><td>48</td></tr>
<tr><td>2014</td><td>5,162</td><td>65</td></tr>
<tr><td>2015</td><td>4,888</td><td>73</td></tr>
<tr><td>2016</td><td>4,640</td><td>65</td></tr>
<tr><td>2017</td><td>4,543</td><td>47</td></tr>
<tr><td>2018</td><td>4,384</td><td>9</td></tr>
<tr><td>TOTAL</td><td>28,275</td><td>307</td></tr>
</table>

Table 2. Preliminary count by fiscal year of SEC Registrants

Data Errors. There were several errors and inconsistencies identified throughout the dataset. These data errors included anomalies such as missing source information, blank cells, and data fragments of vital information such as revenue, earnings, CIK/Ticker missing, and fiscal year. These inconsistencies were filtered and removed, leaving the sub-sample size of Group 1 remaining at 21,072 and the sub-sample size of Group 2 to be 202 (see Table 3). The SEC Registrants from Group 1 were as equally as possible matched with SEC Registrants from Group 2. There were 7,203 SEC Registrants removed from Group 1 and 105 SEC Registrants removed from Group 2 for the reason of missing pertinent financial and non-financial information. The exclusion of SEC Registrants with inconsistent data assists in strengthing the validity and reliability of the results by ensuring the most equivalent and homogenous paired samples were extracted for comparison and testing.

PRELIMINARY DATA ANALYSIS (count by fiscal year)		
Fiscal Year	Group 1	Group 2
2013	3,395	23
2014	3,457	42
2015	3,567	46
2016	3,597	42
2017	3,856	43
2018	3,200	6
Total	21,072	202

Table 3. Count of SEC Registrants by fiscal year minus data errors and analytical anomalies

Secondary Data Analysis. The collected data supported the matched pairs *t*-test design, which was identified as the most appropriate statistical test given the nature of the study research questions and hypotheses that were being tested. The matched pairs were created using If Statements and Boolean Expressions with Microsoft Excel to analyze the data outputs from the AuditAnalytics database. This method of analysis enabled the creation of homogenous matched pairs between SEC Registrants from Group 2 with a Registrant from Group 1 that operated within the same industry based on the criteria described in Table 4.

Grouping Criteria: Sub-Sample A	
1.	Annual 10K Report filed between the Years of 2013-2018.
2.	Standard Industrial Code (SIC)
3.	Total Amount of Annual Earnings
4.	Occurrence of an IT Control Material Weakness

Table 4. Categorical Criteria used to establish Homogenous Pairs for Sub-Sample A

Sub-Sample A. The matched pair sub-sample that was used to test hypotheses H1 and H2 resulted in a selection of 156 SEC Registrants from Group 1 paired with 156 SEC Registrants of Group 2. This sample size is well above the suggested sample size determined through the G*Power analysis output (Appendix A) described in Chapter 3. The G*Power analysis program was used to identify a minimum of 46 SEC Registrants as the required sample size to sufficiently support a matched pair designed study with an effect size (d) of .5, the α error probability of .05, β of .5, and a Power (1- β error probability) of .95. In this study, the sub-sample size is comprised of the data extracted from the 10K annual financial reports from 307 SEC Registrants. The filing dates of the 10K reports of the sub-sample span across the fiscal years of 2013-2018 (see Table 5).

Sub-Sample A: Matched Pair Samples by Fiscal Year		
Fiscal Year	Count of Group 1 by Fiscal Year	Count of Group 2 by Fiscal Year
2013	19	20
2014	33	34
2015	33	34
2016	18	29
2017	29	37
2018	24	2
Total	156	156

Table 5. Sub-Sample A: by Fiscal Year used to test H1 and H2.

Sub-Sample B. In order to test hypothesis H3, an additional sub-sample was collected from the dataset to account for the relationship between IT control material weaknesses and their occurrence over consecutive fiscal years. Microsoft Excel was used to develop If Statements and Boolean Expressions to analyze the data outputs from the AuditAnalytics database. The intent of analyzing the data was to identify the SEC Registrants that reported an IT control material weakness in a particular year between 2013 and 2017 (t) and a similarly matched SEC Registrant that did not report an IT control material weakness in the following consecutive year (t+1).

The secondary analysis was intended to identify homogenous counterparts consisting of the SEC Registrants that did not report an IT control material weakness for two consecutive years throughout the timeframe of 2013 to 2017. The SEC Registrants included in Sub-sample B were then filtered using the previously described criteria of SIC and earnings during the first year (t). The result was a total sub-sample of 266 SEC Registrants comprised of 133 SEC Registrants assigned to Group 1 and homogenously paired with the 133 SEC Registrants assigned to Group 2 (see Table 6).

Sub-Sample B: ((Group 1:Tobin's Q Δ (μ_1) (t-(t+1))) - (Group 2:Tobin's Q Δ (μ_2) (t-(t+1))))		
Fiscal Year	Count of Group 1 by Fiscal Year	Count of Group 2 by Fiscal Year
2013	27	16
2014	24	28
2015	32	31
2016	30	31
2017	20	27
2018	0	0
Total	133	133

Table 6. Sub-Sample B: by Fiscal Year used to test H1 and H2.

Grouping Criteria. The results of this study are primarily displayed through the use of tables developed within IBM SPSS Statistics. The dataset for this study was collected from the AuditAnalytics database with the intent to compare the differences in financial performance between companies and those that did not incur an IT control material weaknesses. Microsoft Excel was used as a preliminary analysis tool to code and filter the data into two groups of matched-pairs based on the criteria found in Table 7. The objective of the criteria shown in Table 7 was to establish the highest level of homogeneity between the paired samples. There were two sub-samples drawn from the dataset. One group consisting of 312 (156 matched-pairs) and the other group consisting of 266 (133 matched-pairs). The implementation of RQ3/H3 introduced the element of the re-occurrence of IT control material weaknesses over time into this comparative study. Sub-sample B was selected from the collected dataset and applied against an additional 5th criterion identified below in Table 7 as Consecutive Annual Occurrence of IT Control Material Weakness. The design of the study and the application of the 5th criterion resulted in the data of 266 SEC Registrants available for testing.

Grouping Criteria: Sub-Sample B
1. Annual 10K Report filed between the Years of 2013-2018.
2. Standard Industrial Code (SIC)
3. Total Amount of Annual Earnings
4. Occurrence of an IT Control Material Weakness
5. Consecutive Annual Occurrence of IT Control Material Weakness (t and (t+1)) (Used to test H3 only)

Table 7. Categorical Criteria used to establish Homogenous Pairs for Sub-Sample B

Validity and Reliability. The collected data has a high level of reliability due to the capabilities provided by AuditAnalytics to allow the access and transfer of the publicly available data of SEC Registrants. The multiple levels of certification of the 10K financial statements along with the ability to cross-reference the data with multiple systems such as EDGAR, AuditAnalytics, and the official websites of SEC Registrants improves the reliability of the collected data and the results of the statistical tests. The inability to manipulate the independent variables during testing reduced the internal validity of the study. In addition, the natural assignment among the two compared groups did not allow for the application of random sampling. The inability to randomize the samples reduced the validity of the results. The highest level of homogeny between the matched pair samples was necessary in order to improve the validity and reliability of the results. A series of retesting was performed following the same procedures in order to ensure the results were consistent and reliable.

Results

The following results of data collected from Sub-Sample A and Sub-Sample B derive from the SPSS output of frequency statistics tests, Descriptive Statistics tests, and pair sample *t*-tests. The frequency statistics were used to provide detailed statistical analysis about the number of times certain events occurred according to the data. The descriptive statistics were used to provide a detailed analysis of the various standard statistical features that make up the data. The matched-pair samples *t*-tests or paired sampled *t*-tests were used to test the hypotheses and answer the research questions.

Frequency Statistics (Group 1 - Sub-Sample A)				
(*** trillions)		Group 1 Earnings	Group 1 OMV1	Group 1 (μ_1) Tobin's Q
N	Valid	156	156	156
	Missing	0	0	0
Mean		$124,233,998	$4,014,351,206	5.360
Std. Error of Mean		$71,688,304	$1,311,917,475	1.422
Median		($221,762)	$563,474,038	2.196
Mode		-$715,000,000[a]	$3,140,610[a]	-60.64a
Std. Deviation		$895,386,625	$16,385,844,010	17.756
Variance		***$8,017,172,083.4	***$268,495,883,921.3	315.290
Skewness		10.23	9.09	4.051
Std. Error of Skewness		0.19	0.19	0.194
Kurtosis		116.39	95.6	28.747
Std. Error of Kurtosis		0.39	0.39	0.386
Range		$11,175,000,000	$183,883,813,886	204.240
Minimum		($715,000,000)	$3,140,610	-60.640
Maximum		$10,460,000,000	$183,886,954,496	143.600
Sum		$19,380,503,634	$626,238,788,196	836.210
%	25	($17,035,455)	0.799	0.8
	50	($221,762)	2.196	2.2
	75	$30,499,301	5.039	5.04
a. Multiple modes exist. The smallest value is shown				

Table 8. Frequency Statistics Group 1: Sub-Sample A: Earnings, OMV, and, Tobin's-Q

Frequency Statistics (Group 2 - Sub-Sample A)				
(*** trillions)		Group 2 Earnings	Group 2 OMV2	Group 2 (μ_2) Tobin's Q
N	Valid	156	156	156
	Missing	0	0	0
Mean		($354,550)	$1,098,012,775	1.6288
Std. Error of Mean		$16,884,290	$222,270,214	1.23984
Median		($919,000)	$246,698,144	1.659
Mode		-$848,000,000[a]	$14[a]	0
Std. Deviation		$210,884,713	$2,776,154,089	15.48559
Variance		***$44,472,362,380.8	***$7,707,031,524,300.4	239.803
Skewness		2.05	5.75	-0.933
Std. Error of Skewness		0.19	0.19	0.194
Kurtosis		17.52	38.86	10.516
Std. Error of Kurtosis		0.39	0.39	0.386
Range		$2,181,000,000	$23,268,669,426	149.7
Minimum		($848,000,000)	$14	-83.12
Maximum		$1,333,000,000	$23,268,669,440	66.58
Sum		($55,309,830)	$171,289,992,835	254.1
%	25	($24,072,500)	-1.5614	-1.56
	50	($919,000)	1.659	1.66
	75	$18,194,750	4.6047	4.6
a. Multiple modes exist. The smallest value is shown				

Table 9. Frequency Statistics Group 2: Sub-Sample A: Earnings, OMV, and, Tobin's-Q

Frequency Statistics: Sub-Sample B				
		Group 1:Tobin's Δ (μ_1) (t-(t+1))	Group 2:Tobin's Q Δ (μ_2) (t-(t+1))	Difference between Group 1:Tobin's Q Δ (μ_1) (t-(t+1)) and Group 2:Tobin's Q Δ (μ_2) (t-(t+1))
N	Valid	133	133	133
	Missing	0	0	0
Mean		27.99	-12.37	40.35
Std. Error of Mean		13.75	7.15	14.61
Median		0.00	-0.06	0.20
Mode		-62.97a	-838.27a	-$29.76a
Std. Deviation		158.60	82.46	168.48
Variance		25152.74	6799.08	28386.21
Skewness		6.56	-8.26	5.23
Std. Error of Skewness		0.21	0.21	0.21
Kurtosis		44.38	78.58	28.26
Std. Error of Kurtosis		0.42	0.42	0.42
Range		1362.26	943.75	1223.58
Minimum		-62.97	-838.27	-29.76
Maximum		1299.29	105.48	1193.81
Sum		3722.27	-1644.84	5367.11
Percentiles	25	-0.73	-1.30	-1.31
	50	0.00	-0.06	0.20
	75	1.19	1.27	6.28
a. Multiple modes exist. The smallest value is shown				

Table 10. Frequency Statistics: Sub-Sample B: Tobin's Q Δ (μ) (t-(t+1))

Descriptive Statistics: Sub-Sample A							
(* millions) (**billions)	N	Range	Minimum	Maximum	Mean		Std. Deviation
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic
Group 1 Earnings	156	*$11,175.0	*-$715.0	*$10,460.0	*$124.2	*$71.7	*$895.4
Group 1 OMV1	156	*$183,883.8	*$3.1	*$183,887.0	*$4,014.4	*$1,311.9	*$16,385.8
Group 1 (μ_1) Tobin's Q	156	204.24	-60.64	143.6	5.3603	1.42165	17.75641
Group 2 Earnings	156	*$2,181.0	*-$848.0	*$1,333.0	*-$0.4	*$16.9	*$210.9
Group 2 OMV2	156	*$23,268.7	*$.000014	*$23,268.7	*$1,098.0	*$222.3	*$2,776.2
Group 2 (μ_2) Tobin's Q	156	149.7	-83.12	66.58	1.6288	1.23984	15.48559

Table 11. Descriptive Statistics: Sub-Sample A: Earnings, OMV, and Tobin's-Q.

Descriptive Statistics Continued: Sub-Sample A						
(* millions) (**billions)	N	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Group 1 Earnings	156	**$801,717,208.3	10.231	0.194	116.386	0.386
Group 1 OMV1	156	**$268,495,883,921.3	9.085	0.194	95.597	0.386
Group 1 (μ_1) Tobin's Q	156	315.29	4.051	0.194	28.747	0.386
Group 2 Earnings	156	**$44,472,362.4	2.049	0.194	17.517	0.386
Group 2 OMV2	156	**$7,707,031,524.3	5.748	0.194	38.862	0.386
Group 2 (μ_2) Tobin's Q	156	239.80	-0.933	0.194	10.516	0.386

Table 12. Descriptive Statistics: Sub-Sample A: Earnings, OMV, and Tobin's-Q.

Descriptive Statistics: Sub-Sample B							
(* millions) (**billions)	N	Range	Minimum	Maximum	Mean		Std. Deviation
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic
Group 1 Earnings($) (t)	133	**$408.2	**-$140.2	**$268.0	**$0.3	**$2.6	**$30.0
Group 1 (μ_1) (t)	133	$2,200.01	-$67.63	$2,132.38	$28.46	$17.78	$205.05
Group 1: Stock Price (t)	133	$505.60	$0.02	$505.62	$26.47	$4.50	$51.90
Group 1 Earnings($) (t+1)	133	**$343.3	**-$196.1	**$147.2	**$2.7	**$2.3	**$25.9
Group 1 (μ_1) (t+1)	133	$2,457.02	-$1,205.08	$1,251.94	$0.48	$13.31	$153.54
Group 1: Stock Price (t+1)	133	$524.20	$0.00	$524.20	$29.82	$5.05	$58.27
Group 1: Δ (μ_1) (t-(t+1))	133	$1,362.26	-$62.97	$1,299.29	$27.99	$13.75	$158.60
Group 1: Δ Stock Price (t-(t+1))	133	$124.54	-$105.85	$18.69	-$3.35	$1.14	$13.12
Group 2 Earnings($) (t)	133	**$218.1	**-$84.8	**$133.3	**-$0.2	**$1.7	**$19.8
Group 2 Tobin's Q (μ_2) (t)	133	$320.81	-$254.23	$66.58	-$2.57	$2.54	$29.24
Group 2: Stock Price (t)	133	$178.94	$0.06	$179.00	$20.17	$2.37	$27.33
Group 2 Earnings($) (t+1)	133	**$100.1	**-$26.4	**$73.6	**$3.1	**$1.2	**$13.3
Group 2 Tobin's Q (t+1)	133	$918.86	-$61.14	$857.72	$9.79	$6.75	$77.80
Group 2: Stock Price (t+1)	133	$191.58	$0.02	$191.60	$20.63	$2.61	$30.15
Group 2: Δ Stock Price (t-(t+1))	133	$53.74	-$30.00	$23.74	-$0.46	$0.71	$8.20
Group 2:Tobin's Q Δ (μ_2) (t-(t+1))	133	$943.75	-$838.27	$105.48	-$12.37	$7.15	$82.46
Difference between Group 1:Tobin's Q Δ (μ_2) (t-(t+1)) and Group 2:Tobin's Q Δ (μ_2) (t-(t+1))	133	$1,223.58	-$29.76	$1,193.81	$40.35	$14.61	$168.48
Difference between Group 1: Δ Stock Price (t-(t+1)) and Group 2: Δ Stock Price (t-(t+1))	133	$107.74	-$23.47	$84.27	$1.77	$1.06	$12.21

Table 13. Descriptive Statistics: Sub-Sample B: Earnings, OMV, and Tobin's-Q

Descriptive Statistics Continued: Sub-Sample B						
(* millions) (**billions)	N	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Group 1 Earnings($) (t)	133	**$9,013,917,569.0	4.648	0.21	51.714	0.417
Group 1 (μ_1) (t)	133	$42,045.09	9.204	0.21	89.321	0.417
Group 1: Stock Price (t)	133	$2,693.86	6.88	0.21	57.632	0.417
Group 1 Earnings($) (t+1)	133	**$6,733,630,316.5	-1.894	0.21	33.767	0.417
Group 1 (μ_1) (t+1)	133	$23,573.09	0.414	0.21	62.113	0.417
Group 1: Stock Price (t+1)	133	$3,395.47	6.106	0.21	44.667	0.417
Group 1: Δ (μ_1) (t-(t+1))	133	$25,152.74	6.557	0.21	44.38	0.417
Group 1: Δ Stock Price (t-(t+1))	133	$172.21	-4.133	0.21	28.671	0.417
Group 2 Earnings($) (t)	133	**$3,921,746,247.5	1.814	0.21	19.523	0.417
Group 2 Tobin's Q (μ_2) (t)	133	$854.75	-5.633	0.21	44	0.417
Group 2: Stock Price (t)	133	$746.95	3.46	0.21	15.124	0.417
Group 2 Earnings($) (t+1)	133	**$1,759,484,014.9	2.664	0.21	10.433	0.417
Group 2 Tobin's Q (t+1)	133	$6,052.87	10.104	0.21	109.214	0.417
Group 2: Stock Price (t+1)	133	$909.25	3.499	0.21	15.064	0.417
Group 2: Δ Stock Price (t-(t+1))	133	$67.30	-0.102	0.21	2.381	0.417
Group 2:Tobin's Q Δ (μ_2) (t-(t+1))	133	$6,799.08	-8.26	0.21	78.581	0.417
Difference between Group 1:Tobin's Q Δ (μ_2) (t-(t+1)) and Group 2:Tobin's Q Δ (μ_2) (t-(t+1))	133	$28,386.21	5.225	0.21	28.255	0.417
Difference between Group 1: Δ Stock Price (t-(t+1)) and Group 2: Δ Stock Price (t-(t+1))	133	$149.15	2.846	0.21	16.558	0.417

Table 14. Descriptive Statistics Continued: Sub-Sample B

Paired Samples Correlations				
		N	Correlation	Sig.
Pair 1	Group 1 (μ_1) Tobin's Q & Group 2 (μ_2) Tobin's Q	156	0.102	0.203
Pair 2	Group 1 OMV1 & Group 2 OMV2	156	0.246	0.002
Pair 3	Group 1: Tobin's Q Δ (μ_1) (t-(t+1)) & Group 2:Tobin's Q Δ (μ_2) (t-(t+1))	133	0.136	0.118

Table 15. Paired Samples Correlations *t*-tests

Paired Samples Tests									
(* millions) (**billions)		Paired Differences					t	df	Sig. (2-tailed)
					95% Confidence Interval of the Difference				
		Mean	Std. Deviation	Std. Error Mean	Lower	Upper			
Pair 1	Group 1 (μ_1) Tobin's Q - Group 2 (μ_2) Tobin's Q	3.7315	22.3330	1.78807	0.1994	7.2636	2.087	155	0.039
Pair 2	Group 1 OMV1 - Group 2 OMV2	*$2,916.3	*$15,932.1	*$1,275.6	*$396.5	*$5,436.1	2.286	155	0.024
Pair 3	Group 1: Tobin's Q Δ (μ_1) (t-(t+1)) - Group 2:Tobin's Q Δ (μ_2) (t-(t+1))	40.3542	168.4821	14.60925	11.4557	69.2528	2.762	132	.007

Table 16. Paired Samples *t*-tests

Research Question 1/Hypothesis. RQ1. What are the differences in financial performance between U.S. publicly traded businesses that report various types of IT control material weaknesses and U.S. publicly traded businesses that do not report IT control material weaknesses? H1: There is no significant difference in Tobin’s Q (Q-Ratio) (y) between U.S. publicly traded businesses that report various types of IT control material weaknesses (x) and U.S. publicly traded businesses that do not report IT control material weaknesses (x). H10: $\mu_1 = \mu_2$. H1a: There is a significant difference in Tobin’s Q (Q-Ratio) (y) between U.S. publicly traded businesses that report various types of IT control material weaknesses (x) and U.S. publicly traded businesses that do not report IT control material weaknesses (x). H1a: $\mu_1 \neq \mu_2$.

RQ1-H1. Paired Samples Test									
(* millions) (**billions)		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	Group 1 (μ_1) Tobin's Q - Group 2 (μ_2) Tobin's Q	3.73151	22.33299	1.78807	0.19938	7.26364	2.087		0.039

Table 17. Results of Paired Sample *t*-test of H1

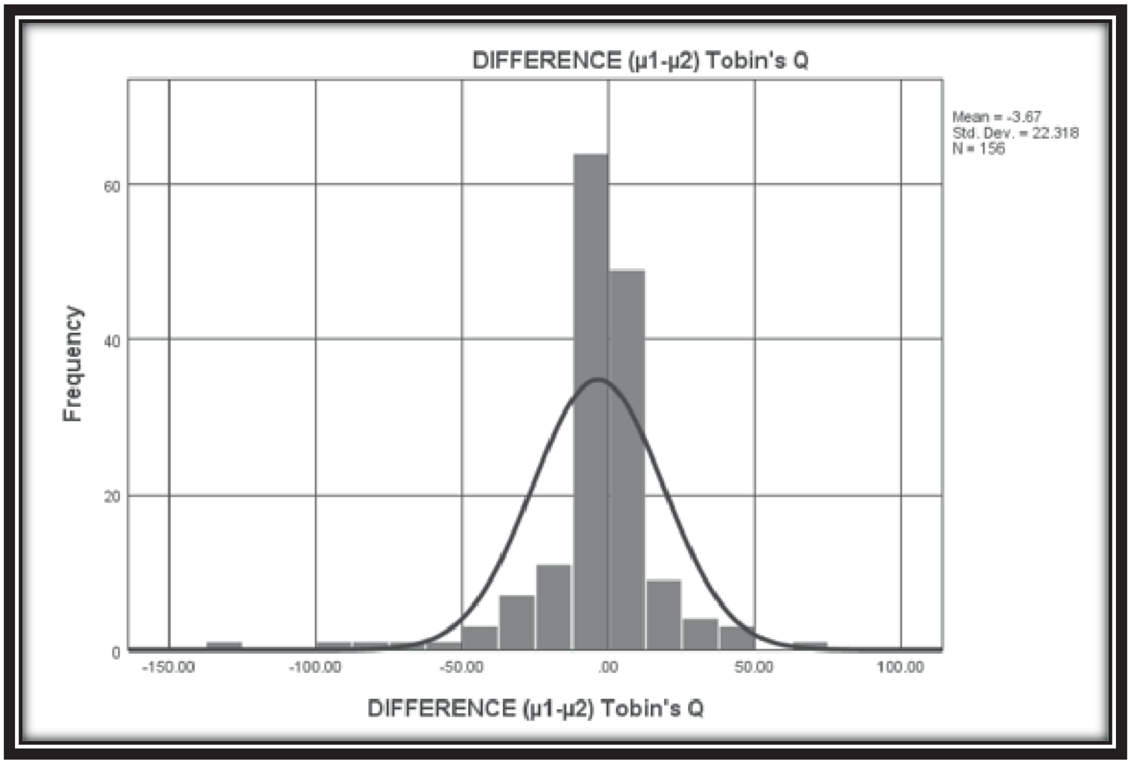


Figure 7. Histogram of Group 1 (μ1) Tobin's Q - Group 2 (μ2) Tobin's Q

Research Question 2/Hypothesis. RQ2. What are the differences in market valuation between U.S. publicly traded businesses that report various types of IT control material weaknesses and U.S. publicly traded businesses that do not report IT control material weaknesses? H2: There is no significant difference in the Open Market Value (OMV) (y) between U.S. publicly traded businesses that report various types of IT control material weaknesses (x) and U.S. publicly traded businesses that do not report various types of IT control material weaknesses (x). $H2_0$: $\mu_1 = \mu_2$. $H2_a$: There is a significant difference in the Open Market Value (OMV) (y) between U.S. publicly traded businesses that report various types of IT control material weaknesses (x) and U.S. publicly traded businesses that do not report various types of IT control material weaknesses (x). H2a: $\mu_1 \neq \mu_2$.

RQ2-H2. Paired Samples Test									
(* millions) (**billions)		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	Group 1 OMV1 - Group 2 OMV2	*$2,916.3	*$15,932.1	*$1,275.6	*$396.5	*$5,436.1	2.286	155	0.024

Table 18. Results of Paired Sample *t*-test of H2

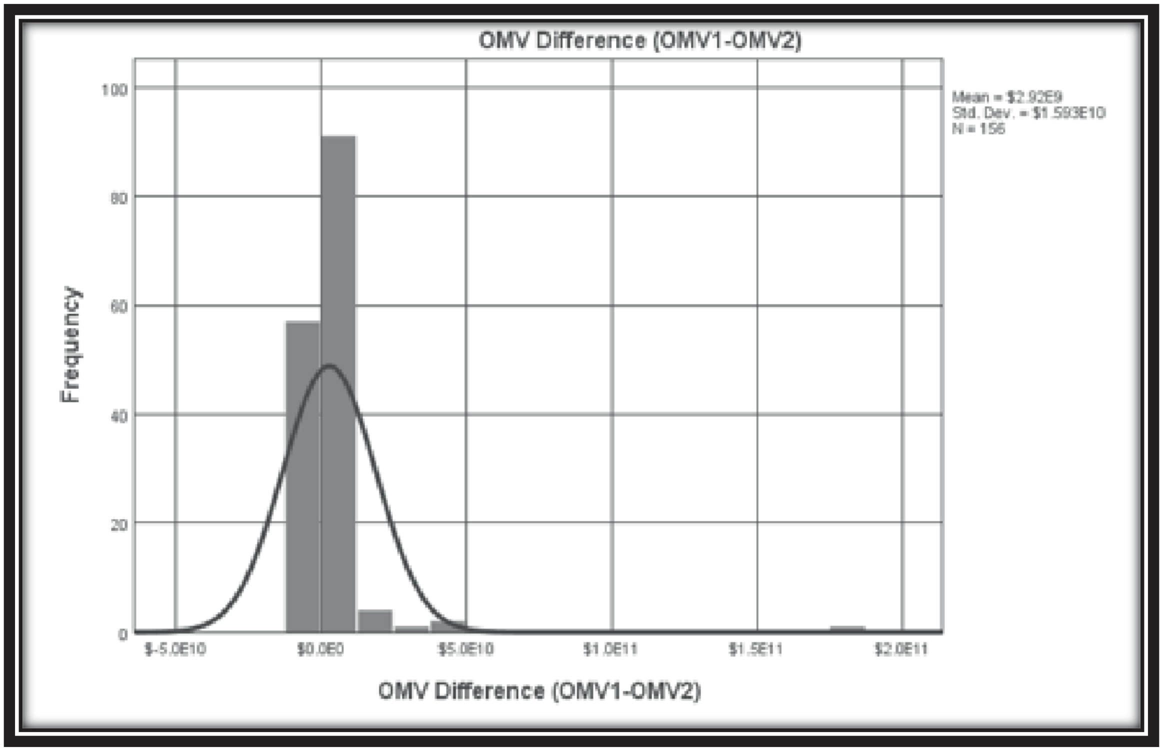


Figure 8. Histogram OMV Difference (OMV1-OMV2)

Research Question 3/Hypothesis. RQ3. What are the differences in financial performance between U.S. publicly traded business that resolved a various type of IT control material weakness in a given year and did not report any in the following year and U.S. publicly traded business that did not report an IT control material weakness in the same given year or the following year? There is no significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded business that resolved a various type of IT control material weakness (*x*) in a given year (t) and did not report any in the following year (t+1) and U.S. publicly traded business that did not report a various type of IT control material weakness (*x*) in the same given year (t) or the following year (t+1) ($H3_0$: $\mu_1 = \mu_{2.}$ H3a). There is a significant difference in Tobin's Q (Q-Ratio) (y) between U.S. publicly traded business that resolved a various type of IT control material weakness (x) in a given year (t) and did not report any in the following year (t+1) and U.S. publicly traded business that did not report a various type of IT control material weakness (x) in the same given year (t) or the following year (t+1) ($H3_a$: $\mu_1 \neq \mu_2$).

RQ3-H3. Paired Samples Test									
		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 3	Group 1:Tobin's Q Δ (μ_1) (t-(t+1)) - Group 2:Tobin's Q Δ (μ_2) (t-(t+1))	40.354	168.482	14.609	11.456	69.253	2.76	132	.007

Table 19. Results of Paired Sample *t*-test of H3

Figure 9 is a visual representation of the negative skewness that exists among the results of the Paired Samples *t*-test of H3. The negative slope shows more larger scores on the left side of and lower scores on the right side within the histogram.

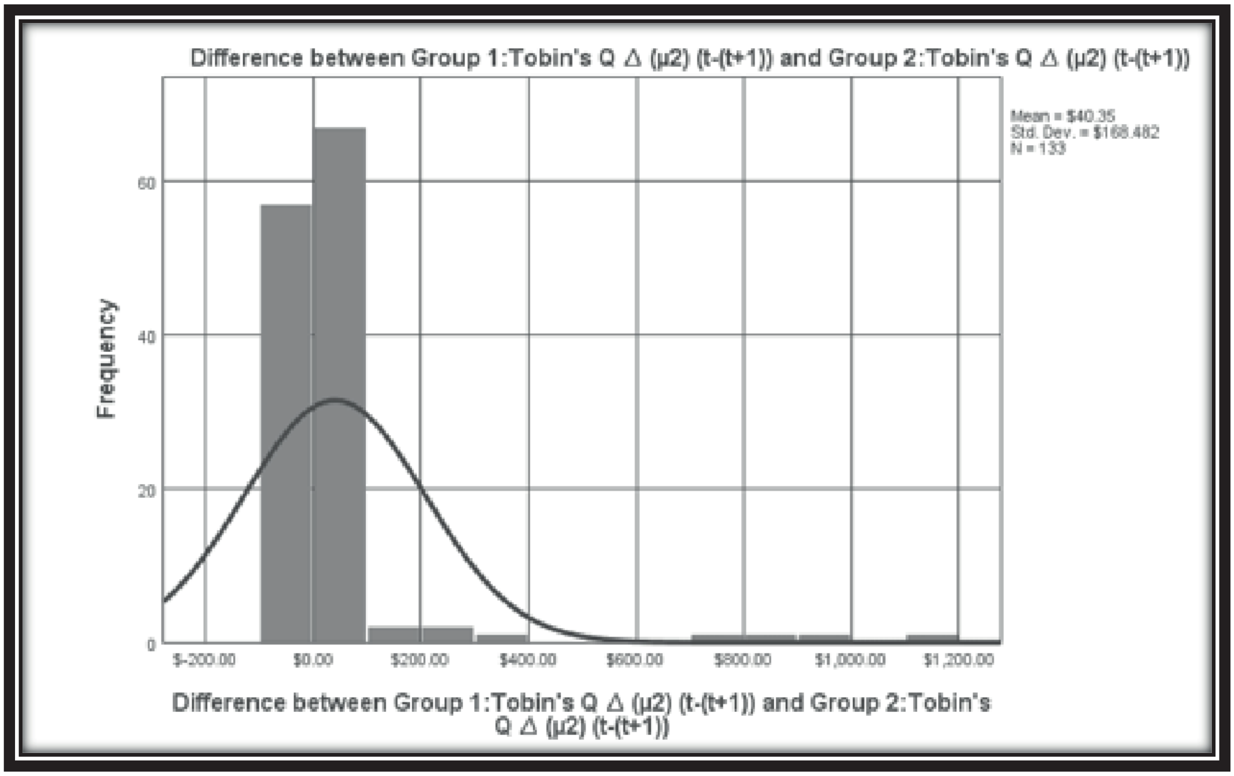
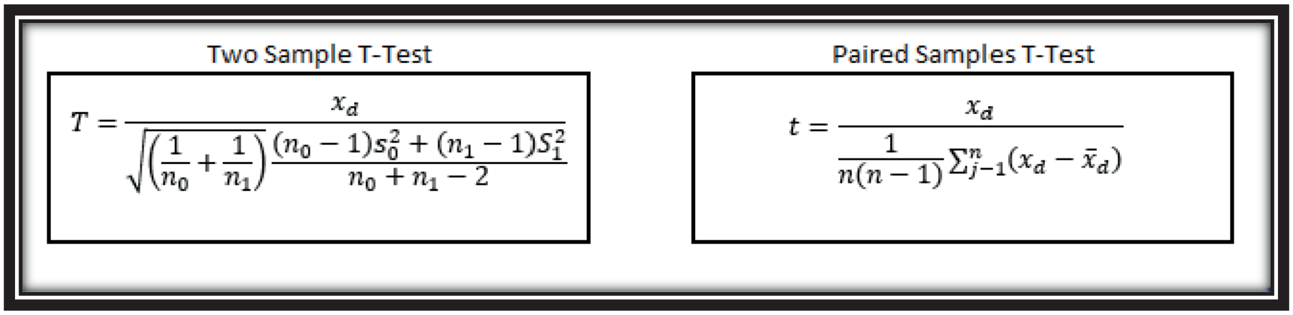


Figure 9. Histogram of ((Group 1: Tobin's Q Δ (μ_1) (t-(t+1))) – (Group 2: Tobin's Q Δ (μ_2) (t-(t+1))))

Evaluation of the Findings

The purpose of this research study was to measure the differences in the effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses. The theoretical framework of this study includes the theories of IT Governance, Accounting, Audit, and Internal Controls. A will be used to assist in closing the gap in internal controls and IT governance literature (Ragothaman & Cornelsen, 2017; Rubino & Vitolla, 2014; Weng et al., 2015). This quantitative study uses a retrospective causal-comparative research design and paired sampled *t*-tests to measure the differences between the OMV and Tobin's Q of SEC Registrant from Group 1 and Group 2 (Apuke, 2017). This study supports the findings of previous studies, such as those conducted by Kuhn et al. (2013) and Ragothaman & Cornelsen (2017). The studies of Kuhn et al. (2013) and Ragothaman & Cornelsen (2017) have shown evidence that suggests there is a negative impact that IT control material weaknesses can have on the financial performance of publicly traded U.S. corporations. A causal-comparative research design along with frequency tests, descriptive tests, and matched-pair sample tests were used to gain a better understating of the differences between the independent variables of various types of reported IT control material weaknesses and both the financial and market performance of SEC Registrants. The following section provides an evaluation of the measurements of Tobin's Q and OMV (Ragothaman & Cornelsen, 2017).

Frequency Statistics. Tables 8 and Table 9 display the frequency statistics of Group 1 and Group 2 of Sub-Sample A. The sample size of this sub-sample is 312 SEC Registrants with 156 matched pairs. The variables that have been included in this analysis are the earnings, OMV, and Tobin's Q. The mean comparison between Group 1 and Group 2 of Sub-Sample A reflects Group 1 earnings as $124,233,998 and Group 2 earnings as ($354,550). The mean OMV of Group 1 is $4,014,351,206 compared to the mean of Group 2 which is $1,098,012,775. When comparing the mean Tobin's Q ratios, Group 1 reflects a ratio of 5.360, and Group 2 reflects a mean ratio of 1.628. An analysis of frequency statistics reflects preliminary evidence that is consistent with previous studies such as those conducted by Kuhn et al. (2013) and Ragothaman & Cornelsen (2017). These figures are a holistic comparison of the two groups rather than the results of the matched-pair tests that were conducted. The 2-sample *t*-test has been used in previous studies to measure the effect size and observed differences between similar samples drawn from the population of SEC registrants. Figure 7 displays a comparison between the formulas used when conducting Two Sample *t*-test and Paired Samples *t*-tests. The Two-Sample *t*-test is always used when the samples are statistically independent. The paired samples *t*-test is used when the subject data is matched with slight technical differences between the pairs. The paired samples *t*-test will always reflect a normal distribution between each pair.



Two Sample T-Test

$$T = \frac{x_d}{\sqrt{\left(\frac{1}{n_0}+\frac{1}{n_1}\right)\frac{(n_0-1)s_0^2+(n_1-1)S_1^2}{n_0+n_1-2}}}$$

Paired Samples T-Test

$$t = \frac{x_d}{\frac{1}{n(n-1)}\sum_{j-1}^{n}(x_d-\bar{x}_d)}$$

Figure 10. Formulas for conducting 2-Sample Tests and Paired Samples T-Tests

The results displayed in table 10 reflect the frequency statistics of Group z 2 of Sub-Sample B (n = 133 matched pairs). This data shows the mean difference in mean Tobin's Q ratio of 27.99 among SEC Registrants from Group 1 which did not report an IT control material weakness for two consecutive years ((t)(t+1)) and a mean difference in mean Tobin's Q ratio of -12.37 for SEC Registrants that reported an IT control material weakness in a given year (t) but not in year (t+1). Analyzing the results using these frequencies statistics reflects a comparison of the independent mean of each group. This method of analysis can be used to identify the results from a Two-Sample *t*-test. Table 10 also shows the difference in mean Tobin's Q scores of all matched pairs. The resulting difference in the mean between the matched pairs consisting of the data from one subject from Group 1 and one from Group 2 is 40.35.

Descriptive Statistics. Tables 11 and 12 contain the results of the descriptive statistics of Sub-Sample A. Sub-Sample A shows that Group 1 has a larger mean of earnings, OMV, and Tobin's Q than Group 2. Group 1 reports mean earnings of $124.2 million compared to the mean of Group 2 with mean earnings of $-0.4 million. Group 1 shows a mean OMV of $4,014.4 million, and Group 2 shows $$1,098.0 million. The mean Tobin's Q of Group 1 is 5.36 compared to Group 2, with a mean Tobin's Q ratio of 1.63.

Tables 13 and 14 reflect the descriptive statistics of Sub-Sample B, which at year t Group 1 reflects a higher mean of earnings than Group 2 at $0.3 billion compared to -$0.2

billion. In year t+1, Group 2 shows a higher mean of earnings at $3.1 billion compared to Group 1 with a mean of $2.7. The mean Tobin’s Q of Group 1 at year t is 28.46 and Group 2 shows -2.57. In year t+1, Group 2 shows a higher mean Tobin’s Q than Group 1 with 9.79 compared to the mean of 0.48 of Group 1.

Correlation. Table 15 is the paired samples correlations *t*-tests of Sub-Sample A and Sub-Sample B. The correlation score between Group 1 and 2 of Sub-Sample A is .102 with a p-value of .203. The OMV correlation between these same subjects is .246 with a p-value of .002. The correlation between change in the mean of Tobin’s Q between year t and year t+1 of Group 1 and Group 2 of Sub-Sample B is .136 with a p-value of .118.

Paired-Samples t-tests. The results of three paired samples *t*-tests used to test each of the hypotheses are found in table 16. Test 1 encompasses the differences in the mean Tobin’s Q of Group 1 and Group 2 of Sub-Sample A, which is 3.73, with a standard deviation of 22.33 and a *t*-value of 2.087. The p-value for this test is .039.

Test 2 consists of the difference in mean OMV of Group 1 and Group 2 of Sub-Sample A. The mean is $2,916.3 million, with a standard deviation of $15,932.1 million and a *t*-value of 2.286. The p-value for this test is .024.

Test 3 results shown in table 16 reflects the difference in mean Tobin’s Q from Group 1 and Group 2 of Sub-Sample B ((Group 1: Tobin's Q Δ (μ_1) (t-(t+1))) – (Group 2: Tobin’s Q Δ (μ_2) (t-(t+1)))). The mean Tobin’s Q ratio of this data is 40.35, with a standard deviation of 168.48 and a *t*-value of 2.762. The p-value for this test is .007.

Summary

The research questions are developed to inquire about the difference in the level of financial performance using Tobin’s Q and Open Market Value (OMV) between public businesses that experience various types of IT control material weaknesses and public businesses that do not experience IT control material weaknesses. A non-random quota sampling method is used to select n = 312 for sub-sample A and n = 266 for sub-sample B from the target population using matched-pair *t*-tests to statistical measure the differences between the mean of Group 1 (μ_1) with the mean of Group 2 (μ_2). This research is not intended to recreate prior studies reflecting the holistic negative impact of IT controls material weaknesses on the financial performance of public businesses. Instead, this research focused on measuring the extent of the negative impacts that individual types of IT control material weaknesses may have on the financial performance of public businesses. The results of this research have the potential to drastically change how stakeholders perceive and react to IT control material weaknesses that are reported by public businesses.

Chapter 5: Implications, Recommendations, and Conclusions

The purpose of this quantitative causal-comparative research study was to identify the differences that exist in the effects of various types of IT control material weaknesses on the financial performance of publicly traded U.S. businesses. The basis for conducting this research stems from the research conducted by Kuhn et al. (2013), which shows that companies that report both IT control material weaknesses and Non-IT control material weaknesses experience lower levels of financial performance. Also, this research was intended to build on the work of Ragothaman & Cornelsen (2017), which describes the negative relationship between internal controls material weaknesses and gross margin. These previous studies have both shown evidence of the negative impact that reported IT control material weaknesses have on the financial performance of publicly traded U.S. corporations. This study is used to describe in further detail the extent of the adverse effects on the financial performance of publicly traded corporations that are possibly caused by individual types of IT control material weaknesses. In this chapter, the implication of this study will be addressed along with the recommendation for future research related to the constructs described in this study. In conclusion, a summary of the main points and findings of this study will be described and related to the theoretical framework of IT Governance Theory, Accounting Theory, Audit Theory, and Internal Control Theory found in the current literature.

Implications

The results of the paired sample *t*-tests provide sufficient evidence to support the purpose of this study and answer each of the three research questions. The implications of the statistical *t*-tests enable an avenue to accurately test each of the three hypotheses and determine the level of statistical significance between variables. In the following sections, the implications of each statistical *t*-tests will be applied to each particular research question and hypotheses.

Research Question 1/Hypothesis 1. RQ1 addressed the differences in financial performance between U.S. publicly traded businesses that report various types of IT control material weaknesses (Group 2) and U.S. publicly traded businesses that do not report IT control material weaknesses (Group 1). The first paired sample *t*-test identified the differences in the mean Tobin's Q of Group 1 and Group 2 of Sub-Sample A as 3.73 with a standard deviation of 22.33 and a *t*-value of 2.087. The p-value was found to be statistically significant, with a score of .039. The α for this study is .05 with a confidence level of .95. Since $p < .05$, the null hypothesis is rejected, and the alternative hypotheses are accepted. The H1: There is no significant difference in Tobin's Q (Q-Ratio) (y) between U.S. publicly traded businesses that report various types of IT control material weaknesses (x) and U.S. publicly traded businesses that do not report IT control material weaknesses (x). H10: $\mu_1 = \mu_2$. H1a: There is a statistically significant difference in Tobin's Q (Q-Ratio) (y) between U.S. publicly traded businesses that report various types of IT control material weaknesses (x) and U.S. publicly traded businesses that do not report IT control material weaknesses (x). H1a: $\mu_1 \neq \mu_2$.

Research Question 2/Hypothesis 2. RQ2 was used to address the question of the differences in market valuation between U.S. publicly traded businesses that report various types of IT control material weaknesses (Group 2) and U.S. publicly traded businesses that do not report IT control material weaknesses (Group 1). The results of the statistical paired sample *t*-test provide evidence that the mean OMV of Group 1 is $2,916.3 million higher than Group 2 of Sub-Sample A, with is a standard deviation of $15,932.1 million and a *t*-value of 2.286. This paired sample *t*-test provides evidence for statistical significance with a resulting p-value of

.024. Since $p <$ the α of .05 the null hypothesis is rejected (H2: There is no significant difference in the Open Market Value (OMV) (y) between U.S. publicly traded businesses that report various types of IT control material weaknesses (x) and U.S. publicly traded businesses that do not report various types of IT control material weaknesses (x). $H2_0$: $\mu_1 = \mu_2$.) and the alternate hypothesis is accepted ($H2_a$: There is a significant difference in the Open Market Value (OMV) (y) between U.S. publicly traded businesses that report various types of IT control material weaknesses (x) and U.S. publicly traded businesses that do not report various types of IT control material weaknesses (x). H2a: $\mu_1 \neq \mu_2$.).

Research Question 3/Hypothesis 3. RQ3 branched out from RQ1 and RQ2 and attempted to explore the impacts of IT control material weaknesses on U.S. publicly traded businesses over time. RQ3 was used to address the differences in financial performance between U.S. publicly traded business that resolved a various type of IT control material weakness in a given year and did not report any in the following year (Group 2) and U.S. publicly traded business that did not report an IT control material weakness in the same given year or the following year (Group 1). The statistical *t*-test presents evidence that there is a difference in mean Tobin's Q between Group 1 and Group 2 of Sub-Sample B ((Group 1: Tobin's Q Δ (μ_1) (t-(t+1))) – (Group 2: Tobin's Q Δ (μ_2) (t-(t+1)))) of 40.35 with a standard deviation of 168.48 and a *t*-value of 2.762. The p-value of this test was .007, which is less than the α of .05 and deemed statistically significant for this study. Therefore, the null hypothesis is rejected (There is no significant difference in Tobin's Q (Q-Ratio) (*y*) between U.S. publicly traded business that resolved a various type of IT control material weakness (*x*) in a given year (t) and did not report any in the following year (t+1) and U.S. publicly traded business that did not report a various type of IT control material weakness (*x*) in the same given year (t) or the following year (t+1)

($H3_0$: $\mu_1 = \mu_2$) and the alternate hypothesis is accepted (H3a: There is a significant difference in Tobin's Q (Q-Ratio) (y) between U.S. publicly traded business that resolved a various type of IT control material weakness (x) in a given year (t) and did not report any in the following year (t+1) and U.S. publicly traded business that did not report a various type of IT control material weakness (x) in the same given year (t) or the following year (t+1). $H3_a$: $\mu_1 \neq \mu_2$.

Recommendations for Practice

The results of this study are consistent with the themes found within the literature of internal controls material weaknesses. Studies such as those conducted by Kuhn et al. (2013) and Ragothaman & Cornelsen (2017) show evidence that supports the theory that companies that experience internal control material weaknesses experience lower levels of financial performance. The three paired samples *t*-tests provide evidence which contributes to the literature and shows that SEC registrants that reported an IT control material weakness would experience a lower level of financial performance. In most cases, the lower level of financial performance could be measured using Tobin's Q ratio and OMV. Also, the results of this study provide evidence which suggests SEC Registrants that experience an IT control material weakness and can resolve it in one year will be outperformed financially by SEC Registrants that do not experience an IT control material weakness. These results suggest a lasting impact that IT control material weaknesses have on business' financial performance even a year after they were resolved.

Management. SOX Section 404 clearly states the requirement of SEC Registrants to provide an assessment of their internal control material weaknesses. Managers must not hesitate to honestly report an accurate depiction of the status of their internal control material weaknesses. Management can use the findings of this study to more accurately prepare for the negative financial impacts that will likely occur in the event of an IT control material weakness. In addition, this study provides a further understanding that IT control material weakness can negatively impact a business's financial performance for up to a year after they are resolved.

Investors. Investors can apply the findings of this study to make better investments decision. The ability to more accurately forecast a business' financial performance allows an investor to make better decisions. The findings of this study provide evidence which shows not only the negative impacts of IT control material weaknesses but also that IT control material weaknesses can negatively impact financial performance for up to a year after they are experienced.

Recommendations for Future Research

There are several areas that this research can be used as a basis to branch out in order to conduct future research. One area of future research is replicating this study and replacing the variable IT control material weaknesses with one or more of the other 21 types of internal control material weaknesses. The literature contains evidence which suggests there is a negative impact that internal control material weaknesses have on financial performance. Research is needed to understand further the extent to which individual types of internal control material weaknesses impact Tobin's Q and OMV of SEC Registrants.

An area for future research can also be found in the length of time that IT control material weaknesses impact the financial performance of firms. This study provides a measurement and evidence which supports a negative impact on financial performance for the extent of a year. Research is needed to measure the extent of the negative impacts of overtime using Tobin's Q or other cumulative measures which display the overall financial setbacks.

Future research is also needed to contribute to the literature of internal controls and accounting by testing the relationship between SEC Registrants reporting IT controls material weaknesses along with additional internal control material weaknesses. Many SEC Registrants are medium to large corporations that rely on ERP and AIS. Computers and technology are the corps framework of many of these companies' business processes. If businesses have issues with their IT controls, it may be highly possible they will experience many other breakdowns in different types of internal controls. A comparison could be made between businesses that experience IT control material weaknesses plus Non-IT control material weaknesses and those that only experience Non-IT control material weaknesses.

Conclusions

This quantitative study is intended to identify the differences in the impact of various types of IT control material weaknesses on the financial performance of SEC Registrants using a retrospective causal-comparative research design. The framework of this study was used to test the impact of various types of IT control material weaknesses on the Tobin's Q and OMV of SEC Registrants. This research builds on the findings of Kuhn et al. (2013) and Ragothaman & Cornelsen (2017). These previous studies have both shown evidence of the negative impact that IT control weaknesses have on the financial performance of publicly traded U.S. corporations. The significance of this study is the ability to close the gap in internal controls, and IT governance literature through a better understanding of the impacts of various types of IT control material weaknesses on the financial performance of SEC Registrants. The archival data collection method was used to retrieve private data from AuditAnalytics database of public information on SEC Registrants. The matched-pair non-random sampling quota sampling method was used to select n = 312 for sub-sample A and n = 266 for sub-sample B from the target population. Also, paired-samples *t*-tests were conducted to analyze the differences in the financial performance of U.S. public corporations that report various types of IT control material weaknesses. The results of three paired samples *t*-tests used to test each of the hypotheses show the differences in the mean Tobin's Q of Group 1 and Group 2 of Sub-Sample A is 3.73, standard deviation of 22.33, *t*-value of 2.087 and a p-value of .039. Test 2 found the difference in mean OMV of Group 1, and Group 2 of Sub-Sample A was $2,916.3 million, standard deviation of $15,932.1 million, *t*-value of 2.286, and p-value of .024. Test 3 found the difference in mean Tobin's Q of Group 1 and Group 2 of Sub-Sample B was 40.35, a standard deviation of 168.48, a *t*-value of 2.762, and p-value of .007. The results of all three paired sample *t*-tests were statistically significant to .05 level. The findings of this study have the potential to change how managers and investors strategically react to IT control material weaknesses.

References

ACFE. (n.d.). Report to the nations on occupational fraud and abuse 2014 global fraud study. Association of Certified Fraud Examiners. Retrieved from https://www.acfe.com/rttn-detection.aspx

Agustiningsih, S., Murni, S., & Putri, G. A. (2017). Audit findings, local government characteristics, and local government financial statement disclosure. *Review of Integrative Business and Economics Research, 6*(3), 179-187. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1918327103?accountid=28180

AICPA. (n.d.). Code of professional conduct. American Institute of Certified Public Accountants. Retrieved from http://www.aicpa.org/

Adnan, M., Just, M., Baillie, L., & Kayacik, H. G. (2015). Investigating the work practices of network security professionals. *Information and Computer Security, 23*(3), 347-367. http://dx.doi.org.proxy1.ncu.edu/10.1108/internal controlsS-07-2014-0049

Apuke, O. D. (2017). Quantitative research methods a synopsis approach. *Kuwait Chapter of the Arabian Journal of Business and Management Review, 6*(11), 40-47. http://dx.doi.org.proxy1.ncu.edu/10.12816/0040336

Al-Sabaawi, M. (2015). Critical success factors for enterprise resource planning implementation. *International Journal of Advances in Engineering & Technology, 8*(4), 496-506. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1712466495?accountid=28180

AuditAnalytics. (n.d.). AuditAnalytics is a premium on-line market intelligence service available from IVES Group, Inc., a leading research provider focused on the accounting, insurance, and investment communities. For information, call (508) 476-7007, e-mail info@auditanalytics.com. Retrieved from www.auditanalytics.com

Babos, A. (2009). Recent developments of the internal control. The COSO and COCO Models. *Land Forces Academy Review, 14*(1), 74-79. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/89153320?accountid=28180

Baker, C. R., & Burlaud, A. (2015). The historical evolution from accounting theory to conceptual framework in financial standards setting. *The CPA Journal, 85*(8), 54-60. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1712288101?accountid=28180

Bawaneh, S. S. (2014). Information security for organizations and accounting information systems: A Jordan banking sector case. *International Review of Management and Business Research, 3*(2), 1174-1188. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1566650452?accountid=28180

Baranov, P. P., Shaposhnikov, A. A., Maksimova, G. V., & Fadeykina, N. V. (2017). Scientific basis of the audit theory. *Journal of Advanced Research in Law and Economics, 8*(4), 1073-1087. http://dx.doi.org.proxy1.ncu.edu/10.14505/jarle.v8.4, (26).05

Bernroider, E. W. N. (2013). Effective ERP adoption processes: The role of project activators and resource investments. *European Journal of Information Systems, 22*(2), 235-250. http://dx.doi.org.proxy1.ncu.edu/10.1057/ejis.2012

Bharaditya, I.W., Sukarsa, I. M., & Buana, P.W. (2017). Internal control improvement for creating good governance. *International Journal of Information Engineering and Electronic Business, 9*(3), 9. http://dx.doi.org.proxy1.ncu.edu/10.5815/ijieeb.2017.03.02

Bhumgara, A., & Sayyed, I. (2017). Enterprise resource planning systems. *International Journal of Advances in Engineering & Technology, 10*(2), 283-284. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1903081515?accountid=28180

Bogodistov, Y., & Wohlgemuth, V. (2017). Enterprise risk management: A capability-based perspective. *The Journal of Risk Finance, 18*(3), 234-251. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1906146458?accountid=28180

Brouard, F., Bujaki, M., Durocher, S., & Neilson, L. (2017). Professional accountants' identity formation: An integrative framework. *Journal of Business Ethics, 142*(2), 225-238. http://dx.doi.org.proxy1.ncu.edu/10.1007/s10551-016-3157-z

Brown, V. L., & Trainor, J. E. (2014). The PCAOB's proposed changes to the auditor reporting model: An in-depth overview for the classroom and beyond. Review of Business, 35(1), 59-75. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1665096304?accountid=28180

Chiu, V., Liu, Q., & Vasarhelyi, M. A. (2014). The development and intellectual structure of continuous auditing research. *Journal of Accounting Literature, 33*(1), 37-57. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1662769927?accountid=28180

Clements, C., Neill, J. D., & Wertheim, P. (2015). Multiple directorships, industry relatedness, and corporate governance effectiveness. *Corporate Governance, 15*(5), 590-606. http://dx.doi.org.proxy1.ncu.edu/10.1108/CG-05-2014-0060

Cook, J. (2015). A six-stage business continuity and disaster recovery planning cycle. *S.A.M. Advanced Management Journal, 80*(3), 23-33, 68, 2. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1725174951?accountid=28180

COSO. (n.d.). Committee of sponsoring organizations of the treadway commission. Retrieved from https://www.coso.org/Documents/COSO-ERM-Presentation-September-2017.pdf

D'Aquila, J. M., & Houmes, R. (2014). COSO's updated internal control and enterprise risk management frameworks. *The CPA Journal, 84*(5), 54-59. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1539323298?accountid=28180

Debreceny, R. S., Gray, G. L., Joeson Jun-Jin Ng, Lee, K. S., & Woon-Foong Yau. (2005). Embedded audit modules in enterprise resource planning systems: Implementation and functionality. *Journal of Information Systems, 19*(2), 7-27. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/235874266?accountid=28180

Deis, D., & Byus, K. (2016). Who audits America's local governments? government clients move downstream to regional and local audit firms. *S.A.M. Advanced Management Journal, 81*(2), 21-30,59,2. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1891259021?accountid=28180

Deng, C., Xiao, Z., & Zhou, L. (2017). Information systems and internal control: Evidence from China. *Electronic Commerce Research, 17*(3), 361-377. http://dx.doi.org.proxy1.ncu.edu/10.1007/s10660-016-9228-5

Derenyielo, B., & Joseph, E. M. (2018). Risk management and enterprise risk management in Nigeria: Implications for national development and growth. *Kuwait Chapter of the Arabian Journal of Business and Management Review, 7*(3), 29-40. http://dx.doi.org.proxy1.ncu.edu/10.12816/0048632

Dhanani, A., & Connolly, C. (2015). Non-governmental organizational accountability: Talking the talk and walking the walk? *Journal of Business Ethics, 129*(3), 613-637. http://dx.doi.org.proxy1.ncu.edu/10.1007/s10551-014-2172-1

Dogaru, O. (2015). Challenges in cyber space – threats to public order and safety. *Studii De Securitate Publica, 4*(2), 91-95. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1692022101?accountid=28180

Eaton, T. V., & Korach, S. (2016). A criminological profile of white-collar crime. *Journal of Applied Business Research, 32*(1), 129. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1778070961?accountid=28180

El-Sayed, H., & Youssef, M. (2015). Modes of mediation for conceptualizing how different roles for accountants are made present. *Qualitative Research in Accounting and Management, 12*(3), 202-229. Retrieved from http://www.emeraldinsight.com

Erickson, S., Lukes, Z., & Weber, M. (2014). Using communication theory to analyze corporate reporting strategies: A study of the health care industry. *Academy of Accounting and Financial Studies Journal, 18*(4), 4-16. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1645738669?accountid=28180

Ettish, A. A., El-Gazzar, S., & Jacob, R. A. (2017). Integrating internal control frameworks for effective corporate information technology governance. *Journal of Information Systems and Technology Management: JISTEM, 14*(3), 361-370. doi:http://dx.doi.org.proxy1.ncu.edu/10.4301/S1807-17752017000300004

Fajardo, C. L. (2016). Convergence of accounting standards worldwide - an update. *The Journal of Applied Business and Economics, 18*(6), 148-160. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1890206424?accountid=28180

Grabski, S. V., Leech, S. A., & Schmidt, P. J. (2011). A review of ERP research: A future agenda for accounting information systems. *Journal of Information Systems, 25*(1), 37-

78. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/858021950?accountid=28180

Gray, D., & Ehoff, C., Jr. (2015). Sarbanes-Oxley and Dodd-Frank: Then there was fraud. *Journal of Business & Economics Research*, 13(1), 19-n/a. Retrieved from https://search-proquest-com.proxy1.ncu.edu/docview/1655539134/6C1FAC564A064B20PQ/1?accountid=28180

Hart, C. A., & Snaddon, D. R. (2014). The organizational performance impact of ERP systems on selected companies. *South African Journal of Industrial Engineering, 25*(1), 14-28. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1536115080?accountid=28180

Jabłoński, A., Kawczyńska, M., Pietrzak, Ż., & Wnukâ-Pel, T. (2018). Desired impact of an ERP implementation on the quality of information. *Acta Universitatis Lodziensis.Folia Oeconomica,* (336), 117-135. http://dx.doi.org.proxy1.ncu.edu/10.18778/0208-6018.336.08

Jahmani, Y., Ansari, M. I., & Dowling, W. (2014). Testing for internal control weaknesses in accelerated filers. *Academy of Accounting and Financial Studies Journal, 18*(1), 97-113. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1532759747?accountid=28180

Jahmani, Y., & Dowling, W. A. (2015). Characteristics of large accelerated filers with internal control weaknesses. *Academy of Accounting and Financial Studies Journal, 19*(2), 129-141. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1750973372?accountid=28180

Johari, R., & Hussin, S. (2016). Enhancing management integrity through auditability concept: A literature review. *Humanomics, 32*(4), 516-524. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1844295894?accountid=28180

Jory, S. R., Peng, J., & Ford, C. O. (2010). The wealth effects of investing in information technology. *Review of Accounting & Finance, 9*(3), 285-305. http://dx.doi.org.proxy1.ncu.edu/10.1108/14757701011068075

Kanellou, A., & Spathis, C. (2011). Auditing in enterprise system environment: A synthesis. *Journal of Enterprise Information Management, 24*(6), 494-519. http://dx.doi.org/10.1108/17410391111166549

Kao, H., Wei, T. (2014). The effect of IFRS, information asymmetry and corporate governance on the quality of accounting information. *Asian Economic and Financial Review, 4*(2), 226-256. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1520177893?accountid=28180

Kim, G., Richardson, V. J., & Watson, M. W. (2018). IT Does Matter: The Folly of Ignoring IT Material Weaknesses. *Accounting Horizons*, *32*(2), 37. Retrieved from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=130889074&site=eds-live

Kimbell, J. P. (2017). How the SEC makes rules by proxy with Sarbanes-Oxley and COSO 2.0: A pedagogical note. *Southern Law Journal, 27*(1), 221-238. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1890508655?accountid=28180

King, D. L., & Case, C. J. (2014). Sarbanes-Oxley Act and the public company accounting oversight board’s first eleven years. *Journal of Business and Accounting, 7*(1), 11-23.

Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1630682522?accountid=28180

Kinkela, K., & Harris, P. (2013). COSO updates practice framework. *Internal Auditing, 28*(4), 35-40. Retrieved from http://search.proquest.com/docview/1431991634?accountid=12085

Kloviene, L. & Gimzauskiene, E. (2014). Development of accounting system according to an information technology. *Review of Economic Studies and Research Virgil Madgearu, 7*(2), 59-74. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1626534492?accountid=28180

Knechel, W. R. (2015). Audit research in the wake of SOX. *Managerial Auditing Journal, 30*(8), 706-726. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1712468557?accountid=28180

Konthong, K., Suwan-natada, P., & Sompong, A. (2016). The investigation of ERP and E-business effects in Thailand: A resource-based view. *Journal of Business and Retail Management Research, 11*(1) Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1864655348?accountid=28180

Kuhn, John R., Jr, & Sutton, S. G. (2006). Learning from WorldCom: Implications for fraud detection through continuous assurance. *Journal of Emerging Technologies in Accounting, 3*, 61-80. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/221166053?accountid=28180

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

Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/235942046?accountid=28180

Kuhn, John R., Jr, Ahuja, M., & Mueller, J. (2013). An examination of the relationship of IT control weakness to company financial performance and health. *International Journal of Accounting and Information Management, 21*(3), 227-240. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1412784851?accountid=28180

Kuhn, John R., Jr, & Morris, B. (2017). IT internal control weaknesses and the market value of firms. *Journal of Enterprise Information Management, 30*(6), 964-986. http://dx.doi.org.proxy1.ncu.edu/10.1108/JEIM-02-2016-0053

Kuo, C. (2014). Effect of enterprise resource planning information system on business performance: An empirical case of Taiwan. *Journal of Applied Finance and Banking, 4*(2), 1-19. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1511118116?accountid=28180

Lackovic, I. D. (2017). Enterprise risk management: A literature survey. Paper presented at the 364-370. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/2070393421?accountid=28180

Lee, J., Cho, E., & Choi, H. (2016). The effect of internal control weakness on investment efficiency. *Journal of Applied Business Research, 32*(3), 649-662. http://dx.doi.org.proxy1.ncu.edu/10.19030/jabr.v32i3.9648

Ling, L. (2015). Research on enterprise internal control financial assessment system based on artificial intelligence. *Revista Ibérica De Sistemas e Tecnologias De Informação,* (16), 224-234. http://dx.doi.org.proxy1.ncu.edu/10.17013/risti.16B.224-234

Lipaj, D., & Davidaviciene, V. (2013). Influence of information systems on business performance. *Mokslas: Lietuvos Ateitis, 5*(1), 38-n/a. http://dx.doi.org.proxy1.ncu.edu/10.3846/mla.2013.06

Ljutic, B., Marjanovic, P., & Djordjevic, Z. (2014). Enterprise resource planning in small and medium-sized enterprises in Serbia. *Aktual'Ni Problemy Ekonomiky = Actual Problems in Economics,* (162), 403-409. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1661107017?accountid=28180

Lodhi, R. N., Aftab, F., Mahmood, Z., & Cheema, F. (2014). Success of absorptive capacity for enterprise resource planning (ERP) system: Empirical evidence from Pakistan. *Global Management Journal for Academic & Corporate Studies, 4*(2), 26-37. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1925704273?accountid=28180

Mentz, M., Barac, K., & Odendaal, E. (2018). An audit evidence planning model for the public sector. *Journal of Economic and Financial Sciences, 11*(1) http://dx.doi.org.proxy1.ncu.edu/10.4102/jef.v11i1.166

Miller, R. P., Bunn, E., & Noe, K. (2016). Accounting information systems: A view from the public eye. *The International Business & Economics Research Journal, 15*(5), 265. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1820322179?accountid=28180

Monk, E. F., & Lycett, M. (2016). Measuring business process learning with enterprise resource planning systems to improve the value of education. *Education and Information Technologies, 21*(4), 747-768. http://dx.doi.org.proxy1.ncu.edu/10.1007/s10639-014-9352-6

Moore, J. (2018). The relationship between organization size and occupational fraud. *International Research Journal of Applied Finance, 9*(5), 248-276. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/2063280710?accountid=28180

Morris, J. J. (2011). The impact of enterprise resource planning (ERP) systems on the effectiveness of internal controls over financial reporting. *Journal of Information Systems, 25*(1), 129-157. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/858021783?accountid=28180

Packenham, J. P., Rosselli, R. T., Ramsey, S. K., Taylor, H. A., Fothergill, A., Slutsman, J., & Miller, A. (2017). Conducting science in disasters: Recommendations from the NIEHS working group for special IRB considerations in the review of disaster related research. *Environmental Health Perspectives (Online), 125*(9) http://dx.doi.org.proxy1.ncu.edu/10.1289/EHP2378

Pirrone, M., & Trainor, J. E. (2015). Code of ethics amendments required by section 406 of the Sarbanes-Oxley Act. *Journal of Leadership, Accountability and Ethics, 12*(1), 25-31. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1726798536?accountid=28180

PCAOB. (n.d.). Public Company Accounting Oversight Board. Retrieved from https://pcaobus.org/Standards/Auditing/Pages/default.aspx

Ragan, J., Puccio, C., & Talisesky, B. (2014). Accounting control technology using SAP: A case-based approach. *American Journal of Business Education (Online), 7*(4), 349. http://dx.doi.org.proxy1.ncu.edu/10.19030/ajbe.v7i4.8846

Ragothaman, S., & Cornelsen, E. (2017). Characteristics of firms with material weaknesses in internal control: An empirical analysis. *Journal of Accounting and Finance, 17*(4), 63-72.

Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1931135204?accountid=28180

Richardson, P., Dellaportas, S., Perera, L., & Richardson, B. (2015). Towards a conceptual framework on the categorization of stereotypical perceptions in accounting. *Journal of Accounting Literature, 35*, 28-46. http://dx.doi.org.proxy1.ncu.edu/10.1016/j.acclit.2015.09.002

RIMS. (n.d.). The risk management society. Retrieved from https://www.rims.org/aboutRIMS/Pages/MissionandDescription.aspx

Rognlie, M. (2015). Deciphering the fall and rise in the net capital share: Accumulation or scarcity? *Brookings Papers on Economic Activity,* , 1-69. http://dx.doi.org.proxy1.ncu.edu/10.1353/eca.2016.0002

Rubino, M., & Vitolla, F. (2014). Internal control over financial reporting: Opportunities using the COBIT framework. *Managerial Auditing Journal, 29*(8), 736-771. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1660950575?accountid=28180

Rubino, M., Vitolla, F., & Garzoni, A. (2017). How IT controls improve the control environment. *Management Research Review, 40*(2), 218-234. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1865678681?accountid=28180

Samithisomboon, S., & Chantatub, W. (2016). Perceptions of information technology processes among IT decision makers in Thailand. *International Journal of Business and Information, 11*(1), 67-91. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1783657953?accountid=28180

Schaltegger, S., & Zvezdov, D. (2015). Gatekeepers of sustainability information: Exploring the roles of accountants. *Journal of Accounting & Organizational Change, 11*(3), 333-361. Retrieved from http://www.emeraldinsight.com

Sherif, K., Pitre, R., & Kamara, M. (2016). Why do information system controls fail to prevent unethical behavior? *VINE Journal of Information and Knowledge Management Systems, 46*(2), 251-266. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1905750097?accountid=28180

Sorensen, D. P., & Miller, S. E. (2017). Financial accounting scandals and the reform of corporate governance in the United States and in Italy. *Corporate Governance, 17*(1), 77-88. http://dx.doi.org.proxy1.ncu.edu/10.1108/CG-05-2016-0125

Sorensen, D. P., Miller, S. E., & Cabe, K. L. (2017). Developing and measuring the impact of an accounting ethics course that is based on the moral philosophy of Adam Smith. *Journal of Business Ethics, 140*(1), 175-191. http://dx.doi.org.proxy1.ncu.edu/10.1007/s10551-015-2656-7

Sprouse, J., & Almeida, D. (2017). Design sensitivity and statistical power in acceptability judgment experiments. *Glossa, 2*(1), 1-32. http://dx.doi.org.proxy1.ncu.edu/10.5334/gjgl.236

Stanciu, V., & Bran, F. P. (2015). The accounting profession in the digital era. *Calitatea, 16*, 546-550. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1667180190?accountid=28180

Strong, J., & Portz, K. (2015). IT knowledge: What do accounting students think they know? do you know more than I do? an exploratory study. *The Review of Business Information*

Systems, 19(2), 39-n/a. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1749622863?accountid=28180

Sularto, L. (2016). Refinement and user acceptance test of accounting information system for restaurants SMEs. *Journal of Internet Banking and Commerce, 21*(2), 1-15. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1826917789?accountid=28180

Taheri, S., Momeni, A. R., & Hashemi, H. (2016). Analyzing the result of the effect of information technology on qualitative features of information in accounting. *Journal of Current Research in Science,* (1), 623-626. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1786068203?accountid=28180

Tahinakis, P., & Samarinas, M. (2016). The incremental information content of audit opinion. *Journal of Applied Accounting Research, 17*(2), 139-169. Retrieved from https://search-proquest-com.proxy1.ncu.edu/docview/2120164729/19F42AA271A94061PQ/1?accountid=28180

The Belmont Report. (1979). HHS.gov. *Office for Human Research Protections*. Retrieved from https://www.hhs.gov

The Institutional Review Board (IRB) Process. (n.d.). NCU Dissertation Center. *Northcentral Universit*y. Retrieved from http://www.ncu.edu

Wang, J. (2015). An empirical study of the effectiveness of internal control and influencing factors. *Management & Engineering,* (18), 8-13. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1703437093?accountid=28180

Wang, L. H. (2014). The analysis of enterprise network security problems. *Applied Mechanics and Materials, 602-605*, 3351-3354. http://dx.doi.org.proxy1.ncu.edu/10.4028/www.scientific.net/AMM.602-605.3351

Weng, T., Chi, H., & Chen, G. (2015). Internal control weakness and information quality. *Journal of Applied Finance and Banking, 5*(5), 135-169. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1716887631?accountid=28180

Zogning, F. (2017). Comparing financial systems around the world: Capital markets, legal systems, and governance regimes. *Economics, Management and Financial Markets, 12*(4), 43-58. http://dx.doi.org.proxy1.ncu.edu/10.22381/EMFM12420172

Appendix A

ANALYSIS OF SOURCES

Year of Publication	Count	Percentage of Sources
<2014	13	14%
No Date (n.d.)	6	7%
≥2014	73	79%
≥2014 + (n.d.)	**79**	**86%**
Total	92	100%

Table 1. Analysis of sources used for this study.

PRELIMINARY GROUP ASSIGNMENT of SAMPLE (count by fiscal year)		
Fiscal Year	Group 1	Group 2
2013	5,166	48
2014	5,162	65
2015	4,888	73
2016	4,640	65
2017	4,543	47
2018	4,384	9
TOTAL	28,275	307

Table 2. Preliminary count by fiscal year of SEC Registrants

PRELIMINARY DATA ANALYSIS (count by fiscal year)		
Fiscal Year	Group 1	Group 2
2013	3,395	23
2014	3,457	42
2015	3,567	46
2016	3,597	42
2017	3,856	43
2018	3,200	6
Total	21,072	202

Table 3. Count of SEC Registrants by fiscal year minus data errors and analytical anomalies

Grouping Criteria: Sub-Sample A	
1.	Annual 10K Report filed between the Years of 2013-2018.
2.	Standard Industrial Code (SIC)
3.	Total Amount of Annual Earnings
4.	Occurrence of an IT Control Material Weakness

Table 4. Categorical Criteria used to establish Homogenous Pairs for Sub-Sample A

Sub-Sample A: Matched Pair Samples by Fiscal Year		
Fiscal Year	Count of Group 1 by Fiscal Year	Count of Group 2 by Fiscal Year
2013	19	20
2014	33	34
2015	33	34
2016	18	29
2017	29	37
2018	24	2
Total	156	156

Table 5. Sub-Sample A: by Fiscal Year used to test H1 and H2.

Sub-Sample B: ((Group 1: Tobin's Q Δ (μ_1) (t-(t+1))) - (Group 2: Tobin's Q Δ (μ_2) (t-(t+1))))		
Fiscal Year	Count of Group 1 by Fiscal Year	Count of Group 2 by Fiscal Year
2013	27	16
2014	24	28
2015	32	31
2016	30	31
2017	20	27
2018	0	0
Total	133	133

Table 6. Sub-Sample B: by Fiscal Year used to test H1 and H2.

Grouping Criteria: Sub-Sample B
1. Annual 10K Report filed between the Years of 2013-2018.
2. Standard Industrial Code (SIC)
3. Total Amount of Annual Earnings
4. Occurrence of an IT Control Material Weakness
5. Consecutive Annual Occurrence of IT Control Material Weakness (t and (t+1)) (Used to test H3 only)

Table 7. Categorical Criteria used to establish Homogenous Pairs for Sub-Sample B

Frequencies (Group 1 - Sub-Sample A)				
(*** trillions)		Group 1 Earnings	Group 1 OMV1	Group 1 (μ_1) Tobin's Q
N	Valid	156	156	156
	Missing	0	0	0
Mean		$124,233,998	$4,014,351,206	5.360
Std. Error of Mean		$71,688,304	$1,311,917,475	1.422
Median		($221,762)	$563,474,038	2.196
Mode		-$715,000,000[a]	$3,140,610[a]	-60.64a
Std. Deviation		$895,386,625	$16,385,844,010	17.756
Variance		***$8,017,172,083.4	***$268,495,883,921.3	315.290
Skewness		10.23	9.09	4.051
Std. Error of Skewness		0.19	0.19	0.194
Kurtosis		116.39	95.6	28.747
Std. Error of Kurtosis		0.39	0.39	0.386
Range		$11,175,000,000	$183,883,813,886	204.240
Minimum		($715,000,000)	$3,140,610	-60.640
Maximum		$10,460,000,000	$183,886,954,496	143.600
Sum		$19,380,503,634	$626,238,788,196	836.210
%	25	($17,035,455)	0.799	0.8
	50	($221,762)	2.196	2.2
	75	$30,499,301	5.039	5.04
a. Multiple modes exist. The smallest value is shown				

Table 8. Frequencies Group 1: Sub-Sample A: Earnings, OMV, and, Tobin's-Q

Frequencies (Group 2 - Sub-Sample A)				
(*** trillions)		Group 2 Earnings	Group 2 OMV2	Group 2 (μ_2) Tobin's Q
N	Valid	156	156	156
	Missing	0	0	0
Mean		($354,550)	$1,098,012,775	1.6288
Std. Error of Mean		$16,884,290	$222,270,214	1.23984
Median		($919,000)	$246,698,144	1.659
Mode		-$848,000,000[a]	$14[a]	0
Std. Deviation		$210,884,713	$2,776,154,089	15.48559
Variance		***$44,472,362,380.8	***$7,707,031,524,300.4	239.803
Skewness		2.05	5.75	-0.933
Std. Error of Skewness		0.19	0.19	0.194
Kurtosis		17.52	38.86	10.516
Std. Error of Kurtosis		0.39	0.39	0.386
Range		$2,181,000,000	$23,268,669,426	149.7
Minimum		($848,000,000)	$14	-83.12
Maximum		$1,333,000,000	$23,268,669,440	66.58
Sum		($55,309,830)	$171,289,992,835	254.1
%	25	($24,072,500)	-1.5614	-1.56
	50	($919,000)	1.659	1.66
	75	$18,194,750	4.6047	4.6
a. Multiple modes exist. The smallest value is shown				

Table 9. Frequencies Group 2: Sub-Sample A: Earnings, OMV, and, Tobin’s-Q

Frequency Statistics: Sub-Sample B

		Group 1:Tobin's Δ (μ_1) (t-(t+1))	Group 2:Tobin's Q Δ (μ_2) (t-(t+1))	Difference between Group 1:Tobin's Q Δ (μ_1) (t-(t+1)) and Group 2:Tobin's Q Δ (μ_2) (t-(t+1))
N	Valid	133	133	133
	Missing	0	0	0
Mean		27.99	-12.37	40.35
Std. Error of Mean		13.75	7.15	14.61
Median		0.00	-0.06	0.20
Mode		-62.97a	-838.27a	-$29.76a
Std. Deviation		158.60	82.46	168.48
Variance		25152.74	6799.08	28386.21
Skewness		6.56	-8.26	5.23
Std. Error of Skewness		0.21	0.21	0.21
Kurtosis		44.38	78.58	28.26
Std. Error of Kurtosis		0.42	0.42	0.42
Range		1362.26	943.75	1223.58
Minimum		-62.97	-838.27	-29.76
Maximum		1299.29	105.48	1193.81
Sum		3722.27	-1644.84	5367.11
Percentiles	25	-0.73	-1.30	-1.31
	50	0.00	-0.06	0.20
	75	1.19	1.27	6.28

a. Multiple modes exist. The smallest value is shown

Table 10. Frequency Statistics: Sub-Sample B: Tobin's Q Δ (μ) (t-(t+1))

Descriptive Statistics: Sub-Sample A							
(* millions) (**billions)	N	Range	Minimum	Maximum	Mean		Std. Deviation
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic
Group 1 Earnings	156	*$11,175.0	*-$715.0	*$10,460.0	*$124.2	*$71.7	*$895.4
Group 1 OMV1	156	*$183,883.8	*$3.1	*$183,887.0	*$4,014.4	*$1,311.9	*$16,385.8
Group 1 (μ_1) Tobin's Q	156	204.24	-60.64	143.6	5.3603	1.42165	17.75641
Group 2 Earnings	156	*$2,181.0	*-$848.0	*$1,333.0	*-$0.4	*$16.9	*$210.9
Group 2 OMV2	156	*$23,268.7	*$.000014	*$23,268.7	*$1,098.0	*$222.3	*$2,776.2
Group 2 (μ_2) Tobin's Q	156	149.7	-83.12	66.58	1.6288	1.23984	15.48559

Table 11. Descriptive Statistics: Sub-Sample A: Earnings, OMV, and Tobin's-Q.

Descriptive Statistics Continued: Sub-Sample A						
(* millions) (**billions)	N	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Group 1 Earnings	156	**$801,717,208.3	10.231	0.194	116.386	0.386
Group 1 OMV1	156	**$268,495,883,921.3	9.085	0.194	95.597	0.386
Group 1 (μ_1) Tobin's Q	156	315.29	4.051	0.194	28.747	0.386
Group 2 Earnings	156	**$44,472,362.4	2.049	0.194	17.517	0.386
Group 2 OMV2	156	**$7,707,031,524.3	5.748	0.194	38.862	0.386
Group 2 (μ_2) Tobin's Q	156	239.80	-0.933	0.194	10.516	0.386

Table 12. Descriptive Statistics: Sub-Sample A: Earnings, OMV, and Tobin's-Q.

Descriptive Statistics: Sub-Sample B							
(* millions) (**billions)	N	Range	Minimum	Maximum	Mean		Std. Deviation
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic
Group 1 Earnings ($) (t)	133	**$408.2	**-$140.2	**$268.0	**$0.3	**$2.6	**$30.0
Group 1 (μ_1) (t)	133	$2,200.01	-$67.63	$2,132.38	$28.46	$17.78	$205.05
Group 1: Stock Price (t)	133	$505.60	$0.02	$505.62	$26.47	$4.50	$51.90
Group 1 Earnings ($) (t+1)	133	**$343.3	**-$196.1	**$147.2	**$2.7	**$2.3	**$25.9
Group 1 (μ_1) (t+1)	133	$2,457.02	-$1,205.08	$1,251.94	$0.48	$13.31	$153.54
Group 1: Stock Price (t+1)	133	$524.20	$0.00	$524.20	$29.82	$5.05	$58.27
Group 1: Δ (μ_1) (t-(t+1))	133	$1,362.26	-$62.97	$1,299.29	$27.99	$13.75	$158.60
Group 1: Δ Stock Price (t-(t+1))	133	$124.54	-$105.85	$18.69	-$3.35	$1.14	$13.12
Group 2 Earnings ($) (t)	133	**$218.1	**-$84.8	**$133.3	**-$0.2	**$1.7	**$19.8
Group 2 Tobin's Q (μ_2) (t)	133	$320.81	-$254.23	$66.58	-$2.57	$2.54	$29.24
Group 2: Stock Price (t)	133	$178.94	$0.06	$179.00	$20.17	$2.37	$27.33
Group 2 Earnings ($) (t+1)	133	**$100.1	**-$26.4	**$73.6	**$3.1	**$1.2	**$13.3
Group 2 Tobin's Q (t+1)	133	$918.86	-$61.14	$857.72	$9.79	$6.75	$77.80
Group 2: Stock Price (t+1)	133	$191.58	$0.02	$191.60	$20.63	$2.61	$30.15
Group 2: Δ Stock Price (t-(t+1))	133	$53.74	-$30.00	$23.74	-$0.46	$0.71	$8.20
Group 2: Tobin's Q Δ (μ_2) (t-(t+1))	133	$943.75	-$838.27	$105.48	-$12.37	$7.15	$82.46
Difference between Group 1: Tobin's Q Δ (μ_2) (t-(t+1)) and Group 2: Tobin's Q Δ (μ_2) (t-(t+1))	133	$1,223.58	-$29.76	$1,193.81	$40.35	$14.61	$168.48
Difference between Group 1: Δ Stock Price (t-(t+1)) and Group 2: Δ Stock Price (t-(t+1))	133	$107.74	-$23.47	$84.27	$1.77	$1.06	$12.21

Table 13. Descriptive Statistics: Sub-Sample B: Earnings, OMV, and, Tobin's-Q

Descriptive Statistics Continued: Sub-Sample B						
(* millions) (**billions)	N	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Group 1 Earnings ($) (t)	133	**$9,013,917,569.0	4.648	0.21	51.714	0.417
Group 1 (μ_1) (t)	133	$42,045.09	9.204	0.21	89.321	0.417
Group 1: Stock Price (t)	133	$2,693.86	6.88	0.21	57.632	0.417
Group 1 Earnings ($) (t+1)	133	**$6,733,630,316.5	-1.894	0.21	33.767	0.417
Group 1 (μ_1) (t+1)	133	$23,573.09	0.414	0.21	62.113	0.417
Group 1: Stock Price (t+1)	133	$3,395.47	6.106	0.21	44.667	0.417
Group 1: Δ (μ_1) (t-(t+1))	133	$25,152.74	6.557	0.21	44.38	0.417
Group 1: Δ Stock Price (t-(t+1))	133	$172.21	-4.133	0.21	28.671	0.417
Group 2 Earnings ($) (t)	133	**$3,921,746,247.5	1.814	0.21	19.523	0.417
Group 2 Tobin's Q (μ_2) (t)	133	$854.75	-5.633	0.21	44	0.417
Group 2: Stock Price (t)	133	$746.95	3.46	0.21	15.124	0.417
Group 2 Earnings ($) (t+1)	133	**$1,759,484,014.9	2.664	0.21	10.433	0.417
Group 2 Tobin's Q (t+1)	133	$6,052.87	10.104	0.21	109.214	0.417
Group 2: Stock Price (t+1)	133	$909.25	3.499	0.21	15.064	0.417
Group 2: Δ Stock Price (t-(t+1))	133	$67.30	-0.102	0.21	2.381	0.417
Group 2: Tobin’s Q Δ (μ_2) (t-(t+1))	133	$6,799.08	-8.26	0.21	78.581	0.417
Difference between Group 1: Tobin’s Q Δ (μ_2) (t-(t+1)) and Group 2: Tobin’s Q Δ (μ_2) (t-(t+1))	133	$28,386.21	5.225	0.21	28.255	0.417
Difference between Group 1: Δ Stock Price (t-(t+1)) and Group 2: Δ Stock Price (t-(t+1))	133	$149.15	2.846	0.21	16.558	0.417

Table 14. Descriptive Statistics Continued: Sub-Sample B

Paired Samples Correlations				
		N	Correlation	Sig.
Pair 1	Group 1 (μ_1) Tobin's Q & Group 2 (μ_2) Tobin's Q	156	0.102	0.203
Pair 2	Group 1 OMV1 & Group 2 OMV2	156	0.246	0.002
Pair 3	Group 1: Tobin's Q Δ (μ_1) (t-(t+1)) & Group 2: Tobin’s Q Δ (μ_2) (t-(t+1))	133	0.136	0.118

Table 15. Paired Samples Correlations T-Tests

Paired Samples Tests									
(* millions) (**billions)		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	Group 1 (μ_1) Tobin's Q - Group 2 (μ_2) Tobin's Q	3.7315	22.3330	1.78807	0.1994	7.2636	2.087	155	0.039
Pair 2	Group 1 OMV1 - Group 2 OMV2	*$2,916.3	*$15,932.1	*$1,275.6	*$396.5	*$5,436.1	2.286	155	0.024
Pair 3	Group 1: Δ (μ_1) (t-(t+1)) - Group 2: Tobin’s Q Δ (μ_2) (t-(t+1))	40.3542	168.4821	14.60925	11.4557	69.2528	2.762	132	.007

Table 16. Paired Samples T-Tests

RQ1-H1. Paired Samples Test									
(* millions) (**billions)		Paired Differences							
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference		t	df	Sig. (2-tailed)
					Lower	Upper			
Pair 1	Group 1 (μ_1) Tobin's Q - Group 2 (μ_2) Tobin's Q	3.73151	22.33299	1.78807	0.19938	7.26364	2.087	155	0.039

Table 17. Results of Paired Sample T-Test of H1

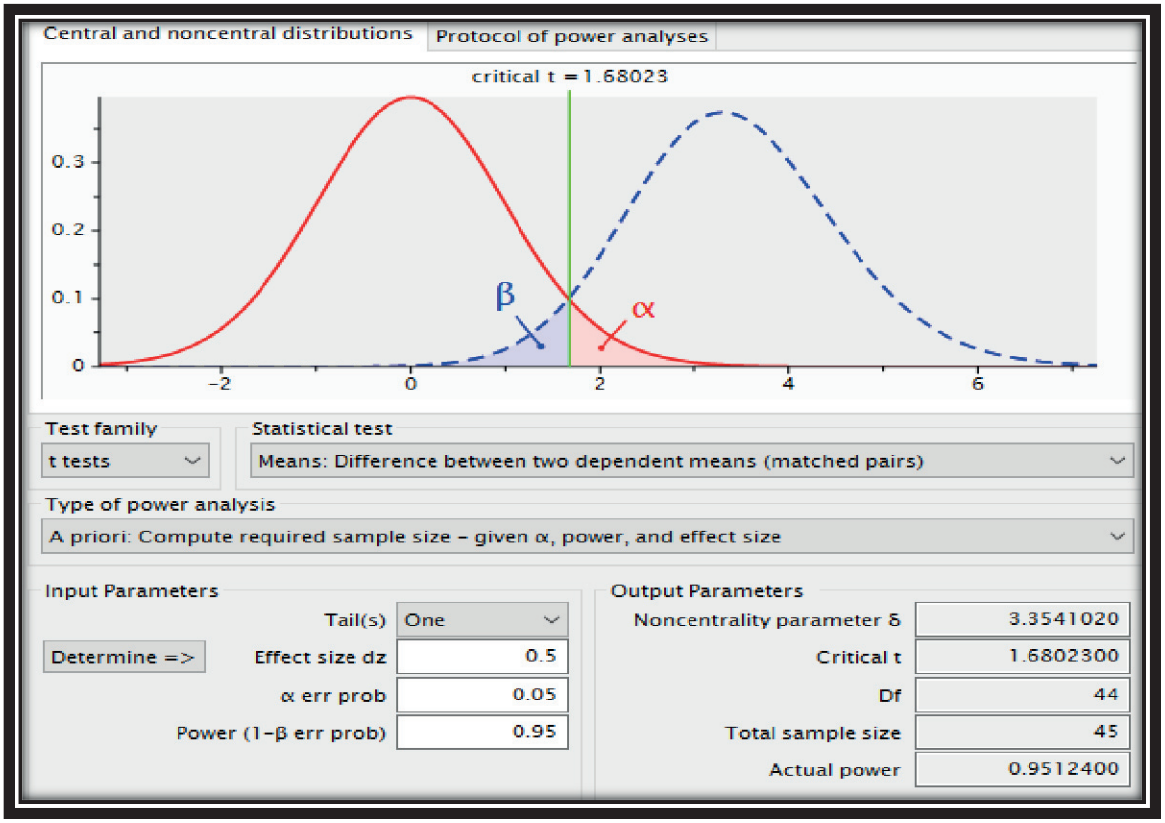
RQ2-H2. Paired Samples Test									
(* millions) (**billions)		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	Group 1 OMV1 - Group 2 OMV2	*$2,916.3	*$15,932.1	*$1,275.6	*$396.5	*$5,436.1	2.286	155	0.024

Table 18. Results of Paired Sample T-Test of H2

RQ3-H3. Paired Samples Test									
		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 3	Group 1: Tobin's Q Δ (μ_1) (t-(t+1)) - Group 2: Tobin's Q Δ (μ_2) (t-(t+1))	40.354	168.482	14.609	11.456	69.253	2.76	132	.007

Table 19. Results of Paired Sample T-Test of H3

Appendix B


Central and noncentral distributions
Protocol of power analyses
critical t = 1.68023
0.3
0.2
0.1
0
−2
0
2
4
6
β
α

Test family: t tests

Statistical test: Means: Difference between two dependent means (matched pairs)

Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters

Tail(s): One

Determine =>

Effect size dz: 0.5

α err prob: 0.05

Power (1−β err prob): 0.95

Output Parameters

Noncentrality parameter δ: 3.3541020

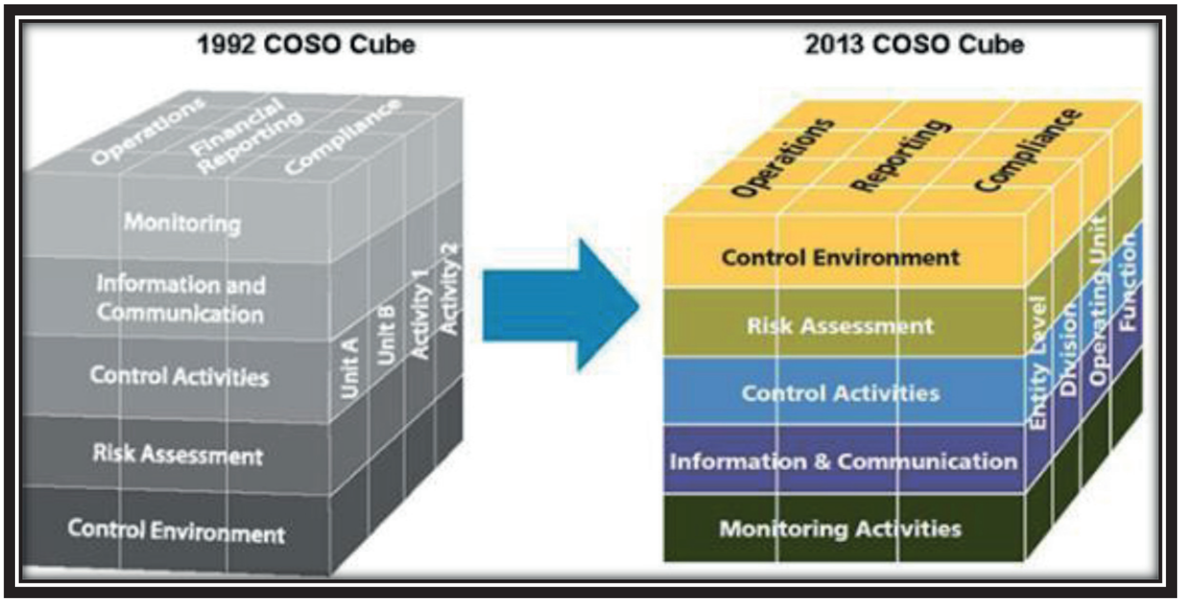
Critical t: 1.6802300

Df: 44

Total sample size: 45

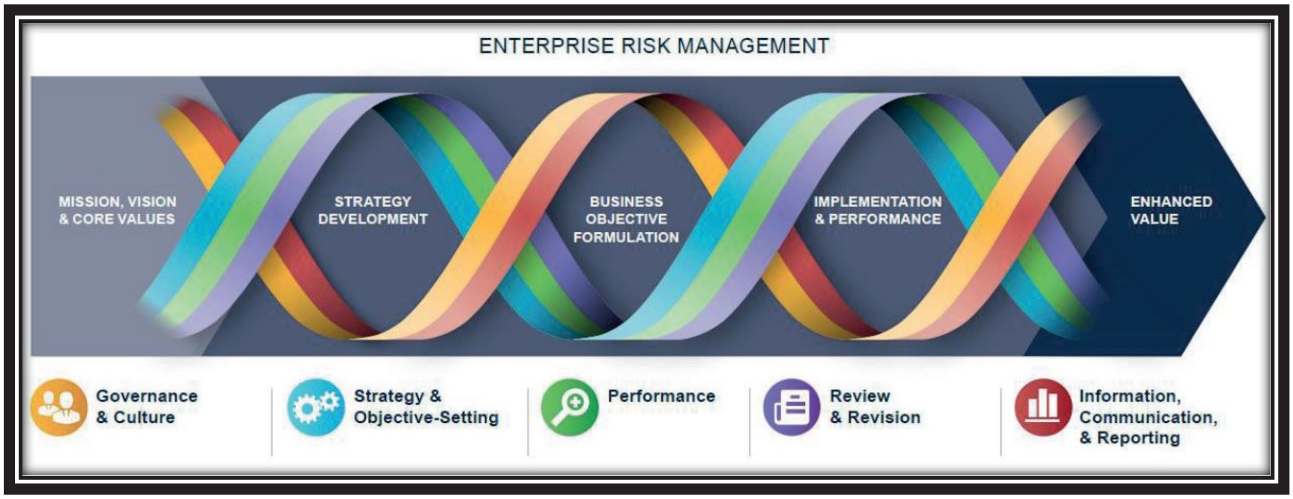
Actual power: 0.9512400

Figure 1. G*Power Analysis

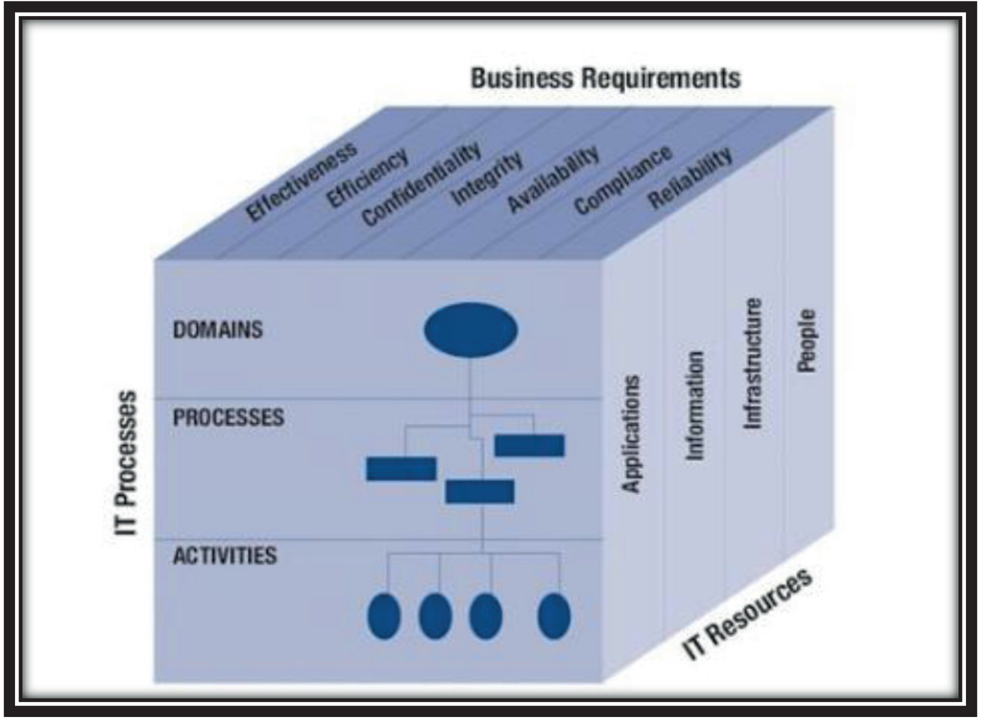


http://rsmus.com/content/dam/mcgladrey/images/figure/coso_cube_comparison.png

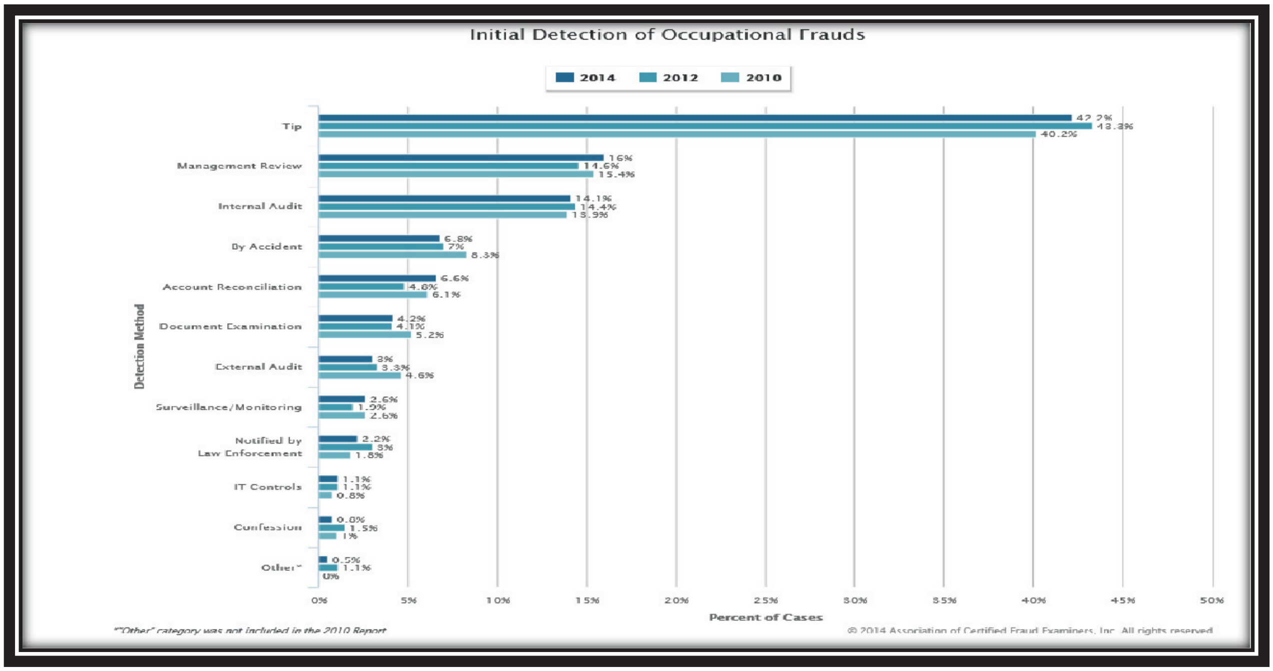
Figure 2. COSO Framework Comparison


ENTERPRISE RISK MANAGEMENT
MISSION, VISION & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting

https://www.coso.org/Documents/COSO-ERM-Presentation-September-2017.pdf
Figure 3. 2017 COSO ERM Framework

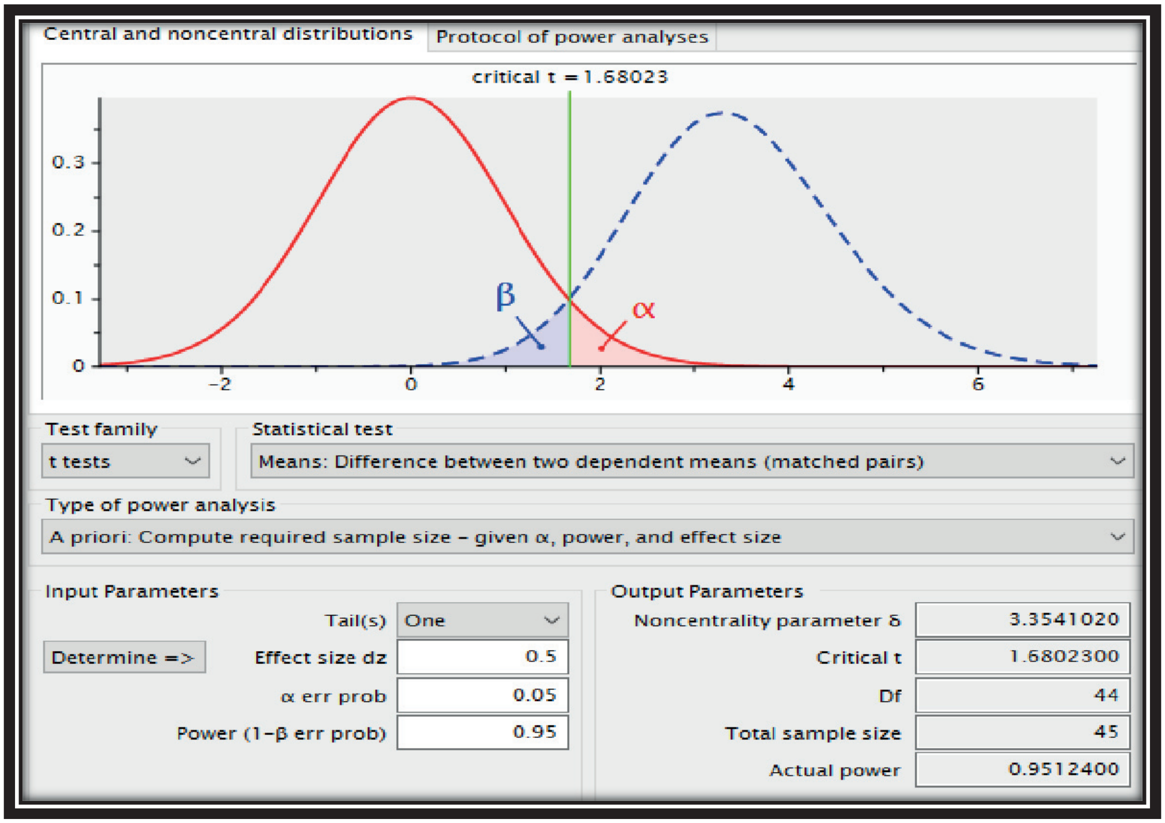


http://www.bmc.com/guides/itil-cobit-introduction.html
Figure 4. COBIT5 Framework



https://www.acfe.com/rttn-detection.aspx

Figure 5. Initial Detection of Occupational Frauds


Central and noncentral distributions
Protocol of power analyses
critical t = 1.68023
0.3
0.2
0.1
0
−2
0
2
4
6
β
α
Determine =>

Test family: t tests

Statistical test: Means: Difference between two dependent means (matched pairs)

Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters

Tail(s)	One
Effect size dz	0.5
α err prob	0.05
Power (1−β err prob)	0.95

Output Parameters

Noncentrality parameter δ	3.3541020
Critical t	1.6802300
Df	44
Total sample size	45
Actual power	0.9512400

Figure 6. G*Power Analysis

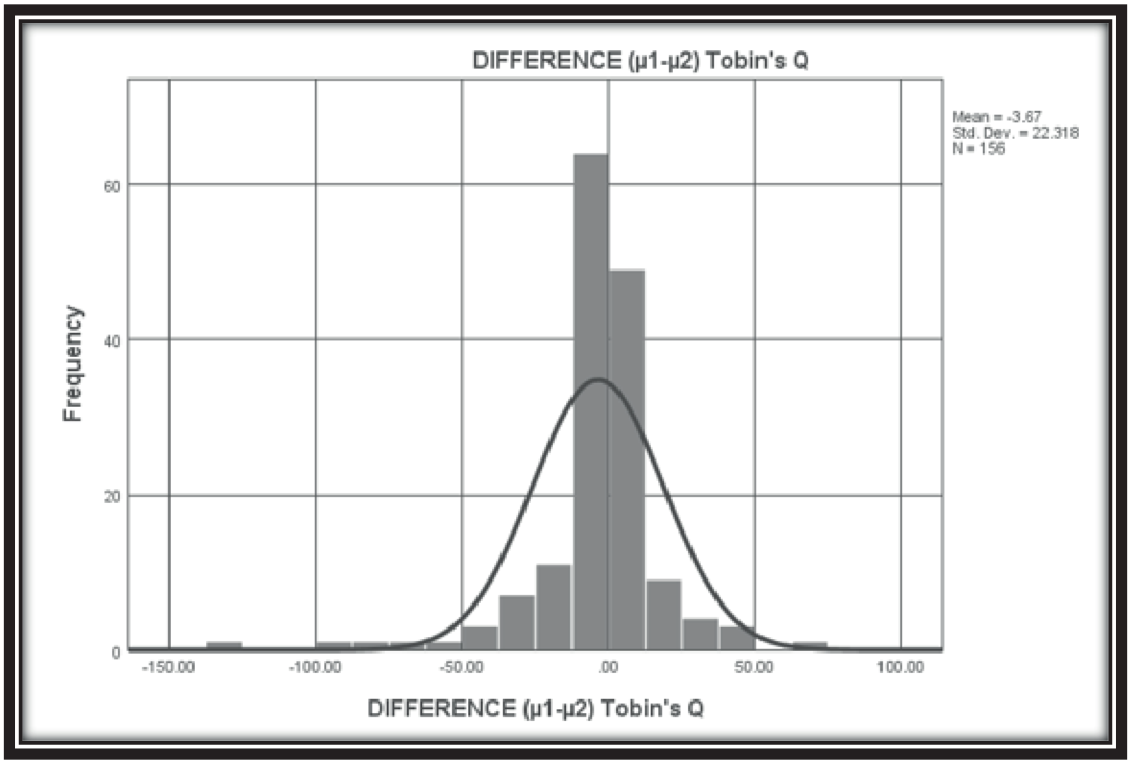


Figure 7. Histogram of Group 1 (µ1) Tobin's Q - Group 2 (µ2) Tobin's Q

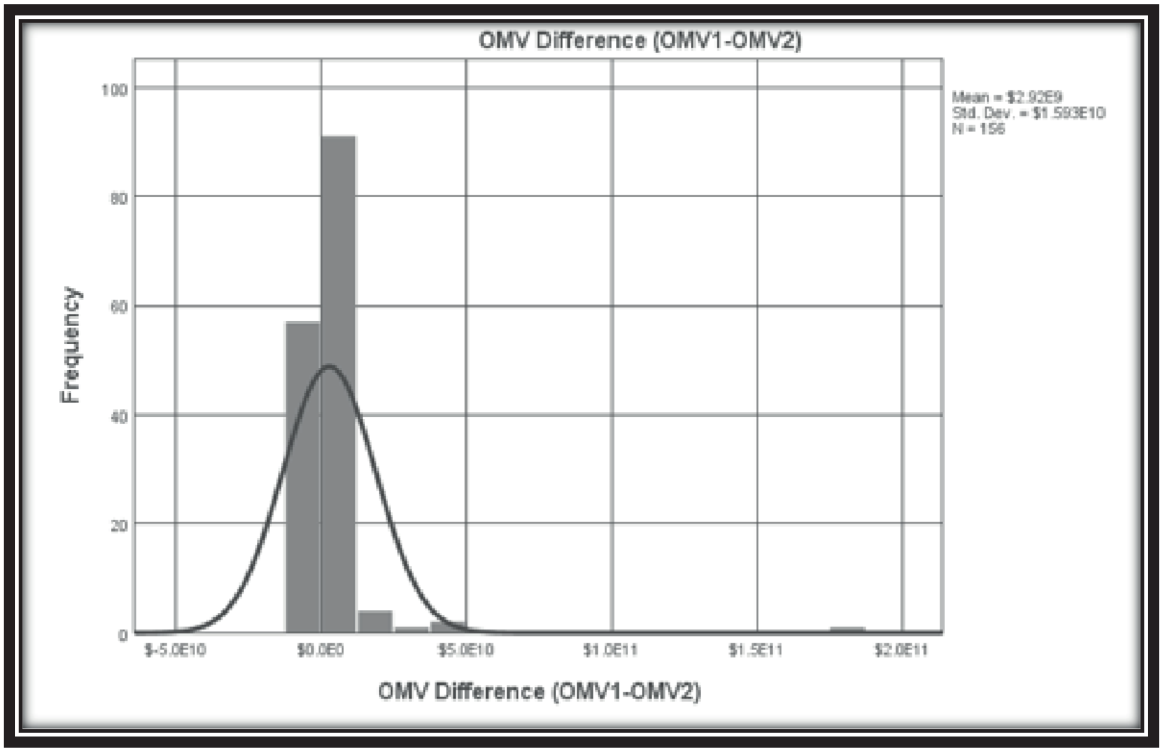


Figure 8. Histogram OMV Difference (OMV1-OMV2)

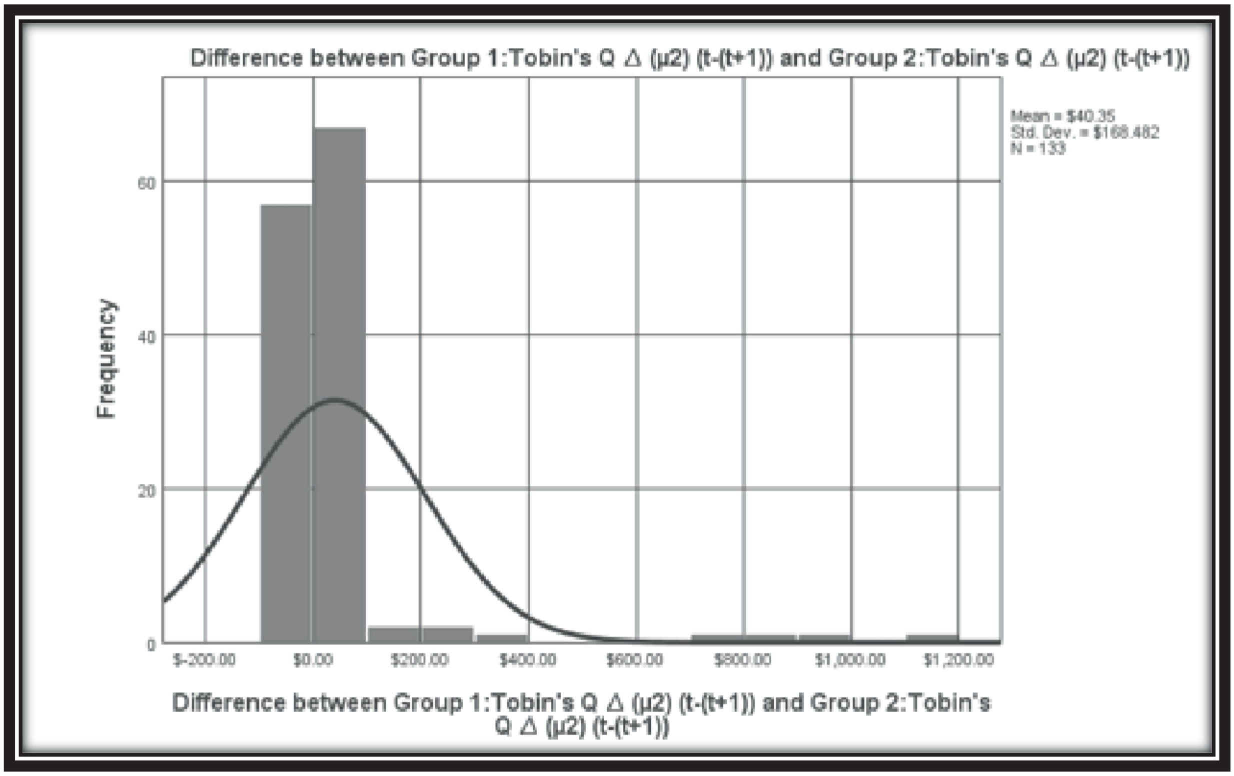


Figure 9. Histogram of ((Group 1: Tobin's Q Δ (μ_1) (t-(t+1))) – (Group 2: Tobin's Q Δ (μ_2) (t-(t+1))))

Two Sample T-Test

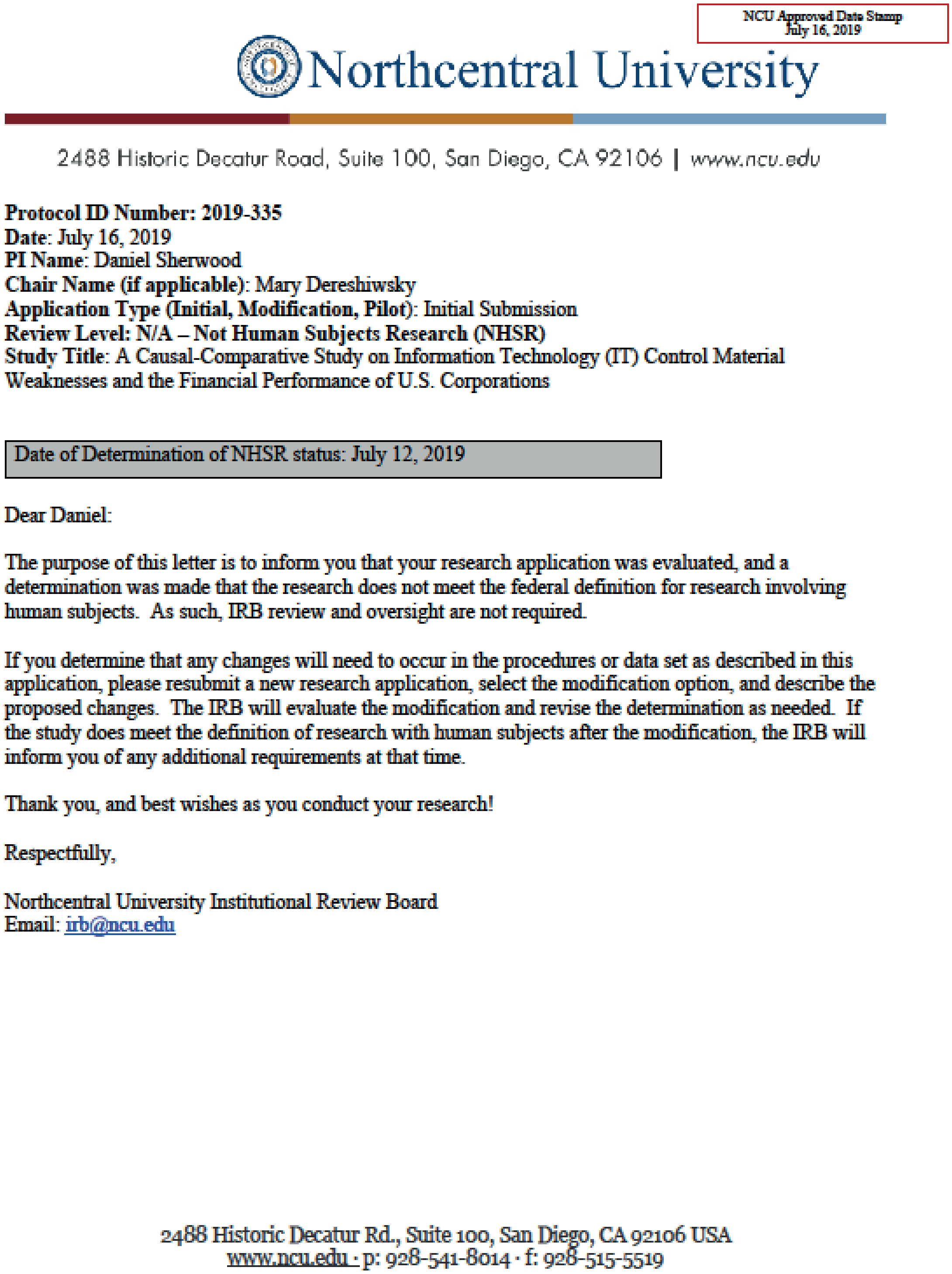
$$T = \frac{x_d}{\sqrt{\left(\frac{1}{n_0}+\frac{1}{n_1}\right)\frac{(n_0-1)s_0^2+(n_1-1)S_1^2}{n_0+n_1-2}}}$$

Paired Samples T-Test

$$t = \frac{x_d}{\frac{1}{n(n-1)}\sum_{j-1}^{n}(x_d-\bar{x}_d)}$$

Figure 10. Formulas for conducting 2-Sample Tests and Paired Samples T-Tests

Appendix C



NCU Approved Date Stamp
July 16, 2019

Northcentral University

2488 Historic Decatur Road, Suite 100, San Diego, CA 92106 | www.ncu.edu

Protocol ID Number: 2019-335
Date: July 16, 2019
PI Name: Daniel Sherwood
Chair Name (if applicable): Mary Dereshiwsky
Application Type (Initial, Modification, Pilot): Initial Submission
Review Level: N/A – Not Human Subjects Research (NHSR)
Study Title: A Causal-Comparative Study on Information Technology (IT) Control Material Weaknesses and the Financial Performance of U.S. Corporations

Date of Determination of NHSR status: July 12, 2019

Dear Daniel:

The purpose of this letter is to inform you that your research application was evaluated, and a determination was made that the research does not meet the federal definition for research involving human subjects. As such, IRB review and oversight are not required.

If you determine that any changes will need to occur in the procedures or data set as described in this application, please resubmit a new research application, select the modification option, and describe the proposed changes. The IRB will evaluate the modification and revise the determination as needed. If the study does meet the definition of research with human subjects after the modification, the IRB will inform you of any additional requirements at that time.

Thank you, and best wishes as you conduct your research!

Respectfully,

Northcentral University Institutional Review Board
Email: irb@ncu.edu

2488 Historic Decatur Rd., Suite 100, San Diego, CA 92106 USA
www.ncu.edu · p: 928-541-8014 · f: 928-515-5519