2011

Investigating the Relationship between Governance Mechanisms and the Disclosure of IT Control Weaknesses

Basil Hamdan
Virginia Commonwealth University

Follow this and additional works at: https://scholarscompass.vcu.edu/etd

Part of the Business Commons

© The Author

Downloaded from
https://scholarscompass.vcu.edu/etd/299

This Dissertation is brought to you for free and open access by the Graduate School at VCU Scholars Compass. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of VCU Scholars Compass. For more information, please contact libcompass@vcu.edu.
Investigating the Relationship between Governance Mechanisms and the Disclosure of IT Control Weaknesses

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University.

By
Basil Hamdan

Bachelor of Business Administration (MBA)
East Carolina University, Greenville, NC, 2005
B.A., Accounting
University of Jordan, Amman, Jordan, 2000

Committee Members:
Co-Chair: Dr. Allen Lee
Professor of Information Systems

Co-Chair: Dr. Carolyn Strand Norman
Professor of Accounting

Dr. Richard T. Redmond
Associate Professor of Information Systems

Dr. Heinz Roland Weistroffer
Associate Professor of Information Systems

Dr. Alisa G. Brink
Assistant Professor of Accounting

Virginia Commonwealth University
Richmond, Virginia
October, 2011
Acknowledgment

First and foremost, my greatest gratitude goes to my family; my father and my mother, my wife and my son, and my siblings. Thank you for your endless support and for your unwavering faith in me. This accomplishment is just as much yours as it is mine.

I must also express my deepest gratitude to my dissertation committee, Dr. Allen Lee (Chair), Dr. Carolyn Norman (Co-Chair), Dr. Richard T. Redmond, Dr. Heinz Roland Weistroffer, and Dr. Alisa G. Brink, for their time and effort advising me throughout the dissertation process. Each, in their own way, contributed to the quality of my dissertation research and the completion of my doctoral work.

Finally, words cannot express how indebted I am to Dr. Allen Lee for opening my mind to scientific inquiry and system thinking and for all the help and support that he provided during my doctoral journey. If it were not for Dr. Lee’s continued guidance, valuable advice, and support, I would not have been able to complete this work.
# Table of Contents

Table of Contents ........................................................................................................................................ iii
List of Tables .................................................................................................................................................. v
List of Figures ................................................................................................................................................ vi
List of Acronyms and Recurring Names ...................................................................................................... vii
Abstract ..................................................................................................................................................... viii

## Chapter 1 INTRODUCTION

1.1. Introduction ........................................................................................................................................ 1
1.2. Basic Concepts Definitions ................................................................................................................. 2
1.3. Research Background and Importance ............................................................................................. 5
1.4. Research Objectives and Questions .................................................................................................. 9
1.5. Dissertation Structure ....................................................................................................................... 12

## Chapter 2 LITERATURE REVIEW

2.1. Introduction ........................................................................................................................................ 13
2.2. Internal Control .................................................................................................................................. 16
2.3. IT Control Over Financial Reporting ................................................................................................. 24
2.4. Synthesis ............................................................................................................................................. 34

## Chapter 3 THEORETICAL PERSPECTIVE & HYPOTHESES DEVELOPMENT

3.1. An Agency Theory Perspective ........................................................................................................ 37
  3.1.1 IT Governance and IT Control Quality ......................................................................................... 40
  3.1.2 CIO Compensation and IT Control Quality ............................................................................... 46
3.2. Summary of Hypotheses and Research Model ............................................................................... 49

## Chapter 4 RESEARCH METHODOLOGY

4.1. Data Sources and Sample Selection ................................................................................................. 52
4.2. Sample for Study ............................................................................................................................. 55
4.3. Measured Variables .......................................................................................................................... 57
  4.3.1 Dependent Variables ................................................................................................................... 57
  4.3.2 Independent Variables ................................................................................................................ 58
  4.3.3 Control Variables ....................................................................................................................... 59
List of Tables
Table 1: Summary of Hypotheses
Table 2: Sample Selection
Table 3: Assessment of the Matching Process Goodness
Table 4: Variable Definitions
Table 5: Analysis of ITCW Firms by 2 Digit SIC Code and ITCW Year
Table 6: Descriptive Statistics
Table 7: Mean Comparison between the Study Group and the Control Group
Table 8: Correlation Matrix and Collinearity Statistics
Table 9: Model (1) Investigating the Effect of IT Governance Mechanisms on the Disclosure of IT Control Weaknesses (H1-H2)
Table 10: Model (2) Investigating the Effect of CIO Incentive Alignment Mechanisms on the Disclosure of IT Control Weaknesses (H3)
List of Figures

Figure 1: Conceptual Framework ................................................................. 12
Figure 2: CIO's impact on organizational outcome, adopted from Preston et al. 2008 .... 44
Figure 3: Theoretical Research Model.......................................................... 51
Figure 4: ITCW Reporting Trend ................................................................ 67
Figure 5: Theoretical Research Model with Logistic Regression Results ............. 77
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Recurring Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AICPA</td>
<td>The American Institute of Certified Public Accountants</td>
</tr>
<tr>
<td>AS</td>
<td>Auditing Standard</td>
</tr>
<tr>
<td>BOD</td>
<td>Board of Directors</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CFO</td>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>COSO</td>
<td>Committee of Sponsoring Organizations of the Treadway Commission’s Internal Control-Integrated Framework of 1992</td>
</tr>
<tr>
<td>IC</td>
<td>Internal Control</td>
</tr>
<tr>
<td>ICFR</td>
<td>Internal Control Over Financial Reporting</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITC</td>
<td>IT Control</td>
</tr>
<tr>
<td>ITCQ</td>
<td>IT Control Quality</td>
</tr>
<tr>
<td>ITCW</td>
<td>IT Control Weaknesses</td>
</tr>
<tr>
<td>ITGI</td>
<td>IT Governance Institute</td>
</tr>
<tr>
<td>PCAOB</td>
<td>Public Company Accounting Oversight Board</td>
</tr>
<tr>
<td>SAS</td>
<td>Statement on Auditing Standards</td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act of 2002</td>
</tr>
<tr>
<td>TIST</td>
<td>Top Information Systems Team</td>
</tr>
<tr>
<td>TMT</td>
<td>Top Management Team</td>
</tr>
</tbody>
</table>
Abstract

INVESTIGATING THE RELATIONSHIP BETWEEN GOVERNANCE MECHANISMS AND THE DISCLOSURE OF IT CONTROL WEAKNESSES

By Basil Hamdan, Ph.D.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business at Virginia Commonwealth University.

Virginia Commonwealth University, 2011

Major Director: Dr. Allen S. Lee Professor, Information Systems

The current research is concerned with exploring the quality of information technology (IT) control over financial reporting systems as reported under Section 404 of the Sarbanes-Oxley Act of 2002. More specifically, this dissertation examines the association between organizational governance mechanisms and the occurrence and subsequent disclosure of IT control weaknesses.

Despite the adverse impact of IT control weaknesses on internal control quality and financial reporting reliability, research on IT controls in general and IT control weaknesses in particular remains largely anecdotal with limited reliance on theory. The current work proposes and tests an integrated theoretical model of the antecedents of IT control weaknesses. The proposed model draws upon agency theory to provide a theoretical perspective of the occurrence of IT control weaknesses and upon corporate governance literature to solicit potential factors that influence the achievement of effective IT control over financial reporting.
Drawing upon agency theory, this research views the existence of IT control weaknesses as a manifestation of an agency problem caused by information asymmetry and lack of alignment between the overall organization represented by its board of directors as a principal and its information systems (IS) organization represented by the top IS team as an agent. Drawing on corporate governance literature, this dissertation proposes two categories of governance and contracting mechanisms that the board of directors can employ to reduce information asymmetry and align the interests of the top IS team with those of the firm thereby reducing the agency problem. These categories are: IT governance mechanisms and IT executive incentive alignment mechanisms.

The IT governance mechanisms involve two elements: first, the IT background element which includes (a) the IT background of the board of directors as reflected by two of its main committees, namely the corporate governance committee and the audit committee and (b) the IT background of the top management team; second, the IT executive element as reflected in terms of the structural and the expert power of the Chief Information Officer (CIO). The IT executive incentive alignment mechanisms include two elements: (a) the CIO’s absolute compensation level and (b) the pay disparity between the CIO and other members of the top management team. A research model integrating these elements is developed and tested with empirical data. For testing the proposed model, this dissertation uses a sample of firms with IT control weaknesses and a control group of similar firms with no IT control weaknesses for the years 2005-2009.

Empirical results provide support for five of the seven hypotheses put forth in this research. Regarding the IT governance mechanisms, study findings indicate that a lower
likelihood of disclosing IT-related control weaknesses is associated with having audit committee and corporate governance committee members with IT expertise. Furthermore, the study findings provide support for the contention that the goal congruence is contingent on the CIO’s power. To this end, the study finds that a lower likelihood of disclosing IT-related control weaknesses is associated with having CIOs with higher levels of structural and expert power.

As for the incentive alignment mechanisms, empirical results provide support for the assertion that goal congruence is contingent on perceived pay equality between the CIO and other members of the top management team. The results indicate that the lower the pay disparity between IT executives and business executives in the top management team, the lower the likelihood of disclosing IT control weaknesses.

The present study contributes to the current body of knowledge of literature in several ways. It is the first study to propose and test an integrated model of the antecedents of IT control weaknesses. The proposed model adds to the current literature by introducing agency theory as a theoretical basis of the antecedents of IT control weaknesses. Furthermore, this study adds to the current literature by introducing and providing empirical evidence linking the IT background of the corporate governance committee, the structural power and expert power of the CIO, and the CIO relative pay to the disclosure of IT control weaknesses over financial reporting. Lastly, this research contributes to practice by offering a much needed understanding for managers, directors, auditors, and regulators in their effort to improve the quality of IT control and the reliability of financial reporting.
Chapter 1  INTRODUCTION

1.1.  Introduction

Providing reliable and timely financial and managerial information for decision makers, internal or external, has always been a top level priority for organizations, regulators, and society at large. To this end and in light of recent high-profile corporate scandals (e.g. Enron, WorldCom, etc.), the United States Congress enacted the Sarbanes-Oxley Act (SOX) of 2002 which aims, among other things, to improve corporate governance and internal control over financial reporting with the ultimate goal of ensuring the reliability of financial reporting. Of special interest to this research is Section 404 Management Assessment of Internal Controls. Per the requirements of this section, management of publicly traded companies are required to assess the design and operating effectiveness of their internal control over financial reporting and to report that assessment in their annual filing with the Securities and Exchange Commission (SEC), namely in the 10-K forms. In addition, the Public Company Accounting Oversight Board’s (PCAOB) Auditing Standard (AS) No. 5 requires external auditors of all publicly traded companies to obtain an understanding of internal control over financial reporting, to test and evaluate the design and operating effectiveness of internal controls, and to opine on management’s report on the assessment of the effectiveness of internal control over financial reporting (PCAOB 2007).

This dissertation is concerned with IT controls; an integral component of internal control over financial reporting (AICPA 2001; Smith 2004). With increasingly computerized business environments where key business processes including accounting
and financial reporting are entirely automated or largely dependent on IT functionality, it is of paramount importance that organizations design and implement IT controls to ensure the reliability of financial information and to safeguard the information systems that capture, process and generate them. To this end, a report by AMR Research, now a part of Gartner Inc., estimates that companies subject to SOX spent roughly six billion U.S. dollars a year in 2005 and 2006 to comply with the Act, 1.9 billion of which (32%) was spent on IT (Bradford and Brazel 2007). Despite these investments, many companies continue to report deficiencies in their internal control over financial reporting with 20% of these being related to IT control weaknesses (ITCW) (Grant et al. 2008).

More specifically, this dissertation purports to obtain an understanding of the antecedents of ITCW and the ways in which these antecedents impact the weaknesses. The remainder of this chapter proceeds as follows. Section 1.2 presents the main concepts in the research. Section 1.3 presents the research background and establishes the significance of the research. Section 1.4 presents the objectives of the research and the research questions. Finally, section 1.5 presents an outline of the remaining chapters of the dissertation.

1.2. Basic Concepts Definitions

This section offers definitions of the basic concepts in this dissertation. In order to avoid any ambiguity, the definitions presented herein draw heavily on auditing standards and other practitioner publications.

Internal control (IC): is defined as “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance
regarding the achievement of objectives in the following categories: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations” (COSO 1992). Although the COSO framework defines internal control in terms of achieving three objectives, Section 404 of Sarbanes-Oxley Act, which defines the scope of the current work, only pertains to internal control over financial reporting.

**Internal control over financial reporting (ICFR):** is defined as “a process designed by, or under the supervision of, the company’s principal executive and principal financial officers, or persons performing similar functions, and effected by the company’s board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with GAAP” (PCAOB 2007). Internal control over financial reporting includes those policies and procedures that:

1. pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;
2. provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and
(3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company’s assets that could have a material effect on the financial statements (PCAOB 2007).

**Information technology control (ITC):** consistent with the aforementioned definitions of internal control and internal control over financial reporting, this research defines IT control as a manual or automated process designed by, or under the supervision of, the company’s principal executive and principal IT officers, or persons performing similar functions, and effected by the company’s board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial information and transactions and the continued proper operation of the information systems that capture, process and generate them.

The IT control literature distinguishes between two classes of IT controls: **application controls and general controls.** As the name suggests, **application controls** relate to individual computer applications. More specifically, they relate to detecting and preventing the financial misstatement and financial fraud risks associated with using IT to initiate, record, process, and report transactions or other financial data. These controls help ensure that transactions are authorized, and completely and accurately recorded and processed. Application controls may be automated (e.g. automated reconciliation of subsystems, an application that updates accounts in the general ledger for sub-ledger activity, an application control that tests input and output accuracy, etc) or exclusively or primarily manual but dependent on IT functionality (e.g. a control that manually investigates items contained in a computer generated exception report). When application
controls are performed by people interacting with IT, they may be referred to as user controls (AICPA 2007, paragraphs 43-44; SEC 2006). General controls, on the other hand, are defined as policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General controls commonly include controls over data center and network operations, access security, IT management, system development, data security, change management, and business continuity planning (AICPA 2007, paragraph 45; Norman et al. 2009).

While the current work recognizes the broad and multidimensional nature of IT quality, it focuses on IT control quality (ITCQ) under Section 404 of the Sarbanes-Oxley Act of 2002. As such, ITCQ is defined in terms of whether or not the firm has disclosed IT control weaknesses in the context of Section 404 reporting. To this end, firms with IT control weaknesses are viewed as having low IT control quality whereas firms with no IT-related control weaknesses are viewed as having high IT control quality.

### 1.3. Research Background and Importance

Given the pervasiveness of information systems in today’s business processes (Canada et al. 2009; Klamm and Watson 2009), auditing standards have explicitly emphasized that financial auditors test and evaluate the effectiveness of IT controls as they pertain to initiating, recording, processing, and reporting transactions or other financial data and that any significant weaknesses in IT controls are disclosed in the management’s report on the assessment of the effectiveness of internal control over financial reporting (AICPA 2007). For example, AU Section (319), titled “Consideration
of Internal Control in a Financial Statement Audit,” dictates that in obtaining an understanding of internal control over financial reporting, the auditor should consider how an organization’s use of IT may affect internal controls relevant to the audit of financial statements and how IT risks could result in financial misstatements (AICPA 2007).

In the same vein, Statement on Auditing Standards (SAS) No. 94, titled “The Effect of Information Technology on the Auditor’s Consideration of Internal Control in a Financial Statement Audit,” alerts external auditors that assessing control risk at maximum and relying only on substantive testing may not be effective for companies with intensively computerized financial reporting systems. To this end, the standard advises financial auditors to use computer-related audit procedures when obtaining an understanding of clients’ internal controls during audit planning and to consider whether specialized skills, possessed by auditor’s staff or obtained through the use of IT audit specialists, are needed to determine the effect of IT on the audit and to understand, design, and perform tests of IT controls (AICPA 2001).

Academic research has also drawn attention to the impact of computerization and IT control problems on financial reporting and internal control over financial reporting. Three streams of research can be recognized: (a) research on the impact of computerization on internal control quality and financial reporting reliability, (b) research on the impact of IT control weaknesses on internal control quality, financial reporting reliability, financial performance, and audit fees, and most recently (c) research on the characteristics of firms reporting IT control weaknesses.
Evidence in the extant literature on the effect of computerization on financial reporting indicates that computerized environments are more prone to internal control problems and financial misstatements than partially computerized or non-computerized environments (Bell et al. 1998; Canada et al. 2009; Hunton et al. 2004; Messier Jr et al. 2004). Along the same lines, recent empirical evidence suggests that significant financial reporting implications may arise from relatively simple to extremely complex information systems (Curtis et al. 2009). For instance, there exists substantial evidence suggesting that enterprise resource planning (ERP) systems lead to heightened risks (IT, business, and overall control risks) and higher likelihood for financial misstatements, misclassifications, and defalcations (Hunton et al. 2004; Pfennig 1999; Sutton and Hampton 2003; Turner 1999). Less complex computerized systems, such as spreadsheets, have also been reported to cause internal control weaknesses and financial reporting problems (EUSPRIG).

The reported positive association between the complexity of computerized information systems and the likelihood of internal control weaknesses and financial misstatements has important implications for management and auditors. Generally speaking, the more complex a computerized environment, the higher the overall control risks, the greater the complexity of assessing internal control risks (Hunton et al. 2004; O'Donnell et al. 2000), and the greater the complexity of audit procedures in terms of the nature, staffing, timing, and extent of the audit testing (Brazel and Agoglia 2007; Janvrin et al. 2009).
Furthermore, empirical evidence in the Sarbanes-Oxley regime points to a host of negative consequences associated with reporting IT control weaknesses. Specifically, findings from recent studies show that IT control weaknesses are associated with a larger number of internal control deficiencies (Bedard and Graham 2011; Canada et al. 2009; Grant et al. 2008), a larger number of financial misstatements (Grant et al. 2008; Klamm and Watson 2009), lower financial performance (Stoel and Muhanna 2009), and higher audit fees (Grant et al. 2008).

Notwithstanding the evident impact of computerization in general and IT control weaknesses in particular on the effectiveness of internal control structure and the reliability of financial reporting, there is a paucity in theory-driven research on IT control quality in general and the antecedents of IT control weaknesses in particular (Li et al. 2007a). This lack of understanding can be attributed to the lack of public disclosures on IT control weaknesses prior to the enactment of Sarbanes-Oxley Act. This is because publicly traded companies were only required to disclose internal controls deficiencies, including IT control weaknesses, if they changed auditors (Krishnan 2005; SEC 1988; Whisenant et al. 2003). However, this situation has changed with the passage of SOX and the issuance of subsequent auditing standards by the PCAOB, specifically AS2 and AS5. Today, companies subject to Sarbanes-Oxley compliance and the PCAOB auditing standards must disclose material weaknesses in internal control including IT control weaknesses in their annual filing with the Securities and Exchange Commission (PCAOB 2007).
This dissertation argues that the lack of understanding about the determinants of IT control weaknesses has significant implications for managers, auditors and regulators who have a vested interest in achieving effective internal control over financial reporting, reliable financial reporting and prudent corporate governance practices.

Without a solid understanding of factors impacting the disclosure of IT control weaknesses, how they interact, and how they vary in terms of the magnitude and direction of their influence, the organizational endeavor to achieve effective IT control is likely to fail. For instance, such lack of understanding could lead organizations to direct their attention and much needed resources towards certain governance mechanisms while ignoring others that are more critical for achieving quality IT controls. Worse yet, organization could unconsciously put in place mechanisms that have conflicting influences on IT control quality.

1.4. Research Objectives and Questions
Evidence from the extant literature indicates that computerization increases the likelihood of internal control deficiencies and financial misstatements (Bell et al. 1998; Messier Jr et al. 2004). Furthermore, recent evidence on IT control quality suggests that IT control weaknesses are associated with a larger number of internal control deficiencies (Bedard and Graham 2011; Grant et al. 2008), a larger number of financial misstatements (Grant et al. 2008; Klamm and Watson 2009), lower financial performance (Stoel and Muhanna 2009), and higher audit fees (Canada et al. 2009; Grant et al. 2008). Combined, these pieces of evidence are indicative of the pervasive nature of information systems and
IT controls and their critical role in enabling or inhibiting effective internal control over financial reporting.

However, to the best of my knowledge, there exists no single study that has investigated the determinants of IT control weaknesses. In fact, apart from Li et al.’s (2007a) study which examined the impact of internal and external governance on IT control quality, this dissertation knows of no other research that has investigated the determinants of IT control weaknesses. Their study, however, suffers from three major limitations: (a) lack of theoretical grounding, (b) failure to consider other factors, besides IT governance, that may impact IT control quality, and (c) use of data from only the first year of Sarbanes-Oxley Section 404 compliance.

The current research purports to answer the following two questions:

(1) What are the antecedents of IT control weaknesses as reported under Section 404 of Sarbanes-Oxley Act of 2002?

(2) In what ways do the identified antecedents have an impact on IT control weaknesses?

This dissertation sets out to answer the aforementioned questions by presenting and testing an integrated theoretical model of the antecedents of IT control weaknesses. The proposed model draws on agency theory to provide a theoretical perspective of the occurrence of IT control weaknesses and the IT governance literature and the executive compensation literature to solicit potential factors that enhance or impede the achievement of effective IT controls. To this end, two categories of governance mechanisms were identified as potentially impacting the disclosure of IT control
weaknesses. These categories are: IT governance mechanisms and IT executive incentive alignment mechanisms.

The IT governance mechanisms involve two elements: first, the IT background element which includes (a) the IT background of the board of directors (BOD) as reflected by two of its main committees, namely the corporate governance committee and the audit committee and (b) the IT background of the top management team (TMT); second, the IT executive element as reflected in terms of the structural and the expert power of the Chief Information Officer (CIO). The IT executive incentive alignment mechanisms include two elements: (a) the CIO absolute compensation level and (b) the pay disparity between the CIO and other members of the TMT. These elements have never been examined empirically in one study. The proposed framework is further delineated in Chapter 3.

For testing the proposed model, this dissertation uses a sample of firms with IT control weaknesses as reported under Sarbanes-Oxley Section 404 for the years 2005-2009. In light of the preceding discussion, a conceptual framework is developed as presented in Figure 1 below:
1.5. Dissertation Structure

The remainder of this dissertation is organized as follows. Chapter Two presents a review of the extant literature covering two streams of research: (1) internal control research in the area of financial statements audit and (2) information technology control research in the area of accounting information systems. Particular attention is given to those studies that consider IT control weaknesses in the context of auditing internal controls over financial reporting. Chapter Three presents the theoretical perspective of the research as well as the research hypotheses. The potential determinants of IT control weaknesses are delineated and the corresponding hypotheses are developed. Chapter Four presents the research methodology, including data sources and empirical research models. Chapter Five presents and analyzes the results of the proposed model and hypotheses. The conclusions, limitations, and suggestions for future research are presented in Chapter Six.
Chapter 2 LITERATURE REVIEW

2.1. Introduction

In the wake of recent high-profile corporate governance scandals (e.g. Enron, WorldCom), the United States Congress enacted the Sarbanes-Oxley Act of 2002 which aims, among other things, to improve corporate governance effectiveness, internal control quality, and financial reporting reliability.

Section 404 of the Act, Management Assessment of Internal Controls, requires management of publicly traded companies to assess the design and operating effectiveness of internal control over financial reporting and to report that assessment in their annual filings with the Securities and Exchange Commission (SEC), namely in the 10-K forms. In the same vein, the Public Company Accounting Oversight Board’s (PCAOB) Auditing Standard (AS) No. 5 requires external auditors of publicly traded companies to understand, test, and evaluate the design and operating effectiveness of internal control over financial reporting and to opine on management’s report on the assessment of the effectiveness of internal control over financial reporting (PCAOB 2007).

Noteworthy is that, prior to the enactment of SOX, auditors did not formally conduct an audit of internal controls. Rather, they assessed internal controls only in conjunction with planning the audit (Bryan and Lilien 2005). Furthermore, publicly traded companies were required to disclose internal control weaknesses only in the event of changing auditors (Krishnan 2005; SEC 1988; Whisenant et al. 2003). Based on the lack of public disclosures up to the passage of SOX, research on internal control weaknesses is relatively recent.
Section 302 of the Act, *Corporate Responsibility for Financial Reports*, requires that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed with the SEC that

1. the signing officer has reviewed the report,
2. the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report,
3. the signing officers are responsible for establishing and maintaining internal control,
4. the signing officers have evaluated the effectiveness of the internal controls, and
5. the signing officers have disclosed to the auditors and the audit committee of the board of directors all significant deficiencies in the design or operation of internal controls and have identified for the auditors any material weaknesses in internal controls; and any fraud, whether or not material, that involves management or other employees who have a significant role in the internal controls (Congress 2002).

Recent evidence shows a positive association between SOX and internal control quality. For example, a recent survey of 171 internal auditors about their assessment of Section 404 benefits reports significant control improvements (Rittenberg and Miller 2005). In the same vein, Patterson and Smith (2007) examined the effects of SOX on auditing and internal control strength. Findings from their study led them to conclude that
“Sarbanes-Oxley has the desired effect of inducing stronger internal control systems and less fraud, but does not necessarily induce higher levels of control testing” (Patterson and Smith 2007).

Given the pervasiveness and ubiquity of information systems in today’s business processes (Canada et al. 2009; Klamm and Watson 2009), and the integral role that IT controls play in enabling or constraining internal control quality (Li et al. 2007a; PCAOB 2007) and financial reporting reliability (Grant et al. 2008; Klamm and Watson 2009), financial auditors are explicitly required to consider how an organization’s use of IT may affect internal control over financial reporting and how IT control risks could result in financial misstatements (AICPA 2007). To this end, auditors of publicly traded companies are required to assess the effectiveness of IT controls as they pertain to initiating, recording, processing, and reporting transactions or other financial data. Further, they are required to ensure that any significant weaknesses in IT controls are disclosed in the management’s assessment of internal control over financial reporting (AICPA 2007).

This dissertation is concerned with investigating the weaknesses in IT controls reported under Section 404 of the Sarbanes-Oxley Act. Here, IT controls are viewed as a subset of an organization’s internal control structure (AICPA 2001; Smith 2004). Therefore, it is natural that perspectives from internal control and IT control literatures would influence the current work.

The remainder of this chapter will proceed as follows. Section 2.2 discusses the internal control literature with a focus on internal control over financial reporting. Section
2.3 reviews the extant literature on IT controls as it relates to internal control over financial reporting. Finally, section 2.4 presents a synthesis of the current state of IT control and establishes the need for the following chapter.

### 2.2. Internal Control

This section presents a critical review of the extant literature in the area of internal controls. Practice-based literature (e.g. COSO 1992), regulatory legislations (e.g. Sarbanes-Oxley Act of 2002), auditing standards (e.g. SAS No. 109; AS No. 5), and academic research (e.g. Beasley 1996; Beasley et al. 1999; Cohen and Hanno 2000; Dechow et al. 1996; Hoitash et al. 2009; Krishnan and Visvanathan 2007; Krishnan 2005) have all emphasized the critical role of internal control structure in ensuring the integrity of the financial reporting process.

The importance of internal control quality is further evident in the dire consequences that are associated with internal control weaknesses. More specifically, empirical evidence from recent studies shows that internal control weaknesses are associated with more financial misstatements (Klamm and Watson 2009), higher risk and cost of capital (Ashbaugh-Skaife et al. 2009; Bryan and Lilien 2005), abnormally negative returns (Beneish et al. 2008), shareholders’ dissatisfaction (Ye and Krishnan 2008), negative stock price reactions (Gupta and Nayar 2007; Hammersley et al. 2008), higher audit fees (Hogan and Wilkins 2005; Hoitash et al. 2008; Raghunandan and Rama 2006), and increasing auditor resignations (Ashbaugh-Skaife et al. 2007; Ettredge et al. 2006; Krishnan and Visvanathan 2007). It is for these consequences that the objectives of ensuring financial reporting reliability, improving internal control quality, and fostering
effective corporate governance are at the heart of the recent regulatory changes under SOX.

The Securities and Exchange Commission (SEC) rules require the management of companies subject to Section 404 of SOX to base the evaluation of effectiveness of internal control over financial reporting on a suitable, recognized control framework (PCAOB 2007). Auditing Standard (AS) No. 5 requires external auditors to perform the audit of internal control over financial reporting using the same control framework used by management (PCAOB 2007). One such framework that has received wide acceptance and that is also recognized by the Public Company Accounting Oversight Board, is the Committee of Sponsoring Organizations of the Treadway Commission’s Internal Control-Integrated Framework of 1992; also known as the COSO framework.

Gupta and Thomson (2006) reviewed management’ assessments of internal control as filed with the SEC under Item 9A of most 10-K forms. Findings from their survey led them to conclude that “almost all the companies are unequivocally claiming that they conduct their internal control evaluation in accordance with the COSO 1992 Framework”.

Along the same lines, Campbell et al. (2006) cited a February 2003 report of the Institute of Internal Auditors (IIA) Research Foundation, titled “Internal Auditors’ Role in Corporate Governance,” which revealed that 63% of publicly traded companies use the COSO framework of internal control.

The COSO framework identifies five components of internal control: the control environment, risk assessment, control activities, information and communication, and monitoring. Most recently, Statement on Auditing Standards (SAS) No. 109 of 2007,
titled “Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement”, embraced the aforementioned components of internal control (AICPA 2007).

Geiger et al. (2004) examined the efficacy of the interrelated internal control components of the COSO framework in 32 Rhode Island state agencies that used the framework. Their study revealed that most internal control deficiencies were found in control activities and control environment with the former accounting for 31% of all deficiencies identified and the latter accounting for 23%. The authors concluded that “this finding may reflect that auditors have historically evaluated control activities in their internal control assessments, and may be better prepared to identify these types of weaknesses or more apt to search for control activities weaknesses.”. In a similar study, Klamm and Watson (2009) examined the interrelatedness of internal control deficiencies classified according to the COSO framework. Results from their study provide support of the interrelationships of the five COSO components.

Furthermore, the internal control literature distinguishes between two classes of internal control over financial reporting based on the pervasiveness and severity of their impact on financial reporting reliability: account or transaction-specific controls and entity-level controls. Account-specific controls relate to controls over specific account balances or transaction-level processes (Doss and Jonas 2004; Doyle et al. 2007). Entity-level controls, on the other hand, relate to more macro-level controls such as the control environment or the overall financial reporting process. More specifically, the SEC’s final management guidance defines entity-level controls as “aspects of a system of internal
control that have a pervasive effect on the entity’s system of internal control”. According to the same guidance, entity-level controls include:

(1) controls related to the control environment (e.g. management’s philosophy and operating style, integrity and ethical values, board or audit committee oversight; and assignment of authority and responsibility),

(2) controls over management override,

(3) the company’s risk assessment process,

(4) centralized processing and controls, including shared service environments,

(5) controls to monitor results of operations,

(6) controls to monitor other controls, including activities of the internal audit function, the audit committee, and self-assessment programs, and

(7) controls over the period-end financial reporting process; and policies that address significant business control and risk management practices (SEC 2006)

Using a sample of 261 companies that disclosed at least one material weakness in internal control under SOX for the period from August 2002 to November 2004, Ge and McVay (2005) found that entity-level material weaknesses in internal control tend to relate to deficient revenue-recognition policies, lack of segregation of duties, deficiencies in the period-end reporting process and accounting policies, and inappropriate account reconciliation. They further found that the most commonly identified account-specific material weaknesses occur in the current accrual accounts, such as the accounts receivable and inventory accounts.
Despite the indirect effect of entity-level controls on the likelihood of detecting or preventing a misstatement on a timely basis (Doyle et al. 2007; PCAOB 2007), practice and academic literatures seem to suggest that entity-level control weaknesses have more serious and negative effects compared to the less severe account-specific control weaknesses (Doss and Jonas 2004; Doyle et al. 2007; Gupta and Leech 2005). The following excerpt from Doss and Jonas (2004) illustrates Moody’s, (the bond rating company), philosophy with respect to the impact of disclosing material weaknesses in internal control on ratings:

We are less concerned about material weaknesses that relate to controls over specific account balances or transaction-level processes. We refer to these material weaknesses as “Category A” material weaknesses. In most cases, we believe that the auditor can effectively “audit around” these material weaknesses by performing additional substantive procedures in the area where the material weakness exists. We expect to give companies reporting Category A material weaknesses the benefit of the doubt and not take any related rating action, assuming management takes corrective action to address the material weakness in a timely manner. Other material weaknesses relate to company-level controls such as the control environment or the financial reporting process. These material weaknesses, which we refer to as “Category B” material weaknesses, may result in us bringing a company to rating committee to determine whether a rating action is necessary. We are concerned about these material weaknesses because we question the ability of the auditor to effectively “audit around” problems that have a pervasive effect on a company’s financial reporting. Also, Category B material weaknesses call into question not only management’s ability to prepare accurate financial reports but also its ability to control the business.

Along the same lines, Gupta and Leah (2005) examined the types of internal control deficiencies reported between November 1, 2003 and October 31, 2004. According to their study, internal control deficiencies related to entity-level controls represented the
majority of deficiencies. Li et al. (2007b) also found that material weaknesses in entity-level controls are less likely to be remediated compared to the less pervasive account-specific material weaknesses.

Raghunandan and Rama (2006) examined the impact of reporting deficiencies in internal control over financial reporting on audit pricing. They found that audit fees are positively associated with material weaknesses. In a similar study, Hoitash et al. (2008) found a significant positive association of audit pricing with both material and significant weaknesses in internal control over financial reporting. Furthermore, Hoitash et al. (2008) report a greater association of audit fees with entity-level control problems than with account-specific control weaknesses. The authors offer two potential explanations: (a) the companies with internal control weaknesses require the expenditure of greater audit engagement effort, and (b) the auditors’ application of risk premia compensates them for residual risk.

Most recently, there has been an effort to investigate the characteristics of the companies reporting internal control deficiencies and the underlying factors that are associated with their occurrence (e.g. Ashbaugh-Skaife et al. 2007; Bryan and Lilien 2005; Doyle et al. 2007; Krishnan and Visvanathan 2007; Krishnan 2005). For example, Krishnan (2005) examined the association between audit committee quality and the quality of corporate internal control between 1994 and 2000 (hence, before the passage of SOX). Using a sample of 128 companies that changed auditors and disclosed internal control problems and a control sample of companies that changed auditors but did not report internal control problems, the study found a negative association between the
proportion of independent members on the audit committee and the existence of internal control problems. Furthermore, the study found a negative association between the number of audit committee members with financial expertise and the existence of internal control problems.

Krishnan and Visvanathan (2007) studied the role of audit committees and auditors in the reporting of internal control deficiencies after the passage of SOX. The study found that, in comparison to firms with no weaknesses in their internal controls, firms that report internal control weaknesses are characterized by higher prior restatements of financial statements, higher number of meetings of the audit committee, smaller proportion of financial experts in the audit committee, and more auditor changes. These results, according to the authors, underscore the important role of internal corporate governance characteristics in examining the reporting of internal control weaknesses.

In the same vein, Li et al. (2007a) examined whether changes in external corporate governance characteristics (e.g. nature of audit firm, analyst following, and blockholder shareholdings) and internal corporate governance characteristics (e.g. board of director, audit committee, and management) are associated with the remediation of internal control material weakness disclosures reported under Section 404 of the Sarbanes-Oxley Act. Findings from their study show that improvements in internal corporate governance were associated with the remediation effort of internal control weaknesses. External governance improvements, however, were not found to be associated with the remediation of internal control material weaknesses. As noted by the authors, the positive association between the improvements in internal corporate governance on one hand and
remediation on the other hand, lends further support to the existing internal corporate governance regulations by SOX.

Bryan and Lilien (2005) found that firms with material weaknesses in internal controls are, on average, both smaller and worse performers than their matched industry counterparts with no material weaknesses. Ge and McVay (2005) also reported that disclosing a material weakness in internal control is negatively associated with firm size and firm profitability and positively associated with business complexity. Controlling for size, profitability, and complexity, they found a positive association between the disclosure of material weaknesses in internal control and the size of the audit firm. To this end, the authors note that “since large audit firms are exposed to a greater legal liability, they might be more diligent about searching for, and reporting, material weaknesses”.

In two concurrent studies, Ashbaugh-Skaife et al. (2007) and Doyle et al. (2007) examined the determinants of internal control problems. More specifically, Ashbaugh-Skaife et al. (2007) examined the determinants of internal control deficiencies based on a sample of 326 firms that disclosed material weaknesses, significant deficiencies and control deficiencies for Section 302 of SOX and prior to audits mandated by Section 404 of the Act (i.e., from November 2003 to December 31, 2004). They found that, relative to non-disclosers, firms disclosing internal control deficiencies have more complex operations, more recent changes in organizational structure, greater accounting risk, higher incidents of auditor resignations prior to the disclosure of internal control deficiencies and fewer resources to invest in internal control.
Using a sample of 779 firms disclosing material weaknesses from August 2002 to 2005, Doyle et al. (2007) examined determinants of *material* weaknesses in internal control and how the determinants of internal control problems differ based on the severity of material weaknesses disclosed (the more serious entity-level versus the less severe account-specific) and the stated reason of material weaknesses disclosed (staffing, complexity, and general). Findings from the study indicate that firms with internal control weaknesses were smaller in size, younger in age, weaker in financial health, more complex in operations, faster in growth, or undergoing restructuring. In addition, the study found that firms with more serious entity-level control problems are smaller, younger, and weaker financially, while firms with less severe account-specific problems are healthy financially but have complex, diversified, and rapidly changing operations. Furthermore, the study found that the determinants of internal control weaknesses vary based on the specific reason for the material weakness.

### 2.3. IT Control Over Financial Reporting

This section presents a critical review of the extant literature on IT controls, a subset of internal control. As part of assessing the effectiveness of internal controls over financial reporting, AU Section (319) requires management and auditors of companies subject to Section 404 of the Sarbanes-Oxley Act to test and evaluate the effectiveness of IT controls and report any significant IT-related weaknesses in their annual filing with the Securities and Exchange Commission (AICPA 2007).

For the purpose of this research, IT control is defined as a manual or automated process designed by, or under the supervision of, the company’s principal executive and
principal IT officers, or persons performing similar functions, and effected by the company’s board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial information and transactions and the continued proper operation of the information systems that capture, process, and generate them.

The IT control literature distinguishes between two classes of IT controls: application controls which are considered a type of account-specific internal controls and general controls which are considered a type of entity-level internal controls (SEC 2006). As the name suggests, application controls relate to individual computer applications. More specifically, they relate to detecting and preventing the financial misstatement and financial fraud risks associated with using IT to initiate, record, process, and report transactions or other financial data. These controls help ensure that transactions are authorized, and completely and accurately recorded and processed. Application controls may be automated (e.g. automated reconciliation of subsystems, an application that updates accounts in the general ledger for sub-ledger activity, an application control that tests input and output accuracy, etc) or exclusively or primarily manual but dependent on IT functionality (e.g. a control that manually investigates items contained in a computer generated exception report). When application controls are performed by people interacting with IT, they may be referred to as user controls (AICPA 2007, paragraphs 43-44; SEC 2006).

General controls, on the other hand, are defined as policies and procedures that relate to many applications and support the effective functioning of application controls by
helping to ensure the continued proper operation of information systems. General controls commonly include controls over data center and network operations, access security, IT management, system development, data security, change management, and business continuity planning (AICPA 2007, paragraph 45; Norman et al. 2009).

Faced with increasingly computerized business environments where key business processes including accounting and financial reporting are entirely automated or exclusively or primarily manual but largely dependent on IT functionality, auditing standards (e.g. SAS No. 94, SAS No. 109; AS No. 5), practice literature (e.g. COSO 1992; COBIT, 1996), and academic research (e.g. Bell et al. 1998; Canada et al. 2009; Grant et al. 2008; Klamm and Watson 2009; Li et al. 2007a; Messier Jr et al. 2004; Sutton and Hampton 2003) have all emphasized the integral role that information systems and IT controls play in enabling or constraining internal control quality, financial reporting reliability, and Sarbanes-Oxley compliance. To this end, a report by AMR Research, now a part of Gartner Inc., estimates that companies subject to SOX spent roughly six billion U.S. dollars a year in 2005 and 2006 to comply with the Act, 1.9 billion of which (i.e., 32%) was spent on IT (Bradford and Brazel 2007).

Audit standards setting bodies (e.g. AICPA; PCOAB) have increasingly emphasized that management and external auditors consider the effect of computerized systems and IT control risks when evaluating the effectiveness of internal control over financial reporting. Especially noteworthy is that the identification of information systems and IT control risks is not viewed as a separate evaluation but rather as an integral part of the
top-down approach used to identify the significant accounts and disclosures and the internal controls to test as part of Sarbanes-Oxley compliance (PCAOB 2007).

For example, AU Section (319), titled “Consideration of Internal Control in a Financial Statement Audit,” explicitly requires auditors to consider how an organization’s use of IT may affect internal controls relevant to the audit of financial statements and how IT risks could result in financial misstatements (AICPA 2007). More specifically, AU Section (319) requires auditors to obtain sufficient knowledge of how IT affects the following:

(1) the transactions in the entity’s operations that are significant to the financial statements,

(2) the procedures by which transactions significant to the financial statements are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements,

(3) the related accounting records, supporting information, and specific accounts in the financial statements involved in initiating, recording, processing, and reporting transactions, and

(4) the financial reporting process including the procedures used to prepare the entity's financial statements and related disclosures, and how misstatements may occur (AU Section 319.49-51 (AICPA 2007).

In the same vein, Statement on Auditing Standards (SAS) No. 94, titled *The Effect of Information Technology on the Auditor’s Consideration of Internal Control in a Financial Statement Audit*, alerts external auditors that assessing control risk at maximum
and relying only on substantive testing may not be effective for companies with intensively computerized financial reporting systems. To this end, the standard advises financial auditors to use computer-related audit procedures when obtaining an understanding of client internal controls during audit planning (AICPA 2001). Moreover, SAS No. 94 requires auditors to consider whether specialized skills, possessed by auditor’s staff or obtained through the use of IT audit specialists, are needed to determine the effect of IT on the audit, to understand the IT controls, or to design and perform tests of IT controls (AICPA 2001).

Academic research has also drawn attention to the impact of computerization and IT control problems on financial reporting and internal controls over financial reporting. Three strands of research can be recognized: (a) research on the impact of computerization on internal control and financial reporting reliability, (b) research on the impact of IT control quality on a host of issues including internal control quality, financial reporting reliability, financial performance, and audit fees, and (c) most recently research on the characteristics of firms reporting IT-related control weaknesses.

Evidence in the extant literature on the effect of computerization on financial statements suggests that computerized environments are more prone to internal control problems and financial misstatements than partially computerized or non-computerized environments (Bell et al. 1998; Canada et al. 2009; Hunton et al. 2004; Messier Jr et al. 2004). For example, Bell et al. (1998) examined the impact of computerization of information systems on the misstatement of financial information and whether the causes of misstatements vary between computerized systems and non-computerized systems.
Findings from the study suggest that misstatements are more likely to occur when accounting information systems are computerized than when they are not. In a similar study, Messier et al. (2004) found that the missing and poorly designed controls and the excessive workload for accounting personnel were more likely to be causes of misstatements in computerized business processes than in non-computerized business processes. Findings from Lynch and Gomaa (2003), who investigated the potential impact of information technology on the vulnerability of organizations to fraudulent employee behavior, show that information systems may provide sophisticated means and opportunities for fraud perpetration by employees. Consistent finds were reported in Beasley et al. (2000) and Ge and McVay (2005).

Using a sample of 261 companies disclosing at least one material weakness in internal control in their SEC filings from August 2002 to November 2004, Ge and McVay (2005) found that the greatest concentration of firms disclosing material weaknesses in internal control was in the computers industry with 21.4 percent of the material weakness firms. Notably, this percentage is far greater than the proportion of computer companies to all 2003 Compustat firms (13.7 percent). Moreover, the study found that 40 percent of ‘revenue recognition’ deficiencies occur within the computers industry; a finding that is consistent with Beasley et al. (2000) who reported a very high incidence of revenue fraud in technology companies. While the causality between computerization and IT control, on one hand, and disclosing internal control deficiencies, on the other hand, is not directly discussed by Ge and McVay (2005), the concentration of internal control deficiencies in the computers industry, presumably highly
computerized, provide support of the pervasive impact of information systems and IT control on a company’s internal control system.

Along the same lines, evidence suggests that significant financial reporting implications may arise from relatively simple to extremely complex information systems (Curtis et al. 2009). For instance, there exists substantial evidence suggesting that ERP systems lead to heightened risks (IT, business, and overall control risks) and higher likelihood for financial misstatements, misclassifications, and defalcations (Hunton et al. 2004; Pfennig 1999; Sutton and Hampton 2003; Turner 1999). Less complex computerized systems, such as spreadsheets, have also been reported to cause internal control deficiencies and financial reporting problems (EUSPRIG).

The reported association between the complexity of computerized information systems and the heightened likelihood of internal control deficiencies, financial misstatements, and/or fraud perpetration has important implications for management and auditors. Generally, the more complex a computerized environment, the higher the overall control risks, the greater the complexity of assessing IT and internal control risks (Hunton et al. 2004; O'Donnell et al. 2000), and the greater the complexity of audit procedures in terms of the nature, staffing, timing, and extent of the audit testing (Brazel and Agoglia 2007; Janvrin et al. 2009).

In addition, recent evidence on IT control quality points to a host of negative consequences associated with having IT control weaknesses. More specifically, empirical evidence from recent studies shows that IT control weaknesses are associated with a larger number of internal control deficiencies (Grant et al. 2008), a larger number of
financial misstatements (Bedard and Graham 2011; Canada et al. 2009; Grant et al. 2008; Klamm and Watson 2009), lower financial performance (Stoel and Muhanna 2009), and higher audit fees (Grant et al. 2008).

Bedard and Graham (2011) examined a sample of companies with problems in internal control over financial reporting under Section 404 of the Sarbanes-Oxley Act for the fiscal year 2004-2005. Results from their study show that 21.4% of all deficiencies in internal control over financial reporting were related to IT. Canada et al. (2009), also covering the same period, reported a slightly lower percentage (20.8%) of companies disclosing material weaknesses in their internal controls with at least one IT control weakness. A consistent finding was also reported by Grant et al. (2008) with 20% of accelerated filers having at least one control deficiency related to IT controls in the first three years of the Sarbanes-Oxley Section 404 compliance. Further results from their study indicate that companies with IT control weaknesses report significantly more internal control deficiencies (other than IT) than companies with no IT-control weaknesses. Klamm and Watson (2009) also found that firms with IT-related weaknesses report more non-IT-related material weaknesses than firms without IT-related weak components. These findings provide support not only to the pervasive nature of IT controls but also to the notion that IT control weaknesses exacerbate internal control deficiencies.

Grant et al. (2008) examined the impact of IT control weaknesses on financial reporting and financial misstatements. As noted by the authors, “six of the ten most commonly occurring accounting errors occur significantly more often in IT deficient
companies than non-IT deficient companies. These six accounting errors involved accounts with a high-level of transaction-based activity common to enterprise systems.” (p. 803). Klamm and Watson (2009) report that firms with IT-related weaknesses report more misstatements than firms without IT-related weaknesses. They further note that “the existence of an IT-related weakness generally has an incremental negative effect on reporting reliability.” Combined together, these findings are indicative of the pervasive nature of IT controls and their impact on financial reporting quality.

Stoel and Muhanna (2009) examine the impact of having material IT control weaknesses in internal control over financial reporting on financial performance. Results from their study indicate that firms reporting IT control weaknesses have lower accounting earnings compared to firms with strong IT controls. A possible explanation of the association between financial performance and IT-control deficiencies is that firms with poorer financial performance have fewer resources to allocate towards putting an effective IT control system in place. Another explanation may have to do with the expenditures that these firms incur to correct internal control weaknesses including IT-related problems. A third possible explanation is the disruptions to operations due to IT material weaknesses. In addition, Stoel and Muhanna (2009) found that IT control weaknesses moderate the association between accounting earnings and market valuation, with firms reporting weaknesses in IT controls having a lower earnings response coefficient. As noted by the authors, “information systems risk is priced by the capital markets”. Hence, IT control weaknesses are costly.
Further evidence on the cost of IT control weaknesses is found in Grant et al. (2008) and Canada et al. (2009) who examined the association between material weaknesses in IT control and audit fees. Both studies report that firms with IT control weaknesses are associated with higher audit fees when compared to firms with material weaknesses that are non-IT control related and firms with no material weaknesses. Echoing Hoitash et al. (2008), cited above, the positive association between audit fees and IT control weaknesses can be attributed to the idea that companies with IT control weaknesses require the expenditure of greater audit engagement effort. Another explanation could be the need to utilize the service of IT audit specialists. As noted by Curtis et al. (2009), “it might be assumed that the increased audit costs after discovery of material misstatements signal greater use of IS auditors, who typically bill at higher hourly fees than generalist auditors”.

Most recently, there has been an effort to investigate the characteristics of the companies reporting IT control deficiencies and the structural factors underlying their occurrence. Li et al. (2007a) examined the impact of internal and external governance on IT control quality for companies reporting IT-related material weaknesses in 2005. Findings from the study show that companies with favorable internal governance characteristics, specifically having more IT-experienced senior managers, CIO positions or longer tenured CIOs, are less likely to report IT-related material weaknesses. As for the influence of external governance characteristics, the study found that companies with higher percentages of independent board directors are associated with fewer IT material
weaknesses. However, partial evidence was found in support of the notion that more IT-experienced audit committee members are associated with fewer IT material weaknesses.

2.4. Synthesis

While research on IT control quality provides answers regarding the influence of IT control weaknesses on internal control deficiencies (Bedard and Graham 2011; Canada et al. 2009; Grant et al. 2008), financial reporting reliability (Grant et al. 2008; Klamm and Watson 2009), financial performance (Stoel and Muhanna 2009), management earnings forecast (Li et al. 2010) and audit fees (Canada et al. 2009; Grant et al. 2008), several other questions pertinent to IT control weaknesses remain unanswered. The current research attempts to answer the following two questions:

(1) What are the antecedents of IT control weaknesses reported under Section 404 of the Sarbanes-Oxley Act of 2002?

(2) In what ways do the identified antecedents have an impact on IT control weaknesses?

While recent studies have investigated the determinants of weaknesses in internal control over financial reporting (e.g., Ashbaugh-Skaife et al. 2007; Doyle et al. 2007), there is a paucity in theory-driven research on the antecedents of IT control weaknesses resulting in a lack of understanding of the determinants of IT control quality. In fact, apart from Li et al.’s (2007a) study, this dissertation knows of no other research that has investigated the determinants of IT control weaknesses. Li et al.’s (2007a) study, however, suffers from three major limitations: (a) lack of theoretical grounding, (b) failure to consider other factors other than IT governance that may impact IT control
quality, and (c) employing data from only the first year of Sarbanes-Oxley Section 404 compliance.

Without a solid understanding of the determinants of IT control weaknesses, how they interact, and how they vary in terms of the magnitude and direction of their influence, the organizational endeavor to achieve effective IT control is likely to fail. For instance, such lack of understanding could lead organizations to direct their attention and much needed resources towards certain governance mechanisms while ignoring others that are more critical for achieving quality IT controls. Worse yet, organizations could unconsciously put in place mechanisms that have conflicting influences on IT control quality.

The current study contributes to the existing literature by presenting an integrated theoretical model of the antecedents of IT control weaknesses. The proposed model draws on agency theory to provide a theoretical perspective of the occurrence of IT control weaknesses and the IT governance literature and the executive compensation literature to solicit potential factors that enhance or impede the achievement of effective IT controls. To this end, two categories of governance mechanisms were identified as potentially impacting IT control quality. These categories are: IT governance mechanisms and CIO incentive alignment mechanisms. For testing the proposed model, this dissertation uses a sample of firms with IT control weaknesses as reported under Sarbanes-Oxley Section 404 for the years 2005-2009.

By presenting and empirically testing a theory-based framework of the antecedents of IT control weaknesses, this dissertation offers a much needed understanding for (a)
managers in their effort to achieve effective IT governance and thus improve the quality of IT control and internal control over financial reporting, (b) financial auditors in their effort to obtain an understanding of what impacts IT control quality in a financial statement audit, and (c) regulators in their effort to improve financial reporting quality and foster effective corporate governance.
Chapter 3  THEORETICAL PERSPECTIVE & HYPOTHESES DEVELOPMENT

3.1. An Agency Theory Perspective

In spite of the evident impact of IT control weaknesses on the overall quality of internal control structure, the IT control research, especially in the area of IT control weaknesses, remains largely anecdotal with limited reliance on theory. This research proposes and tests an integrated theoretical model of the antecedents of IT control weaknesses. More specifically, this dissertation draws on agency theory (Eisenhardt 1989; Jensen and Meckling 1976) to provide a theoretical perspective of the occurrence and subsequent disclosure of IT control weaknesses. In general, an agency situation arises whenever one party (the principal) relies on another party (the agent) to perform some service on its behalf which typically involves the delegation of some decision making authority to the agent (Jensen and Meckling 1976).

The current work utilizes agency theory as the theoretical basis for two reasons: (1) the dominance of this theory as the guiding framework for corporate governance (Daily et al. 1998) of which IT governance is a subset and (2) the fact that the information systems (IS) function is in essence an agent that provides IT solutions and services to a principal; other business functions and the organization as a whole. In the context of Section 404 of Sarbanes-Oxley Act, the principal is the board of directors (BOD) who delegates to the top management team (TMT) the responsibility of corporate governance including internal control over financial reporting. The agent, on the other hand, is the top IS team (TIST) to whom the TMT delegates the responsibility of IT control governance. Such delegation is normally caused by business functions’ lacking
the time and resources, specifically specialized IT skills and knowledge, which are necessary to govern IT control over financial reporting.

A central problem that could arise in such principal-agent relationship is one of moral hazard or goal incongruence; a situation where agents engage in self-interested behavior driven by their own objectives and interests rather than those of their principals (Baiman 1982; Baiman 1990; Jensen and Meckling 1976). Evidence from agency theory literature indicates that when such goal incongruence occurs, it could lead to the principal’s interests being ill-served by the agent which could prove very harmful to the well-being of the principal. Extrapolated to the context of IT control weaknesses, this evidence would suggest that the occurrence and subsequent disclosure of IT control weaknesses is a manifestation of an agency problem caused by goal disagreement between the BOD and the TIST.

The first question that arises is: why would such goal incongruence occur? More specifically, why would the top IS team, as an agent, have different goals and/or be less committed to designing and implementing a system of IT controls that is consistent with the organization’s internal control objectives? According to agency theory, goal incongruence between the principal and the agent is affected by information. (Baiman 1982; Eisenhardt 1989; Tuttle et al. 1997). To this end, agents are less motivated to act in a way that is contrary to the objectives of their organizations when the principals possess some or complete information that enable them (i.e., the principals) to verify the quality and adequacy of the agents’ actions; a condition known as information symmetry. However, when the principals cannot completely monitor and verify the actions of the
agents due to an information gap, the condition becomes one of information asymmetry (Baiman 1982; Tuttle et al. 1997). Here, agents are said to possess privately held information or knowledge which could motivate them to act contrary to the objectives of their organizations without fearing detection.

Another explanation as to what could cause the goal incongruence is offered by motivation theories such as expectancy theory (Vroom 1964) and equity theory (Adams 1965). That is, when people have unfavorable perceptions about their performance outcomes (e.g. recognition, rewards, pay), they are more likely to engage in self-interested behavior. Furthermore, when people perceive the ratio of their outcomes to their inputs (e.g. effort, education, expertise) to be inequitable to that of their referents, the situation becomes one of perceived inequity which can cause them to behave in ways that are not in line with the objectives of their organizations (Henderson and Fredrickson 2001; Lazear 1989). In the context of the current study, this would suggest that IT executives who perceive their outcomes unfavorably or as inequitable are more likely to engage in self-interested behavior driven by their own objectives as opposed to those of their organizations.

The second question that follows is: how can the TIST, whose motives may not be aligned with those of the organization, be influenced to behave in a way that is consistent with the organization’s internal control objectives? According to the corporate governance literature, the answer to this agency problem involves development and implementation of effective governance mechanisms whose aim is to reduce the agency costs and provide monitoring over the actions of the agent (Coles et al. 2001; Daily et al.
2003a; Daily et al. 2003b). More specifically, this research adopts the view that there are two important categories of governance and/or contracting mechanisms that the BOD can employ in order to align the interests of the TIST with the interests of the firm. These categories are: IT governance mechanisms and IT executive incentive alignment mechanisms.

3.1.1 IT Governance and IT Control Quality

Boynton et al. (1992) define IT governance as “the locus of decision making for IT-related processes within a firm where the concern is with the location, distribution, and pattern of managerial responsibilities and control that ultimately affect how IT resources are applied and then implemented” (Boynton et al. 1992). The IT Governance Institute defines IT governance as “an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives” (ITGI). Another definition is offered by Weill and Ross (2004) who define IT governance as “specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT”. Two underlying themes can be noted in the aforementioned definitions: the locus of decision authority and responsibility for IT-related activities and processes and the alignment between business and IT to ensure desirable behavior in the use of IT.

In theory, IT governance; an integral part of corporate governance, is the responsibility of the board of directors. In practice, however, the board delegates the responsibility of corporate governance including internal control over financial reporting to the TMT, primarily the CEO and CFO. The TMT, in turn, delegates fully or partially
to the TIST the authority to make key IT control decisions as well as the responsibility to
design and implement IT controls over financial reporting systems. Drawing on the IT
governance literature, this research proposes two IT governance elements to influence the
alignment between the TIST and the BOD: (1) the IT background element which includes
(a) the IT background of the corporate governance committee, (b) the IT background of
the audit committee and (c) the IT background of the top management team (TMT) and
(2) the IT executive element in terms of whether or not the firm has a CIO and the power
of the CIO.

The responsibilities of the corporate governance committee include, but are not
limited to, reviewing and making recommendations to the BOD regarding matters
pertaining to corporate governance, reviewing the composition of committees of the BOD
including the audit committee, and recommending persons to be members of such
committees. The audit committee, on the other hand, is responsible, among other things,
for reviewing the company’s system of internal control over financial reporting,
monitoring the integrity of the company’s financial statements, and ensuring the
company’s compliance with laws and regulations including the Sarbanes-Oxley Act of
2002. To this end, the Auditing Standard (AS) No. 5 requires external auditors of
publicly traded companies to communicate, in writing, to the audit committee all material
weaknesses in internal control as identified during the audit of internal control over
financial reporting. This written communication should be made prior to the issuance of
the auditor's report on internal control over financial reporting. In light of these
responsibilities, it can be argued that corporate governance committees with IT
background are more likely to recommend IT experienced persons for the membership of the audit committee.

Drawing on agency theory and the notion of information asymmetry, this research expects organizations with IT-experienced corporate governance and audit committees to exhibit lower levels of IT knowledge gap and thus lower information asymmetry between the BOD and the TIST. The same is true for firms with IT-experienced TMTs. In such organizations, the BOD and the TMT are in a better position to monitor and verify the actions taken by the TIST in the course of governing IT controls over financial reporting. At the same time, the TIST, whose actions are being monitored and verified, is less motivated to implement a system of IT controls that is not consistent with the organization’s internal control objectives. This, in turn, is expected to result in better IT controls; hence fewer IT control weaknesses.

Moreover, IT knowledgeable boards and top management teams are likely to have a better understanding and appreciation of the risks associated with using IT in capturing and processing business and financial transactions and the negative impact of IT control weaknesses on internal control and financial reporting. Further, organizations with IT experienced corporate governance and audit committees are more likely to instruct the TMT to provide adequate support and resources to the TIST to design and implement an effective system of IT controls and to resolve IT control weaknesses as they arise. This, in turn, results in fewer IT control weaknesses. Therefore, this research posits that:

**H1a:** Companies with corporate governance committee members who do not have an IT-related background are more likely to have IT control
weaknesses relative to companies with corporate governance committee members who have an IT-related background.

**H1b:** Companies with audit committee members who do not have an IT-related background are more likely to have IT control weaknesses relative to companies with audit committee members who have an IT-related background.

**H1c:** Companies with top management team members who do not have an IT-related background are more likely to have IT control weaknesses relative to companies with top management team members who have an IT-related background.

The second IT governance element is the IT executive. For the sake of simplicity and consistency with the extant literature, the current study uses the chief information officer (CIO) title to refer to the top IT executive in an organization. Numerous IS researchers have emphasized the fundamental role that CIOs play in dictating the performance of and deriving value from IT in organizations (Earl and Feeny 1995; Preston et al. 2008; Raghunathan and Raghunathan 1989). Figure 2, adopted from Preston et al. (2008), presents a summary of the literature on the CIO’s influences on organizational performance.

While there is an extant body of research on the impact of CIOs on organizational performance, the research on the impact of CIOs on the quality of IT control over financial reporting remains fairly new.

Recent empirical evidence indicates that firms with CIO positions are less likely to have IT-related control weaknesses (e.g. Li et al. 2007a). Notwithstanding this evidence, it is important to note that many firms with CIO positions still disclosed IT control
weaknesses. This suggests that the impact of the IT executive on the quality of IT control goes beyond the presence of the position itself. One way to further investigate this impact is by considering IT executive power and his/her decision making authority within an organization. Here, power is seen as an enabler of authority. Finkelstein (1992) distinguishes between four dimensions of power: structural power, expert power, ownership power and prestige power. This research focuses on the first two dimensions because prestige power and ownership power are more relevant to chief executive officers (Preston et al. 2008).

<table>
<thead>
<tr>
<th>Study</th>
<th>Theory / Framework</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Raghunathan &amp; Raghunathan, 1989)</td>
<td>Organizational Theory Literature</td>
<td>The organizational rank of the CIO influences the level of IT effectiveness within the organization.</td>
</tr>
<tr>
<td>(Boynton et al., 1994)</td>
<td>Absorptive Capacity</td>
<td>IT use is influenced by managerial IT knowledge, which is in turn influenced by the managerial climate of the organization.</td>
</tr>
<tr>
<td>(Katimi et al., 1996)</td>
<td>Miles and Snow Typology</td>
<td>The CIO's rank and strategic role within the organization are linked to the competition in the strategic roles of the organization.</td>
</tr>
<tr>
<td>(Armstrong &amp; Sambamurthy, 1999)</td>
<td>Resource-Based View; Knowledge-Based View of the Firm</td>
<td>CIO business knowledge and IT knowledge significantly influence IT assimilation.</td>
</tr>
<tr>
<td>(Chatterjee et al., 2001)</td>
<td>Resource-Based View</td>
<td>Announcements of newly created CIO positions improve the market valuation of firms.</td>
</tr>
<tr>
<td>(Johnson &amp; Lederer, 2005)</td>
<td>Strategic Management Literature</td>
<td>A convergent view of the current role of IT within the organization between the CIO and CEO influences the contribution of IT to the firm's financial performance.</td>
</tr>
<tr>
<td>(Karahanna &amp; Chen, 2006)</td>
<td>Resource-Based View</td>
<td>Firms with effective CIOs are consistently more profitable, have lower total operating expenses, and have a higher stock valuation than the average firm in the industry.</td>
</tr>
</tbody>
</table>

Note: CEO = Chief Executive Officer, CIO = Chief Information Officer, IT = information technology.

Figure 2: CIO's impact on organizational outcome, adopted from Preston et al. 2008
The extant CIO literature describes CIO structural power in terms of the CIO’s formal membership in the TMT (Preston et al. 2008; Raghunathan and Raghunathan 1989). The CIO is expected to have greater authority in influencing the performance of IT in organizations including the quality of IT control over financial reporting when the organization officially elevates his/her power so that he/she is at peer level with other executives in the top management team. Echoing an argument by Preston et al. (2008), the current study argues that a CIO who is (is not) at peer level with the firm’s TMT will be more likely (less likely) to be accepted into the firm’s inner circle and therefore will be more successful (less successful) in influencing other members of the TMT (Chatterjee et al. 2001; Earl and Feeny 1995; Preston et al. 2008). Therefore, the following hypothesis will be tested:

**H2a:** Companies with CIOs who have a lower level of structural power are more likely to have IT control weaknesses relative to companies with CIOs who have a higher level of structural power.

Regarding expert power, there exists evidence in the extant literature to suggest that the decision making authority of executives is not only contingent on their possession of relevant expertise in their respective functional areas but also on how other members of the TMT perceive their effectiveness (Preston et al. 2008; Yukl and Yukl 2002). Accordingly, and consistent with Preston et al. (2008), the CIO expert power is described in terms of the extent to which the CIO is perceived as effective by the other members of the TMT. Here, the perceived effectiveness of the CIO is seen as important as, if not more important than, the possession of IT expertise.
The perceived effectiveness of the CIO can be further described in terms of how long the CIO has been in the current position. Drawing on stewardship theory, the current research views longer CIO tenure as indicative of effectiveness and good stewardship. CIOs that are perceived to be good stewards will be entrusted by the TMT to make key IT decisions (Chan et al. 2006) and will retain their positions longer than CIOs that are perceived to be ineffective. Furthermore, the present study argues that longer CIO tenure enables CIOs to build stronger and more lasting relationships with other members of the TMT giving the CIO greater latitude in advising and influencing other TMT members (Earl and Feeny 1995; Preston et al. 2008). Moreover, longer CIO tenure enables the CIO to obtain a more comprehensive and undisrupted understanding of the organization’s information systems; its structures, strengths and weaknesses; and also the organization’s overall operations. Not only is this understanding paramount to a CIO’s ability to align IT and business and thus derive value from IT but it is also critical to the CIO’s ability to manage and mitigate the risks associated with using IT. Therefore, this research posits that:

**H2b:** Companies with CIOs who have lower expert power are more likely to have IT control weaknesses relative to companies with CIOs who have higher expert power.

3.1.2 CIO Compensation and IT Control Quality

While this research acknowledges the importance of IT governance mechanisms in decreasing information asymmetry and increasing alignment between the BOD and the TIST, it also recognizes the reality that the behavior of the TIST is subject to the
influence of multiple factors. Therefore, a pragmatic theoretical perspective must consider other mechanisms that influence IT control quality either directly or indirectly through influencing the TIST’s behavior. One such mechanism is executive compensation structure.

The executive compensation stream of research, firmly grounded in agency theory (Daily et al. 2003b; Murphy 1999), argues that organizations need to engage in incentive contracting with the TMT to address the agency problem caused by information asymmetry and the high costs associated with monitoring the TMT’s behavior. As such, executive compensation structure is viewed as an alignment mechanism which the board of directors can use to motivate TMT members to align their interests with those of the shareholders (Coles et al. 2001; Core et al. 1999; Daily et al. 2003b; Himmelberg et al. 1999).

Studies within this stream of research examine the association between TMT pay and firm performance with a majority investigating the relation between CEO compensation and firm performance. The focus on CEO pay can be attributed to the crucial role of CEOs as heads of TMTs and the implicit view of the CEO pay as a proxy for the TMT pay (Jonas 2007).

Recently, and as more executive compensation data became available, many studies extended their examination to include the association between TMT pay disparity and firm performance (e.g., Carpenter and Sanders 2004; Henderson and Fredrickson 2001; Main et al. 1993). Generally, when employees perceive the ratio of their performance outcomes (e.g. compensation, promotion, etc) to their inputs (e.g. effort, time, education,
skills, etc) to be lower than that of others, the situation becomes one of perceived inequity (Adams 1965). Within the context of executive compensation research, a central theme is that TMT pay disparity that is perceived to be inequitable can cause members of the TMT to engage in self-interested and uncollaborative behavior (Henderson and Fredrickson 2001; Lazear 1989) leading to negative impacts on firm performance (Carpenter and Sanders 2004).

Drawing on the executive compensation literature, the present study argues that CIO compensation influences the CIO’s behavior and the alignment between the organization and the TIST in two ways. First, CIO absolute pay is viewed as an incentive alignment mechanism. That is, CIO compensation is a means to reduce agency costs and to induce the CIO to make IT-related decisions and take actions that are in line with IT governance objectives (e.g. create value from IT, mitigate IT risks, and achieve regulatory compliance). As the level of CIO absolute pay increases, the CIO’s motivation to engage in behaviors or actions that are not in the best interest of the organization is reduced. Therefore, CIOs with higher absolute compensations should be more committed towards enhancing the quality of IT controls and correcting IT control weaknesses as they arise. This discussion leads to the following hypothesis:

**H3a**: Companies with CIOs who have lower absolute pay are more likely to have IT control weaknesses relative to companies with CIOs who have higher absolute pay.

Second, CIO relative pay, measuring the pay disparity between the CIO and other members of the TMT, is viewed as a proxy of CIO perceptions of equity. Here, lower
relative pay is seen as indicative of higher level of perceived inequity. Evidence from the executive compensation literature and pay disparity research indicates that inequity perceptions can cause members of the TMT to engage in self-interested behavior. Extrapolated to the context of the CIO-TMT pay disparity, this evidence would suggest that CIOs who perceive their compensations as inequitable will be less committed to organizational objectives and thus less motivated to design and put in place a system of IT controls that is consistent with the organization’s internal control objectives.

The present study views the CIO-TMT pay gap as a proxy of CIOs level of acceptance by other members of the TMT. That is, a higher (lower) pay gap between the CIO and other members of the TMT is an indication of a lower (higher) level of CIO acceptance by the TMT. As such, CIOs who are faced with lower levels of acceptance should be less committed to organizational objectives. Such CIOs, whose inputs may not be valued or even sought by the TMT, are less likely to collaborate and coordinate with other members of the TMT and less motivated to implement effective IT controls. This, in turn, could be expected to result in lower quality IT controls; hence, more IT control weaknesses. Based on the preceding discussion, the following hypothesis will be tested:

**H3b**: Companies with CIOs who have lower relative pay are more likely to have IT control weaknesses relative to companies with CIOs who have higher relative pay.

### 3.2. Summary of Hypotheses and Research Model

Table 1 below summarizes the hypotheses and respective expectations.

[Insert Table 1 about here]
Except for H1b, H1c and H2b, of which close variations were tested in Li et al. (2007a), the hypothesized relationships are original and theory-driven and have never been examined empirically in a single study. In light of the hypothesized relationships, a research model is presented in Figure 3. This model places IT governance and CIO alignment incentive mechanisms in a nomological network relating these mechanisms to the presence (absence) of IT control weaknesses.
Figure 3: Theoretical Research Model
Chapter 4  RESEARCH METHODOLOGY

In this chapter, the data sources and the sample selection criteria are presented. Next, the study variables are identified as well as how they are measured. Finally, the research method and the statistical models are described. These models will be used to test the research hypotheses presented in the previous chapter.

4.1 Data Sources and Sample Selection

Data for this research comes from two main sources: Audit Analytics database and proxy statements. Coverage in these data sources is required for firms to be included in the sample.

The initial study sample consists of firms that reported IT control weaknesses under Section 404 of Sarbanes-Oxley Act for the years 2005-2009. Given the unique nature of foreign firms in terms of the varying legal, cultural, political, and economic environments in which they operate and in order to avoid the complexities and discrepancies that may arise from currency conversions (e.g. currency rate fluctuations, purchasing power disparity), such firms are eliminated from the study sample.

The identification of IT control weakness firms is performed in two steps. The first step involves identifying firms with internal control weaknesses. Audit Analytics database tabulates a wide range of variables pertaining to companies subject to SOX Section 404 compliance. Noteworthy is that Audit Analytics has been widely used in both internal control studies (e.g., Ashbaugh-Skaife et al. 2009; Doyle et al. 2007) and IT control studies (e.g. Klamm and Watson 2009; Li et al. 2007a). Of special interest is a
dummy variable (Yes/No) in Audit Analytics indicating the effectiveness (or ineffectiveness) of firms’ internal controls as reported in the auditor’s assessment of the effectiveness of internal control over financial reporting, namely 10-K reports. Thus, the initial pool of firms consists of those firms that received an adverse opinion on their internal controls from January 2005 to December 2009. The second step involves identifying IT control weakness firms. For each of the firms identified in the first step above, the different categories of internal control weaknesses as reported in Audit Analytics are examined to identify the firms that reported at least one IT-related weakness.

Following the recommendations of Barber and Lyon (1997) and Desai et al. (2006), and the approach used by Li et al. (2007a) and Grant et al. (2008), the present study uses Audit Analytics to identify a control group of firms that reported non-IT control weaknesses during the study period. Firms in the study sample and the control group are matched on industry (4-digit, 3-digit, or 2-digit SIC) and size (revenues) so that each firm with an IT-related weakness is matched with a similar control firm that reported internal control weaknesses but no IT weaknesses. This should provide a baseline for understanding the incremental impact of the proposed governance elements on the disclosure of IT control weaknesses. If a match is not found, the IT control weakness firm is dropped from the sample.

Data on IT governance and executive compensation are available in the annual proxy statements which publicly traded firms are required to file in compliance with SEC regulations. I hand-collect this data by searching these statements using Mergent Online.
database which provides a full text Internet-based search into a wide range of data including SEC filings.

For each firm in the study sample and the control group, I search the proxy statements for information about the educational and professional background of the individuals who were members of its corporate governance committee, audit committee, and top management team in the year of disclosing an internal control weakness or the preceding year. I carefully read the biographies of these members as disclosed in the proxy statements to determine if they have IT background or not. For example, if a member previously held an IT executive position, held a senior executive position in an IT company (e.g. software, programming, database or Internet companies), worked as an IT auditor/consultant, or received a university degree in an IT related field (e.g. computer science, information systems), I consider this individual as having an IT background.

Next, I search the proxy statements for information on whether or not a firm had an IT executive in the year of disclosing an internal control weakness or the preceding year. Given the fact that IT executives’ titles vary among organizations, I use a host of job titles in my search: chief information officer (CIO), chief technology officer (CTO), chief information security officer (CISO), executive vice president IT/IS, and senior vice president IT/IS. If the search yields no results, I relax the search criterion by using more general phrases such as “information technology” and “information systems” and I carefully read the search results to look for other titles that firms may have assigned to their IT executives. If none of the above procedures returns a senior management position with an IT-related job title, I deem the firm as having no IT executive.
For firms with IT executive positions, I search the proxy statements to document the number of years the IT executives have been in their current positions. As pointed out in chapter 3, the present study views tenure as a proxy of the IT executive expert power. I also document the age of the identified IT executives and whether or not they have an IT-related background. I capture information about the IT background of IT executives because some firms assign the IT executive title to business executives who do not necessarily have an IT background or expertise. Next, I carefully examine the list of named executive officers (NEO’s) as reported in annual proxy statements, namely in form DEF 14A. If the identified IT executive is listed among the firm’s NEOs, I deem the executive as a member in the top management team. As pointed out earlier, the current research views membership in the TMT as a proxy of the IT executive structural power.

Executive compensation data comes from the annual proxy statements as well. For each firm with an IT executive, I examine the Summary Compensation Table in the DEF 14A form. If the firm disclosed the IT executive’s compensation information, I document that information as well as the compensation information for the TMT.

All other data (financial data and industry type) are extracted from Audit Analytics.

4.2 Sample for Study

The study sample consists of US firms that reported IT control weaknesses under Section 404 of SOX from January 2005 to December 2009. The initial sample consists of 1,712 firm-year observations with internal control weaknesses and 381 firm-year observations with at least one IT control weakness. After eliminating foreign firms, the sample size drops to 358 firm-year observations with one or more IT-related control
weaknesses. In order to study the impact of IT governance and CIO compensations on the disclosure of IT control weaknesses, a matched pairs approach was used where IT control weakness firms were matched with similar firms that reported internal control weaknesses but no IT weaknesses. Consistent with the extant literature, this matching process was conducted based on industry (4-digit, 3-digit, or 2-digit SIC) and size (revenues at the end of the fiscal year in which the firm reported an internal control weakness). If a firm-year observation has no appropriate match based on the 4-digit SIC code, then the 3-digit SIC code is used to find a match. If no match is found, the 2-digit SIC code is used. If no match is found based on the 2-digit SIC code, the firm-year observation is dropped from the sample. The matching process resulted in eliminating 172 firm-year observations which brought the sample size to 180 firm-year observations with at least one IT control weakness. After eliminating firms for which no data was available for independent variables (18), the sample size dropped to 162. Thus, the final sample consists of 162 firm-year observations with one or more IT-related control weaknesses matched with 162 firm-year observations with non-IT weaknesses. These two samples are referred to as the “study group” sample and the “control group” sample, respectively. Table 2 provides a summary of the sample selection process.

At the end of the matching process, 40 percent of the firm-year observations in both groups were matched based on the 4-digit SIC code, 20 percent on the 3-digit SIC code, and 40 percent on the 2-digit SIC code. In order to assess the goodness of the matching
procedure and that the study sample is not materially different from the control group, a t-test was conducted to examine whether the difference in size, measured in terms of total revenues, between firms in the two groups is statistically significant. Table 3 provides a comparison of the mean revenues between the two groups for each of the fiscal years covered as well as for the entire period. Although firms in the study group are smaller, on average, than their counterparts in the control group, the t-tests indicate that the differences in revenues are not statistically significant for the 5 years suggesting that the matching procedure was successful. In addition, Table 3 provides a comparison of the two groups in terms of total assets, as another measure of size. The difference in total assets between firms in the two groups was not statistically significant providing further support for the goodness of the matching procedure.

[Insert Table 3 about here]

4.3 Measured Variables

The current study uses three classes of variables: dependent variables, independent variables, and control variables. Definitions and measures of these variables are presented below.

4.3.1 Dependent Variables

The disclosure of IT control weaknesses (ITCW) is the only dependent variable in this research. It is an indicator variable that is equal to 1 if the firm disclosed an IT-related weakness in its Section 404 report and 0 if the firm is a control firm (i.e. disclosed an internal control weakness but not an IT-related weakness).
4.3.2 Independent Variables

4.3.2.1 IT Governance Variables

The IT background of the corporate governance committee (CORGOVIT) variable refers to whether members of the committee previously held CIO positions, whether they were IT consultants, or whether they worked as senior managers in IT companies (e.g., software, programming, database or internet companies). It is an indicator variable that is equal to 1 if the corporate governance committee had at least one member with an IT background in the year of disclosing an IT control weakness and/or the preceding year.

The IT background of the audit committee (AUDITIT) variable refers to whether members of the committee previously held CIO positions, whether they were IT consultants, or whether they worked as senior managers in IT companies (e.g., software, programming, database or internet companies). It is an indicator variable that is equal to 1 if the audit committee had at least one member with an IT background in the year of disclosing an IT control weakness and/or the preceding year.

The IT background of the top management team (TMTIT) variable refers to whether members of the TMT previously held CIO positions, whether they were IT consultants, or whether they worked as senior managers in IT companies (e.g., software, programming, database or internet companies). It is an indicator variable that is equal to 1 if the TMT had at least one member with an IT background in the year of disclosing an IT control weakness and/or the preceding year.

The CIO structural power (CIOSPWR) variable refers to the CIO formal membership in the top management team (TMT). For the purpose of this research, a CIO is considered a member of the TMT if the firm listed him/her as one of its named executive officers.
(NEOs). Therefore, this variable is an indicator variable that is equal to 0 if the firm had a CIO who was not a named executive officer and 1 if the CIO was a named executive officer in the year of disclosing an IT control weakness and/or the preceding year.

The CIO expert power (CIOEPWR) variable refers to the perceived effectiveness of the CIO which is measured in terms of how long, in years, the CIO has been in the current position.

4.3.2.2 Executive Compensation Variables

The CIO compensation (CIOCOMPS) refers to the CIO absolute pay in a given year and is based on the sum of the CIO annual salary and bonus. The CIO relative compensation (CIOTMTS) refers to the CIO-TMT compensation gap which is derived by computing the ratio of the CIO annual salary and bonus (CIOCOMPS) to the average annual salary and bonus of the non-IT executive in the TMT.

4.3.3 Control Variables

While this research is concerned with firms reporting at least one IT control weakness, it is important to note that all firms included in this study have internal control weaknesses. Therefore, in addition to the hypothesized relationships, this research includes control variables that have been found to impact the disclosure of internal control weaknesses, including IT-related weaknesses, and that may impact other study variables.

Evidence from the extant research on internal controls suggests that less profitable firms are more likely to disclose internal control weaknesses or have misstated accounts (Ashbaugh-Skaife et al. 2007; Doyle et al. 2007; Ge and McVay 2005). Firms with lower
profitability have fewer resources to allocate towards implementing effective internal control systems and/or correcting internal control weaknesses including IT-related problems. Therefore, this research includes return on assets (ROA) to control for profitability.

Further research evidence points to a positive association between the disclosure of internal control weaknesses and the size of the audit firm. As noted by Ge and McVay (2005) “since large audit firms are exposed to a greater legal liability, they might be more diligent about searching for, and reporting, material weaknesses”. Therefore, this research includes a variable to control for the size of the audit firm (Big4). This variable is an indicator variable that is equal to 1 if the audit firm in the year of disclosing an IT control weakness and/or the preceding year was one of the big four and 0 otherwise.

Another variable that has been shown to have a relationship with two of the study variables is firm size. Specifically, evidence from the extant research on internal controls suggests that smaller firms are more likely to disclose internal control weaknesses (Ashbaugh-Skaife et al. 2007; Doyle et al. 2007; Ge and McVay 2005). Furthermore, evidence from the extant research on executive compensation suggests that larger firms tend to reward their executives with larger compensation packages (Baker and Hall 2004; Coles et al. 2001). However, since the present study uses firm size, measured in terms of total revenues, to match IT control weakness firms with non-IT control weakness firms, this variable will not have any impact on the disclosure of IT control weaknesses and thus will not be included as a control variable.
In addition to the aforementioned variables, the present study includes a control variable to capture the effect of the CIO background (CIOBACK) on the odds of disclosing an IT control weakness. The decision to add this variable is because some firms assign the IT executive title to business executives who do not necessarily have an IT background and expertise. Therefore, this variable is an indicator variable that is equal to 1 if the CIO had an IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

Table 4 provides functional descriptions of all the variables along with their data sources.

[Insert Table 4 about here]

4.4 Method

The present study uses logistic regression to investigate and test the relationship between the disclosure of IT control weakness and the proposed governance elements. Hypotheses 1 and 2 ascertain the association between the IT governance elements and the disclosure of IT control weaknesses. These hypotheses are tested using Model (1) which is divided into two sub models: Model 1a and Model 1b.

Model 1a tests H1a, H1b, and H1c regarding the relationship between the disclosure of IT control weaknesses as a dependent variable and (a) the IT background of the corporate governance committee, (b) the IT background of the audit committee, and (c) the IT background of the top management team as independent variables, respectively.
The model controls for the client firm profitability and the size of the audit firm. The expectation is that the coefficients of $\beta_1$, $\beta_2$, and $\beta_3$ will be negative and significant.

\[
\text{ITCW} = \beta_0 + \beta_1 \text{CORGOVITIT} + \beta_2 \text{AUDITIT} + \beta_3 \text{TMTIT} + \beta_4 \text{ROA} + \beta_5 \text{BIG4}
\]

Where:

ITCW = 1 if the firm disclosed an IT-related control weakness in Section 404 report; 0 otherwise (control firm).

CORGOVITIT = 1 if the corporate governance committee had IT background in the year of disclosing an IT control weakness and/or the preceding year; 0 otherwise.

AUDITIT = 1 if the audit committee had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

TMTIT = 1 if the top management team had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

ROA = Income Before Extraordinary Items divided by the average of the current year’s Total Assets and the prior year’s Total Assets, multiplied by 100.

BIG4 = 1 if the audit firm in the year of disclosing an IT control weakness and/or the preceding year is one of the big 4, 0 otherwise.

**Model 1b** tests H2a and H2b regarding the relationship between the disclosure of IT control weaknesses as a dependent variable and (a) the CIO structural power and (b) expert power as independent variables, respectively. The model controls for the IT
background of the CIO, the client firm profitability and the size of the audit firm. The expectation is that the coefficients of $\beta_1$ and $\beta_2$ will be negative and significant.

$$ITCW = \beta_0 + \beta_1 \text{CIOSPWR} + \beta_2 \text{CIOEPWR} + \beta_3 \text{CIOBACK} + \beta_4 \text{ROA} + \beta_5 \text{BIG4}$$

Where:

CIOSPWR = 1 if the firm had a CIO who was a named executive officer in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

CIOEPWR = the number of years the CIO has been in the current position.

CIOBACK = 1 if the CIO had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

ROA = Income Before Extraordinary Items divided by the average of the current year’s Total Assets and the prior year’s Total Assets, multiplied by 100.

BIG4 = 1 if the audit firm in the year of disclosing an IT control weakness and/or the preceding year is one of the big 4, 0 otherwise.

Finally, Model 1c presents results for the full model of Model (1) where ITCW is regressed on all IT governance variables and all control variables. The expectation is that the coefficients of $\beta_1$, $\beta_2$, $\beta_3$, $\beta_4$, and $\beta_5$ will be negative and significant.

$$ITCW = \beta_0 + \beta_1 \text{CORGOVITIT} + \beta_2 \text{AUDITIT} + \beta_3 \text{TMTIT} + \beta_4 \text{CIOSPWR} + \beta_5 \text{CIOEPWR} + \beta_6 \text{CIOBACK} + \beta_7 \text{ROA} + \beta_8 \text{BIG4}$$
Where:

ITCW = 1 if the firm disclosed an IT-related control weakness in Section 404 report; 0 otherwise (control firm).

CORGOVITIT = 1 if the corporate governance committee had IT background in the year of disclosing an IT control weakness and/or the preceding year; 0 otherwise.

AUDITIT = 1 if the audit committee had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

TMTIT = 1 if the top management team had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

CIOSPWR = 1 if the firm had a CIO who was a named executive officer in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

CIOEPWR = the number of years the CIO has been in the current position.

CIOBACK = 1 if the CIO had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

ROA = Income Before Extraordinary Items divided by the average of the current year’s Total Assets and the prior year’s Total Assets, multiplied by 100.

BIG4 = 1 if the audit firm in the year of disclosing an IT control weakness and/or the preceding year is one of the big 4, 0 otherwise.

Hypothesis 3 ascertaining the association between the CIO incentive alignment elements and the disclosure of IT control weaknesses is tested using Model (2). More specifically, Model 2 tests H3a and H3b about the relationship between the disclosure of
IT control weaknesses as a dependent variable and (a) the CIO absolute pay and (b) the CIO relative pay as independent variables, respectively. Consistent with extant executive compensation literature, the CIO absolute pay variable is a natural log transformation to help control for potential scale effects. Finally, the model controls for the IT background of the CIO, the client firm profitability and the size of the audit firm. The expectation is that the coefficients of $\beta_1$ and $\beta_2$ will be negative and significant.

$$ITCW = \beta_0 + \beta_1 \ln CIOCOMPS + \beta_2 CIOTMTS + \beta_3 CIOBACK + \beta_4 ROA + \beta_5 BIG4$$

**Where:**

$\ln CIOCOMPS = $ The natural log of the CIO salary and bonus in the year of disclosing IT control weakness and the preceding year.

$CIOTMTS = $ The ratio of the CIO salary and bonus ($CIOCOMPS$) to the average salary and bonus of the non-IT executive.

$CIOBACK = 1$ if the CIO had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.

$ROA = $ Income Before Extraordinary Items divided by the average of the current year’s Total Assets and the prior year’s Total Assets, multiplied by 100.

$BIG4 = 1$ if the audit firm in the year of disclosing an IT control weakness and/or the preceding year is one of the big 4, 0 otherwise.
Chapter 5  RESULTS

5.1  Descriptive Statistics

Table 5 identifies the ITCW firms by industry and weakness year. As shown in the table, firms in the study group are spread across 34 industries based on the 2-digit SIC code. Interestingly, more than 50% of the firm-year observations in the study group are concentrated in only 4 industries (out of 34): Business Services (SIC code 73) with 23.5%, Electronic and Other Electric Equipment (SIC code 36) with 15.4%, Industrial Machinery & Equipment (SIC code 35) with 7.4%, and Communications (SIC code 48) with 5.6%. A drill-down of the Business Services industry reveals that approximately two-thirds (68%) of the firm-year observations with IT control weakness within this industry are computer and data processing companies. Collectively, these ratios lend further support to the current body of evidence that companies with higher level of computerization are more prone to IT control weaknesses.

[Insert Table 5 about here]

Figure 4 provides insights about the trend of reporting IT control weaknesses. More specifically, it shows that the number of firm-year observations with IT control weaknesses is down trending over the study period. Stated differently, a fewer number of firms reported IT control weaknesses in each subsequent year compared to the previous year. One explanation could be that firms have acquired and accumulated experience in implementing and managing IT controls effectively. For example, the decrease in the number of firms with IT control weaknesses was paralleled with an increase in the
percentage of firms with a CIO position and an increase in the percentage with CIOs amongst their top management teams, as shown in Figure 4 below.

![Figure 4: ITCW Reporting Trend](image)

Descriptive statistics on the IT governance elements, the CIO incentive alignment elements, and the control variables are presented in Table 6. This information is presented for both the IT control weakness firms (ITCW) and the non-IT control weakness firms (Non-ITCW) and before applying log transformation to the compensation data. The mean values for all the variables are greater for the control group firm-year observations compared to those of the study group firm-year observations. This suggests
that firms with no IT control weaknesses have more IT knowledgeable corporate governance and audit committees, more powerful, higher compensated, and more IT knowledgeable CIOs, and higher revenues and ROA rates.

[Insert Table 6 about here]

Table 7 provides a comparison of the mean differences between the study group and the control group for all the variables included in the analysis. Except for the CIO structural power and compensation level, the t-tests indicate that the mean differences are statistically significant. The significant differences between the two groups indicate the relevance of the study variables.

[Insert Table 7 about here]

The correlation matrix for all variables of the study is presented in Table 8. As displayed in the table, the disclosure of IT control weaknesses is negatively associated with the IT background of the corporate governance committee and the audit committee. Furthermore, there is a negative association between reporting IT control weaknesses on one hand and the expert power, structural power, compensation level, and IT background of the CIO as well as the CIO-TMT pay disparity on the other hand. Finally, the disclosure of IT control weaknesses is negatively associated with the ROA rates and the size of the audit firm.

[Insert Table 8 about here]
A potential issue of concern that could arise in any multivariate analysis is that of multicollinearity where two or more predictor variables in a regression model are highly correlated. The high correlations, in the presence of multicollinearity, can cause the coefficient estimates to be unstable in that they can change drastically in response to minor changes in the data or model specifications. In this study, only one pair of variables which appear together in a regression model is highly correlated and thus may raise concerns about the presence of multicollinearity. These variables are the IT background of the corporate governance committee and the IT background of the audit committee at 71.3 percent (p-value < .01).

To assess the potential of multicollinearity between these two variables as well as all other variables, multicollinearity diagnostic statistics are computed, namely the Variance Inflator Factor (VIF) and Tolerance, for each variable. The VIF measures how much the variance of the coefficient of each predictor variable is inflated relative to a situation in which all predictor variables are uncorrelated. As shown in Table 8, the highest VIF (2.355) corresponded to the IT background of the audit committee and the second highest VIF (2.276) corresponded to the IT background of the corporate governance committee. However, both values are well below the threshold value of 5 and the higher cut-off value of 10 which are suggested to indicate potential multicollinearity concerns. Thus, multicollinearity is not expected to pose problems. Nevertheless, the model that contains these two variables is examined before and after dropping one of them. In either case, no substantial change resulted in the magnitude of the remaining variable’s coefficient. Therefore, multicollinearity is not considered to be an issue of concern.
5.2 Logistic Regression Model

This research employs logistic regression to ascertain the relation between governance mechanisms and the quality of IT control over financial reporting systems. Here, IT control quality is proxied by the presence (absence) of IT control weaknesses in the management’s report on the assessment of internal control over financial reporting.

Two categories of governance and contracting mechanisms are hypothesized to improve the quality of IT control through the means of decreasing information asymmetry and increasing goal congruence between the board of directors and the top management team (TMT) on one hand and the top information systems team (TIST) on the other hand. These categories are: IT governance mechanisms and CIO incentive alignment mechanisms.

Two models are constructed to investigate and test the relationship between the odds of disclosing an IT control weakness and the elements of each governance mechanism. Model (1) estimates the relation between the disclosure of IT control weaknesses and the IT governance elements whereas Model (2) estimates the relation between the disclosure of IT control weaknesses and the CIO incentive alignment elements.

5.2.1 Model (1): Effect of IT Governance Mechanisms (H1-H2)

The IT governance mechanisms include two elements. The first element is the IT background element which includes (a) the IT background of the corporate governance committee, (b) the IT background of the audit committee, and (c) the IT background of the top management team (TMT). The second element is the IT executive element which includes (a) the CIO structural power and (b) the CIO expert power. To examine the effect of these two elements on the disclosure of IT control weaknesses, two sets of
Hypotheses (H1 and H2) were formulated and tested with empirical data using logistic regression Model (1).

Hypotheses H1a, H1b, and H1c estimate the relation between the disclosure of IT control weaknesses on one hand and (a) the IT background of the corporate governance committee, (b) the IT background of the audit committee, and (c) the IT background of the top management team (TMT) on the other hand, respectively. Drawing on agency theory and the notion of information asymmetry, this research expects organizations with IT-experienced BODs and TMTs to exhibit lower levels of an IT knowledge gap and thus lower levels of information asymmetry. The lower the level of information asymmetry between the BOD and the TMT on one hand and the TIST on the other hand, the lower the likelihood that the TIST will engage in self-interested behavior. Hence, the lower the likelihood of IT-related weaknesses occurring and/or not being fixed in a timely manner. Therefore, Hypothesis H1 predicts a negative association between the IT expertise of the BOD and the TMT and the disclosure of IT control weaknesses.

Hypotheses H2a and H2b estimate the relation between the disclosure of IT control weaknesses on one hand and (a) the CIO structural power and (b) the CIO expert power on the other hand, respectively. The structural power of the CIO is operationalized in terms of the CIO formal membership (or lack of it) in the TMT. To this end, a CIO is considered a member of the TMT if the firm listed him/her as one of its named executive officers (NEOs). The CIO expert power is operationalized in terms of how long, in years, the CIO has been in the current position.
Evidence from the CIO literature suggests that CIOs with higher levels of structural power are more likely to influence other TMT members and gain their support for IT initiatives. Further evidence suggests that CIOs with longer tenures (hence, higher expert power) are more likely to build stronger relationships with other TMT members and to obtain more comprehensive and undisrupted understanding of the organization’s information systems. This research expects organizations with higher levels of CIO structural power and expert power to exhibit higher levels of goal congruence with the BOD and the TMT. The higher the level of alignment, the lower is the likelihood of having and subsequently disclosing IT weaknesses. Therefore, Hypothesis H2 predicts a negative association between the structural power and the expert power of the CIO and the disclosure of IT control weaknesses.

Table 9 provides coefficients and significance levels for estimating model (1) with the disclosure of IT control weaknesses (ITCW) as the dependent variable. Model 1a displays results of a regression of ITCW on the IT background of the corporate governance committee (CORPGOVIT), the IT background of the audit committee (AUDITIT), and the IT background of the TMT (TMTIT) as independent variables and the client firm profitability (ROA) and the size of the audit firm (BIG4) as control variables. Model 1b displays results of a regression of ITCW on the CIO structural power (CIOSPWR) and the CIO expert power (CIOEPWR) as independent variables and the CIO IT background (CIOBACK) as a control variable. Finally, Model 1c presents results for the full model where ITCW is regressed on all IT governance variables and all control variables.
As for the independent variables, the statistical results in Model 1c indicate that except for the IT background of the TMT, all other IT governance elements were significant predictors of the disclosure of IT control weaknesses. More specifically, the results indicate that a higher likelihood of disclosing IT-related control weaknesses is associated with having no IT expertise among members of the corporate governance and the audit committees providing support for H1a and H1b. Furthermore, the results indicate that a higher likelihood of disclosing IT control weaknesses is associated with having CIOs who are not among their firms’ named-executive officers (hence, CIOs with lower structural power) and who have shorter tenures (hence, CIOs with lower expert power) providing support for H2a and H2b.

With respect to the control variables, the statistical results in Model 1c indicate that a higher likelihood of disclosing IT-related control weaknesses is associated with having CIOs who do not have an IT background. The results further indicate a negative and marginally significant (p-value of .053) association between the likelihood of disclosing IT control weaknesses and the size of the audit firm. This finding seemingly contradicts Bryan and Lilien (2005) who found the disclosure of material weaknesses in internal control (hence, not just IT) to be positively associated with the size of the audit firm. This contradiction seems to suggest that firms that are audited by the larger and more diligent audit firms (i.e. Big4) are likely to respond to this by implementing more effective IT
controls and/or remediating any IT-related control weaknesses than firms audited by smaller audit firms.

Collectively, Model 1c has the highest explanatory power with an R-square of 48%. Further, the overall classification accuracy of the model is 82% with 86% of the non-IT control weakness firms and 74% of the IT control weakness firms predicted correctly, respectively.

5.2.2 Model (2) Effect of CIO Incentive Alignment Mechanisms (H3)

Model (2) tests Hypotheses H3a and H3b which estimate the relation between the disclosure of IT control weaknesses and (a) the CIO absolute pay and (b) the CIO relative pay, respectively. For a given firm-year, the CIO absolute compensation is based on the sum of CIO annual salary and bonus. The CIO relative pay is derived by computing the ratio of the CIO annual salary and bonus to the average annual salary and bonus of the non-IT executive in the TMT.

Drawing on expectancy theory (Vroom 1964), equity theory (Adams 1965) and the executive compensation literatures, the present study expects CIOs with higher absolute and relative pay to be more committed to organizational objectives and thus to be more motivated to design and implement IT controls that are consistent with the organization’s internal control objectives. In the event of IT control weaknesses, such CIOs are more likely to take the necessary measures to remedy these weaknesses before they are reported. Therefore, hypotheses H3a and H3b predict a negative association between the disclosure of IT control weaknesses and the CIO absolute and relative pay.
Table 10 provides coefficients and significance levels for estimating model (2) with the disclosure of IT control weaknesses (ITCW) being the dependent variable. The model regresses ITCW on the CIO absolute compensation (lnCIOCOMPS) and the CIO relative pay (CIOTMTS) and includes three independent variables: CIO IT background (CIOBACK), firm profitability (ROA), and size of the audit firm (BIG4).

[Insert Table 10 about here]

Contrary to what is hypothesized, results show that the association between the CIO absolute pay and the disclosure of IT control weaknesses is largely insignificant, providing no support for H3a.

As predicted in hypothesis H3b, empirical results show that the CIO relative pay (hence, the pay disparity between the CIO and other TMT members) is a significant predictor of the disclosure of IT control weaknesses. To this end, the lower the pay disparity between the CIO and other business executives in the top management team, the lower the likelihood of disclosing IT control weaknesses. This finding is consistent with evidence from the executive compensation literature showing that higher pay disparities among TMT members trigger feelings of perceived inequity which in turn undermine team collaboration and cooperation and increase the likelihood of executives engaging in self-interested behavior at the expense of organizational objectives.

Combined, these findings suggest that it is the level of the CIO relative as opposed to absolute compensation that has an impact on IT control quality; a result that is consistent
with evidence from the executive compensation literature underscoring the importance of relative pay over absolute pay (Bloom 1999).

Figure 5 presents the final research model with the coefficients and significance levels (shown in parentheses) for each of the hypothesized relationships.
Figure 5: Theoretical Research Model with Logistic Regression Results
Chapter 6  SUMMARY AND CONCLUSION

6.1  Summary

Research on IT control over financial reporting has primarily focused on investigating the consequences of IT control weaknesses on the effectiveness of internal control structure and the reliability of financial reporting. Despite the evident negative impact of IT control weaknesses, there is a paucity in theory-driven research on the antecedents of such weaknesses.

The current work proposes and tests an integrated theoretical model of the antecedents of IT control weaknesses. Central to the proposed model is the view that the existence of IT control weaknesses is a manifestation of an agency problem caused by information asymmetry and lack of alignment between the overall organization represented by the board of directors (BOD) as a principal and the information systems (IS) organization represented by the top IS team (TIST) as an agent.

Drawing on agency theory and equity theory, the proposed model postulates that the board of directors can employ two categories of governance and contracting mechanisms to reduce information asymmetry and align the interests of the TIST with those of the organization thereby reducing the agency problem. These categories are: IT governance mechanisms and IT executive incentive alignment mechanisms.

The IT governance mechanisms involve two elements. First, the IT background element which includes (a) the IT background of the corporate governance committee, (b) the IT background of the audit committee, and (c) the IT background of the top management team (TMT). Second, the IT executive element which is viewed in terms of
having a CIO position and the structural and the expert power of the CIO. The IT executive incentive alignment mechanisms include two elements: (a) the CIO absolute pay level and (b) the CIO relative pay as proxied by the pay disparity between the CIO and other members of the TMT.

The current research uses logistic regression to test three sets of hypotheses: H1, H2, and H3 corresponding to the IT background element, the CIO power element, and the CIO compensation element, respectively. More specifically, the current work tests hypotheses H1a, H1b, and H1c to establish the existence of an association between the disclosure of IT control weaknesses on one hand and (a) the IT background of the corporate governance committee, (b) the IT background of the audit committee, and (c) the IT background of the top management team (TMT), respectively.

Hypothesis 2 focuses on establishing the existence of an incremental effect that the CIO power has on the disclosure of IT control weaknesses beyond the effect of the presence of the CIO position. More specifically, the current research tests hypotheses H2a and H2b to establish the existence of an association between the disclosure of IT control weaknesses on one hand and the CIO structural power and the CIO expert power, on the other hand, respectively.

Hypothesis 3 focuses on whether CIO pay affects the disclosure of IT control weaknesses. Specifically, this study tests hypotheses H3a and H3b to establish the existence of an association between the disclosure of IT control weaknesses on one hand and the CIO absolute pay and the CIO relative pay on the other hand, respectively.
In order to test these hypotheses, the present research uses a study sample of 162 firm-year observations with one or more IT-related control weaknesses for the years 2005-2009. Consistent with the extant literature, the study sample was matched with a control sample of 162 firm-year observations with non-IT control weaknesses for the same period. This matching procedure should provide a baseline for understanding the incremental impact of the proposed governance elements on the disclosure of IT control weaknesses.

Support is found for five of the seven hypothesized antecedents of IT control weaknesses. As predicted, the IT background of the corporate governance committee and the IT background of the audit committee significantly influenced the disclosure of IT control weaknesses over financial reporting. To this end, firms with IT knowledgeable corporate governance and audit committee members are less likely to disclose IT-related control weaknesses. Furthermore, the results provide support for higher levels of CIO structural and expert power leading to lower likelihood of disclosing IT-related control weaknesses. In addition, results indicate that the lower the pay disparity between the CIO and other business executives in the top management team, the lower the likelihood of disclosing IT control weaknesses.

6.2 Limitations

While the empirical results offer interesting and promising insights into the antecedents of IT control weaknesses, the current research has several limitations. One such limitation is that it views IT control weaknesses through a dichotomous lens. This binary view might be limiting. For example, a company with one or two severe IT control
weaknesses would possibly have lower IT control quality than a company with five weaknesses that are less severe in nature. Therefore, future research should go beyond this dichotomous view of IT control weaknesses to document and classify the specific types, severity, and frequency of these weaknesses, followed by an examination of the associations between them and the proposed antecedents.

Another related limitation has to do with the binary nature of many of the independent variables that the current study uses. For example, a company having more members with IT expertise on its audit committee, corporate governance committee, and top management team would possibly have a higher level of IT knowledge (hence, lower level of information asymmetry) than a company with fewer IT knowledgeable members. Therefore, future research might go beyond this dichotomous view to measure IT background as a continuum. For instance, the IT background of the TMT could be measured in terms of the percentage of IT knowledgeable executives on the team.

Finally, due to the secondary nature of the data sources used in the current research, it is not possible to measure information asymmetry and goal congruence between the board of directors and the top management team on one hand and the top information systems team on the other hand. Future research might develop, validate, and incorporate measurement scales for these two constructs in order to provide a more robust testing of the proposed model.

6.3 Contribution

While research provides answers regarding the consequences of IT control weaknesses on the quality of internal controls (Bedard and Graham 2011; Canada et al.
2009; Grant et al. 2008), the reliability of financial reporting (Klamm and Watson 2009), and the accuracy of management earnings forecast (Li et al. 2010), the question of the antecedents of IT control weaknesses remains largely unanswered. The only other study that investigated the determinants of IT control weaknesses is Li et al. (2007a). Their study, however, suffers from three major limitations: (a) lack of theoretical grounding, (b) failure to consider other factors, besides IT governance, that may impact IT control quality, and (c) use of data from only the first year of Sarbanes-Oxley Section 404 compliance.

This study contributes to the current body of knowledge on IT control weaknesses in several ways. First, the present study is the first to propose and test an integrated model of the antecedents of IT control weaknesses. The proposed model adds to the current literature by introducing (a) agency theory with its notions of information asymmetry and goal congruence and (b) equity theory with its notion of perceived equity as a theoretical basis of the antecedents of ITCW. Furthermore, the current study adds to the literature on the influence of IT governance on the disclosure of IT control weaknesses by introducing and examining the impact of the IT background of the corporate governance committee. Moreover, this research goes beyond investigating the impact of the presence (absence) of the CIO position by providing empirical evidence linking the structural power and the expert power of the CIO to the disclosure of IT control weaknesses.

In addition, the current research contributes to the Information Systems and the Accounting Information Systems literatures by introducing and providing empirical evidence linking CIO compensation to the disclosure of IT control weaknesses.
Lastly, this research contributes to practice by offering a much needed understanding for managers, directors, auditors, and regulators in their effort to improve the quality of IT control and the reliability of financial reporting. For example, the present study contributes to the ongoing public policy debate about the effectiveness of SOX by providing evidence that the act has the desired effect of inducing stronger IT control systems and better IT governance practices. Specifically, this research provides empirical evidence linking the decline in the number of firms with IT control weaknesses over the study period to the increase in the percentage of firms with CIO positions and the increase in the percentage of firms with CIOs amongst their top management teams.
References


EUSPRIG, T.E.S.R.I.G.- from http://www.eusprig.org/about.htm


ITGI. "Board Briefing on IT Governance."


Table 1: Summary of Hypotheses

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Hypothesis Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1a</td>
<td>Companies with corporate governance committee members who don’t have IT-related background are more likely to have IT control weaknesses.</td>
</tr>
<tr>
<td>H1b</td>
<td>Companies with audit committee members who don’t have IT-related background are more likely to have IT control weaknesses.</td>
</tr>
<tr>
<td>H1c</td>
<td>Companies with TMT members who don’t have IT-related background are more likely to have IT control weaknesses.</td>
</tr>
<tr>
<td>H2a</td>
<td>Companies with CIOs with lower level of structural power are more likely to have IT control weaknesses.</td>
</tr>
<tr>
<td>H2b</td>
<td>Companies with CIOs with lower expert power are more likely to have IT control weaknesses.</td>
</tr>
<tr>
<td>H3a</td>
<td>Companies with CIOs with lower absolute pay are more likely to have IT control weaknesses.</td>
</tr>
<tr>
<td>H3b</td>
<td>Companies with CIOs with lower relative pay are more likely to have IT control weaknesses.</td>
</tr>
</tbody>
</table>
Table 2: Sample Selection

<table>
<thead>
<tr>
<th>Sample Selection Steps</th>
<th>No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total firm-year observations with internal control weaknesses</td>
<td>1,712</td>
</tr>
<tr>
<td>Less firm-year observations with non-IT related control weaknesses</td>
<td>1,331</td>
</tr>
<tr>
<td>Total firm-year observations with IT control weaknesses</td>
<td>381</td>
</tr>
<tr>
<td>Less foreign firm-year observations with IT control weaknesses</td>
<td>23</td>
</tr>
<tr>
<td>Maximum available firm-year observations with IT control weaknesses</td>
<td>358</td>
</tr>
<tr>
<td>Less firm-year observations for which no match was found</td>
<td>172</td>
</tr>
<tr>
<td>Total firm-year observations with IT control weaknesses for which a match is found</td>
<td>180</td>
</tr>
<tr>
<td>Less firm-year observations with IT control weaknesses for which no data is available</td>
<td>18</td>
</tr>
<tr>
<td>Maximum usable firm-year observations with IT control weaknesses</td>
<td>162</td>
</tr>
</tbody>
</table>
## Table 3: Assessment of the Matching Process Goodness

<table>
<thead>
<tr>
<th></th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NON-ITCW</td>
<td>ITCW</td>
<td>NON-ITCW</td>
<td>ITCW</td>
<td>NON-ITCW</td>
<td>ITCW</td>
</tr>
<tr>
<td><strong>REVENUES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>50</td>
<td>50</td>
<td>39</td>
<td>39</td>
<td>35</td>
<td>35</td>
</tr>
<tr>
<td>Mean</td>
<td>926</td>
<td>996</td>
<td>1,117</td>
<td>1,027</td>
<td>521</td>
<td>452</td>
</tr>
<tr>
<td>Std. Deviation</td>
<td>1,552</td>
<td>1,946</td>
<td>2,601</td>
<td>2,197</td>
<td>948</td>
<td>785</td>
</tr>
<tr>
<td>t-statistics</td>
<td>-0.199</td>
<td>0.165</td>
<td>0.333</td>
<td>0.141</td>
<td>0.619</td>
<td>0.144</td>
</tr>
<tr>
<td>p-value</td>
<td>0.843</td>
<td>0.870</td>
<td>0.740</td>
<td>0.889</td>
<td>0.543</td>
<td>0.886</td>
</tr>
<tr>
<td><strong>ASSETS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>50</td>
<td>50</td>
<td>39</td>
<td>39</td>
<td>35</td>
<td>35</td>
</tr>
<tr>
<td>Mean</td>
<td>1,417</td>
<td>948</td>
<td>1,135</td>
<td>1,569</td>
<td>685</td>
<td>1,781</td>
</tr>
<tr>
<td>Std. Deviation</td>
<td>3,057</td>
<td>1,562</td>
<td>2,265</td>
<td>3,052</td>
<td>807</td>
<td>5,857</td>
</tr>
<tr>
<td>t-statistics</td>
<td>0.967</td>
<td>-0.713</td>
<td>-1.096</td>
<td>1.163</td>
<td>0.855</td>
<td>-0.100</td>
</tr>
<tr>
<td>p-value</td>
<td>0.336</td>
<td>0.478</td>
<td>0.277</td>
<td>0.250</td>
<td>0.403</td>
<td>0.920</td>
</tr>
</tbody>
</table>
Table 4: Variable Definitions

<table>
<thead>
<tr>
<th>Variable Type</th>
<th>Variable Label</th>
<th>Variable Description</th>
<th>Data Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependent</td>
<td>ITCW</td>
<td>1 if the firm disclosed an IT-related control weakness in Section 404 report; 0 otherwise (control firm).</td>
<td>Audit Analytics</td>
</tr>
<tr>
<td>Independent</td>
<td>CORGOVIT</td>
<td>1 if the corporate governance committee had IT background in the year of disclosing an IT control weakness and/or the preceding year; 0 otherwise.</td>
<td>Proxy Statements</td>
</tr>
<tr>
<td>Independent</td>
<td>AUDITIT</td>
<td>1 if the audit committee had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.</td>
<td>Proxy Statements</td>
</tr>
<tr>
<td>Independent</td>
<td>TMTIT</td>
<td>1 if the top management team had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.</td>
<td>Proxy Statements</td>
</tr>
<tr>
<td>Independent</td>
<td>CIOSPWR</td>
<td>1 if the firm had a CIO who was a named executive officer in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.</td>
<td>Proxy Statements</td>
</tr>
<tr>
<td>Independent</td>
<td>CIOEPWR</td>
<td>The number of years the CIO has been in the current position.</td>
<td>Proxy Statements</td>
</tr>
<tr>
<td>Independent</td>
<td>lnCIOCOMPS</td>
<td>The natural log of the CIO salary and bonus in the year of disclosing IT control weakness and the preceding year.</td>
<td>Proxy Statements</td>
</tr>
<tr>
<td>Independent</td>
<td>CIOTMTS</td>
<td>The ratio of the CIO salary and bonus (CIOCOMPS) to the average salary and bonus of the non-IT executive.</td>
<td>Proxy Statements</td>
</tr>
<tr>
<td>Control</td>
<td>CIOBACK</td>
<td>1 if the CIO had IT background in the year of disclosing an IT control weakness and/or the preceding year, 0 otherwise.</td>
<td>Proxy Statements</td>
</tr>
<tr>
<td>Control</td>
<td>ROA</td>
<td>Income Before Extraordinary Items divided by the average of the current year’s Total Assets and the prior year’s Total Assets, multiplied by 100.</td>
<td>Audit Analytics</td>
</tr>
<tr>
<td>Control</td>
<td>BIG4</td>
<td>1 if the audit firm in the year of disclosing an IT control weakness and/or the preceding year is one of the big 4, 0 otherwise.</td>
<td>Audit Analytics</td>
</tr>
</tbody>
</table>
### Table 5: Analysis of ITCW Firms by 2 Digit SIC Code and ITCW Year

<table>
<thead>
<tr>
<th>2-Digit SIC</th>
<th>Industry Description</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Coal Mining</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>Oil And Gas Extraction</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Food And Kindred Products</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Textile Mill Products</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Paper And Allied Products</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td>Printing And Publishing</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Chemicals And Allied Products</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Rubber &amp; Misc. Plastics Products</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Primary Metal Industries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Industrial Machinery &amp; Equipment</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Electronic &amp; Other Electric Equipment</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>25</td>
</tr>
<tr>
<td>37</td>
<td>Transportation Equipment</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>Instruments &amp; Related Products</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>Misc. Manufacturing Industries</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Transportation Services</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Communications</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td></td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Electric, Gas &amp; Sanitary Services</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Wholesale Trade-Durable Goods</td>
<td>3</td>
<td>2</td>
<td></td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Wholesale Trade-Nondurable Goods</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>Automotive Dealers &amp; Service Stations</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>Apparel And Accessory Stores</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>Furniture And Home furnishings Stores</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>Miscellaneous Retail</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Depository Institutions</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>Non-depository Institutions</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Insurance Carriers</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>Insurance Agents, Brokers &amp; Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>Holding &amp; Other Investment Offices</td>
<td>1</td>
<td>1</td>
<td></td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>Business Services</td>
<td>13</td>
<td>10</td>
<td>9</td>
<td>4</td>
<td>2</td>
<td>38</td>
</tr>
<tr>
<td>75</td>
<td>Auto Repair, Services, And Parking</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>Amusement &amp; Recreation Services</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>Health Services</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>Educational Services</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>Engineering &amp; Management Services</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>50</td>
<td>39</td>
<td>35</td>
<td>27</td>
<td>11</td>
<td>162</td>
</tr>
<tr>
<td>Percentage</td>
<td></td>
<td>31%</td>
<td>24%</td>
<td>22%</td>
<td>17%</td>
<td>7%</td>
<td>100%</td>
</tr>
<tr>
<td>Variable</td>
<td>Group</td>
<td>N</td>
<td>Minimum</td>
<td>Maximum</td>
<td>Mean</td>
<td>Std. Deviation</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>--------</td>
<td>-----</td>
<td>---------</td>
<td>---------</td>
<td>-------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td>CORGOVIT</td>
<td>NON-ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.65</td>
<td>0.48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.28</td>
<td>0.45</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>324</td>
<td>0</td>
<td>1</td>
<td>0.46</td>
<td>0.50</td>
<td></td>
</tr>
<tr>
<td>AUDITIT</td>
<td>NON-ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.72</td>
<td>0.45</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.35</td>
<td>0.48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>324</td>
<td>0</td>
<td>1</td>
<td>0.54</td>
<td>0.50</td>
<td></td>
</tr>
<tr>
<td>TMTIT</td>
<td>NON-ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.65</td>
<td>0.48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.38</td>
<td>0.49</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>324</td>
<td>0</td>
<td>1</td>
<td>0.52</td>
<td>0.50</td>
<td></td>
</tr>
<tr>
<td>CIO</td>
<td>NON-ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.61</td>
<td>0.49</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.27</td>
<td>0.45</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>324</td>
<td>0</td>
<td>1</td>
<td>0.44</td>
<td>0.50</td>
<td></td>
</tr>
<tr>
<td>CIOSPWR</td>
<td>NON-ITCW</td>
<td>99</td>
<td>0</td>
<td>1</td>
<td>0.69</td>
<td>0.47</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>44</td>
<td>0</td>
<td>1</td>
<td>0.59</td>
<td>0.50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>143</td>
<td>0</td>
<td>1</td>
<td>0.66</td>
<td>0.48</td>
<td></td>
</tr>
<tr>
<td>CIOEPWR</td>
<td>NON-ITCW</td>
<td>89</td>
<td>0.25</td>
<td>18</td>
<td>5.16</td>
<td>3.66</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>43</td>
<td>0.75</td>
<td>15</td>
<td>3.82</td>
<td>3.08</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>132</td>
<td>0.25</td>
<td>18</td>
<td>4.73</td>
<td>3.53</td>
<td></td>
</tr>
<tr>
<td>CIOBACK</td>
<td>NON-ITCW</td>
<td>94</td>
<td>0</td>
<td>1</td>
<td>0.98</td>
<td>0.15</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>43</td>
<td>0</td>
<td>1</td>
<td>0.84</td>
<td>0.37</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>137</td>
<td>0</td>
<td>1</td>
<td>0.93</td>
<td>0.25</td>
<td></td>
</tr>
<tr>
<td>CIOCOMPS</td>
<td>NON-ITCW</td>
<td>82</td>
<td>106</td>
<td>680</td>
<td>304</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>42</td>
<td>107</td>
<td>656</td>
<td>283</td>
<td>113</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>124</td>
<td>106</td>
<td>680</td>
<td>297</td>
<td>122</td>
<td></td>
</tr>
<tr>
<td>CIOTMTS</td>
<td>NON-ITCW</td>
<td>82</td>
<td>0.23</td>
<td>2.29</td>
<td>0.89</td>
<td>0.37</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>42</td>
<td>0.19</td>
<td>1.25</td>
<td>0.73</td>
<td>0.21</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>124</td>
<td>0.19</td>
<td>2.29</td>
<td>0.84</td>
<td>0.33</td>
<td></td>
</tr>
<tr>
<td>BIG4</td>
<td>NON-ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.76</td>
<td>0.43</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>162</td>
<td>0</td>
<td>1</td>
<td>0.58</td>
<td>0.50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>324</td>
<td>0</td>
<td>1</td>
<td>0.67</td>
<td>0.47</td>
<td></td>
</tr>
<tr>
<td>ROA</td>
<td>NON-ITCW</td>
<td>162</td>
<td>-3.81</td>
<td>0.65</td>
<td>-0.04</td>
<td>0.34</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITCW</td>
<td>162</td>
<td>-6.96</td>
<td>0.32</td>
<td>-0.14</td>
<td>0.65</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>324</td>
<td>-6.96</td>
<td>0.65</td>
<td>-0.09</td>
<td>0.52</td>
<td></td>
</tr>
</tbody>
</table>
Table 7: Mean Comparison between the Study Group and the Control Group

<table>
<thead>
<tr>
<th>Variable</th>
<th>Mean</th>
<th>Mean Difference</th>
<th>t-statistics</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NON-ITCW</td>
<td>ITCW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CORGOVIT</td>
<td>0.65</td>
<td>0.28</td>
<td>0.37</td>
<td>7.178</td>
</tr>
<tr>
<td>AUDITIT</td>
<td>0.72</td>
<td>0.35</td>
<td>0.37</td>
<td>7.178</td>
</tr>
<tr>
<td>TMTIT</td>
<td>0.65</td>
<td>0.38</td>
<td>0.28</td>
<td>5.191</td>
</tr>
<tr>
<td>CIO</td>
<td>0.61</td>
<td>0.27</td>
<td>0.34</td>
<td>6.528</td>
</tr>
<tr>
<td>CIOSPWR</td>
<td>0.69</td>
<td>0.59</td>
<td>0.10</td>
<td>1.113</td>
</tr>
<tr>
<td>CIOEPWR</td>
<td>5.16</td>
<td>3.82</td>
<td>1.34</td>
<td>2.068</td>
</tr>
<tr>
<td>CIOBACK</td>
<td>0.98</td>
<td>0.84</td>
<td>0.14</td>
<td>2.403</td>
</tr>
<tr>
<td>CIOCOMPS</td>
<td>304</td>
<td>283</td>
<td>21</td>
<td>.894</td>
</tr>
<tr>
<td>CIOTMTS</td>
<td>0.89</td>
<td>0.73</td>
<td>0.16</td>
<td>3.167</td>
</tr>
<tr>
<td>ROA</td>
<td>-0.04</td>
<td>-0.14</td>
<td>0.10</td>
<td>1.705</td>
</tr>
<tr>
<td>BIG4</td>
<td>0.76</td>
<td>0.58</td>
<td>0.18</td>
<td>3.479</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>ITCW</td>
<td>1</td>
<td>.371**</td>
<td>.439</td>
<td>2.276</td>
</tr>
<tr>
<td>CORGOVIT</td>
<td>-.371**</td>
<td>.713**</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>AUDITIT</td>
<td>.278**</td>
<td>.529**</td>
<td>.536**</td>
<td>1</td>
</tr>
<tr>
<td>TMTIT</td>
<td>-.093</td>
<td>0.143</td>
<td>0.102</td>
<td>.285**</td>
</tr>
<tr>
<td>CIOSPWR</td>
<td>0.268</td>
<td>0.088</td>
<td>0.225</td>
<td>0.001</td>
</tr>
<tr>
<td>CIOEPWR</td>
<td>-.178</td>
<td>0.060</td>
<td>0.095</td>
<td>0.090</td>
</tr>
<tr>
<td>CIOBACK</td>
<td>-.265**</td>
<td>.199*</td>
<td>0.133</td>
<td>0.079</td>
</tr>
<tr>
<td>CIOCOMPS</td>
<td>-.081</td>
<td>0.084</td>
<td>0.006</td>
<td>0.166</td>
</tr>
<tr>
<td>CIOTMTS</td>
<td>-0.236**</td>
<td>0.052</td>
<td>0.146</td>
<td>0.169</td>
</tr>
<tr>
<td>ROA</td>
<td>-.095</td>
<td>0.108</td>
<td>0.060</td>
<td>0.032</td>
</tr>
<tr>
<td>BIG4</td>
<td>-.190**</td>
<td>.152**</td>
<td>.125*</td>
<td>.081</td>
</tr>
</tbody>
</table>

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).
Table 9: Model (1) Investigating the Effect of IT Governance Mechanisms on the Disclosure of IT Control Weaknesses (H1-H2)

**Model 1a: Investigating the Effect of the IT Background (H1a, H1b, & H1c)**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Expected Sign</th>
<th>Coefficient Estimate</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>CORGOVIT(1)</td>
<td></td>
<td>-.744</td>
<td>.002</td>
</tr>
<tr>
<td>AUDITIT(1)</td>
<td></td>
<td>-.840</td>
<td>.001</td>
</tr>
<tr>
<td>TMTIT(1)</td>
<td></td>
<td>-.340</td>
<td>.099</td>
</tr>
<tr>
<td>ROA</td>
<td></td>
<td>-.267</td>
<td>.293</td>
</tr>
<tr>
<td>BIG4(1)</td>
<td></td>
<td>-.631</td>
<td>.001</td>
</tr>
</tbody>
</table>

% of non-ITCW firms predicted correctly: 71.60
% of ITCW firms predicted correctly: 67.90
Pseudo R-Squared: 0.23

# of firm-year observations: 324

**Model 1b: Investigating the Effect of the CIO Power (H2a & H2b)**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Expected Sign</th>
<th>Coefficient Estimate</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIOSPWR(1)</td>
<td></td>
<td>-1.013</td>
<td>.001</td>
</tr>
<tr>
<td>CIOEPWR</td>
<td></td>
<td>-1.125</td>
<td>.010</td>
</tr>
<tr>
<td>CIOBACK(1)</td>
<td></td>
<td>-2.371</td>
<td>.000</td>
</tr>
<tr>
<td>ROA</td>
<td></td>
<td>.336</td>
<td>.376</td>
</tr>
<tr>
<td>BIG4(1)</td>
<td></td>
<td>-.713</td>
<td>.032</td>
</tr>
</tbody>
</table>

% of non-ITCW firms predicted correctly: 91.33
% of ITCW firms predicted correctly: 33.72
Pseudo R-Squared: 0.21

# of firm-year observations: 259

**Model 1c: Investigating the Effect of IT Governance (H1a-H1c & H2a-H2b)**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Expected Sign</th>
<th>Coefficient Estimate</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>CORGOVIT(1)</td>
<td></td>
<td>-1.724</td>
<td>.001</td>
</tr>
<tr>
<td>AUDITIT(1)</td>
<td></td>
<td>-1.211</td>
<td>.011</td>
</tr>
<tr>
<td>TMTIT(1)</td>
<td></td>
<td>.206</td>
<td>.614</td>
</tr>
<tr>
<td>CIOSPWR(1)</td>
<td></td>
<td>-.908</td>
<td>.017</td>
</tr>
<tr>
<td>CIOEPWR</td>
<td></td>
<td>-.118</td>
<td>.045</td>
</tr>
<tr>
<td>CIOBACK(1)</td>
<td></td>
<td>-1.863</td>
<td>.006</td>
</tr>
<tr>
<td>ROA</td>
<td></td>
<td>.448</td>
<td>.280</td>
</tr>
<tr>
<td>BIG4(1)</td>
<td></td>
<td>-.761</td>
<td>.053</td>
</tr>
</tbody>
</table>

% of non-ITCW firms predicted correctly: 86.13
% of ITCW firms predicted correctly: 74.42
Pseudo R-Squared: 0.48

# of firm-year observations: 259
Table 10: Model (2) Investigating the Effect of CIO Incentive Alignment Mechanisms on the Disclosure of IT Control Weaknesses (H3)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Expected Sign</th>
<th>Coefficient Estimate</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>InCIOCOMPS</td>
<td>-</td>
<td>.259</td>
<td>.645</td>
</tr>
<tr>
<td>CIOTMTS</td>
<td>-</td>
<td>-2.852</td>
<td>.002</td>
</tr>
<tr>
<td>CIOBACK(1)</td>
<td>-</td>
<td>-2.148</td>
<td>.005</td>
</tr>
<tr>
<td>ROA</td>
<td>-</td>
<td>-1.155</td>
<td>.370</td>
</tr>
<tr>
<td>BIG4(1)</td>
<td>-</td>
<td>-1.004</td>
<td>.057</td>
</tr>
</tbody>
</table>

| % of non-ITCW firms predicted correctly | 92.7 |
| % of ITCW firms predicted correctly   | 42.9 |
| Pseudo R2                             | 0.283|
| # of firm-year observations           | 124  |