JOURNAL OF INFORMATION SYSTEMS
Vol. 23, No. 2
Fall 2009
pp. 1–23

SOX 404 Reported Internal Control Weaknesses: A Test of COSO Framework Components and Information Technology

Bonnie K. Klamm
North Dakota State University

Marcia Weidenmier Watson
Mississippi State University

ABSTRACT: This paper examines internal controls, from both an information technology (IT) and non-IT perspective, in relation to the five components of the Committee of Sponsoring Organization's *Internal Control-Integrated Framework* (COSO 1992), as well as the achievement of one of COSO's three objectives-reporting reliability. Our sample consists of 490 firms with material weaknesses reported under Sarbanes-Oxley Section 404 during the first year of compliance. We classify the weaknesses by COSO component and as IT-related or non-IT-related. Our results support the interrelationships of the COSO *Framework*. The results also show that the number of misstated accounts is positively related to the number of weak COSO components (i.e., scope) and certain weak COSO components (i.e., existence). Firms with IT-related weak components report more material weaknesses and misstatements than firms without IT-related weak components, providing evidence on the pervasive negative impact of weak IT controls, especially in control environment, risk assessment, and monitoring.

Keywords: COSO; internal control weaknesses; information technology; Sarbanes-Oxley Act of 2002.

Data Availability: Contact the authors.

I. INTRODUCTION

Beginning on November 15, 2004, Section 404 of the Sarbanes-Oxley Act of 2002 (SOX 404) requires *all* accelerated firms (with at least $75 million in public equity float) to report on the effectiveness of their internal controls over financial reporting. Management must (1) state that they are responsible for establishing and maintaining internal controls, (2) identify the internal control framework used to evaluate controls, (3) provide an assessment on the effectiveness of internal controls, and (4) identify material weaknesses (MWs). An MW is a "deficiency, or a combination of deficiencies ... such that there is a **reasonable possibility** that a material misstatement" (emphasis in the original)

The authors thank the IMA Foundation for Applied Research, Mississippi State University, and North Dakota State University for their financial support.

of the firm's financial statements will not be prevented or detected on a timely basis (PCAOB 2007, para. A7).[1]

A wave of control studies using SOX data has emerged, primarily investigating the characteristics of firms reporting MWs and the effect of internal control reports on market conditions. Firms reporting MWs are smaller, younger, riskier, more complex, and financially weaker, with poorer accrual earnings quality (e.g., Ge and McVay 2005; Doyle et al. 2007a, 2007b). Market studies indicate that the stock-price reaction to reports of MWs is negative, especially for severe MWs (e.g., Hammersley et al. 2008; Beneish et al. 2008). Moreover, Enron and other high-profile accounting scandals reduced market liquidity, which rebounded following SOX, suggesting that the legislation was effective at restoring investor confidence (Jain et al. 2008). The objective of this study is to expand extant control literature by analyzing MWs with respect to information technology (IT) and the Committee of Sponsoring Organization's *Internal Control-Integrated Framework* (COSO 1992; hereafter, COSO).

COSO consists of five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring. Using SOX 404 reports during the first year of compliance, we classify the reported MWs by COSO component and as IT-related or non-IT-related. We examine the interrelatedness of weak COSO components and their relationship with the number of misstated accounts, a measure of financial reporting reliability.

Our results support the interrelatedness of weak COSO components. We provide evidence that a weak control environment has a positive association with other weak COSO components and that the remaining weak components are positively associated with the preceding (weak) component. The model also provides additional support on the interrelatedness of weak monitoring as it is positively associated with weak risk assessment and weak control activities.

We also show that weak COSO components affect reporting reliability. We find that reporting reliability is affected by the *scope* (i.e., the number of weak COSO components) and *existence* of control problems in specific weak components, in addition to whether the weakness is IT or non-IT-related. Firms with IT-related weak components report not only more non-IT-related MWs and misstatements than firms without IT-related weak components, but also have a greater scope of MWs. Moreover, the existence of an IT-related weak component generally has an incremental negative effect on reporting reliability and the number of non-IT material weaknesses reported, especially for the control environment, risk assessment, and monitoring components. Thus, the IT domain appears to affect overall control effectiveness.

This study contributes to the understanding of the relationship between the weak components, which is important to regulators, investors, auditors, and managers because a firm's design and execution of its internal control systems affect reporting accuracy as well as operational efficiency and effectiveness. Understanding IT's role in internal controls is imperative given that (1) computerized systems process most business information, (2) IT changes the nature of misstatements (Kinney 2000), and (3) little empirical evidence exists regarding IT's role in controls (*cf.*, Eilifsen and Messier 2000; Kreutzfeldt and Wallace 2000; ITGI 2004). Moreover, current *mandated* guidance gives auditors an effort-reducing

[1] This definition differs slightly from and supersedes the AS No. 2 definition, which states that "a *material weakness* is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected" (emphasis in original) (PCAOB 2004, 156).

incentive to use tests of IT controls (PCAOB 2007, Appendix B28), which requires auditors to clearly understand how IT and non-IT MWs can affect the effectiveness of the *Framework*.

The remainder of the paper is as follows. Section II provides the background and hypotheses. Section III describes the research method. Section IV presents the results, and Section V concludes.

II. BACKGROUND AND HYPOTHESES

COSO Internal Control—Integrated Framework

SOX 404 requires management to use a framework to evaluate internal controls. Given that most firms are using COSO, we analyze internal control by examining MWs within the context of the following five components of COSO. The first component, control environment, provides the foundation for all of the other control components and sets the tone of the firm. It includes the integrity, ethical values, competence, philosophy, and operating style of the firm's managers and employees. The second component, risk assessment, is the identification, analysis, and management of (operating, economic, industry, regulatory) risks that may prevent a firm from achieving its objectives. Management implements control activities, the third component, to mitigate the identified risks. Control activities include segregation of duties, approvals, reviews, reconciliations, and authorizations. The fourth component, information, and communication, refers to the timely capture and dissemination of pertinent information on internal and external events (horizontally and vertically) throughout the organization's value chain, and includes communication among and between management, employees, suppliers, and customers. The last component, monitoring, is the continual evaluation of the other components' effectiveness.

COSO explicitly defines the components as ''interrelated.'' Yet, only one study, Geiger et al. (2004), examines this interrelatedness. They categorize internal control MWs reported by 32 Rhode Island state agencies and find a (univariate) positive correlation between weak control environment and weak risk assessment and negative relationships between weak control activities and the other weak components. Using SOX 404 data for hundreds of publicly traded firms, we expand this analysis to consider not only the relation between weak COSO components, but also the relation of weak COSO components with misstatements. This analysis provides insights about the consequences of the reported MWs, and in turn, the value of internal control reports.

Hypotheses

To have effective internal controls, a firm needs to have all five COSO components functioning together. The theoretical basis of COSO is a strong control environment, the ''foundation'' for the effectiveness of the other components. Thus, if the control environment is strong (weak), the other four components are less (more) likely to have MWs. Therefore, we hypothesize:

> **H1a:** Positive associations are expected between a weak control environment and other weak components of the COSO *Framework*.

In addition to the foundation provided by the control environment, the remaining components also build upon the effectiveness of the preceding component (COSO 1992, Exhibit 1, 19). Moreover, COSO clearly describes these ''building'' relationships as: (1) prioritize risks, (2) identify controls to address these risks, (3) identify needed information to monitor established controls, and (4) implement monitoring to evaluate the collected information (COSO 2008, 8). If the risk assessment component is not effective, a firm cannot implement necessary control activities to mitigate unidentified risks. Thus, if risk assessment is weak, control activities are more likely to also be weak; if control activities are weak, information and communication is more likely to be weak; and finally, if information and communication is weak, monitoring is more likely to be weak. Thus, we hypothesize:

H1b: A positive association is expected between a weak risk assessment component and a weak control activities component.

H1c: A positive association is expected between a weak control activities component and a weak information and communication component.

H1d: A positive association is expected between a weak information and communication component and a weak monitoring component.

Internal control is a ''multidirectional iterative process in which almost any component can and will influence another'' (COSO 1992, 18). While model restrictions prevent us from testing all possible relationships, we focus on the monitoring component, because, when properly implemented, it helps firms improve controls while also reducing the costs of assuring that controls are effective (COSO 2008). Despite these benefits, the monitoring component has not been fully utilized by firms due to a lack of clear guidance and understanding (COSO 2008). Effective monitoring should determine that internal control system ''continues to be *relevant* and able to *address new risks*'' (COSO 2008, 3, emphasis in original). As risks change, management must recognize and evaluate those new risks and implement appropriate internal controls to mitigate them. Therefore, firms with weak monitoring are likely to have MWs in risk assessment and control activities as hypothesized below:

H1e: A positive association is expected between a weak monitoring component and a weak risk assessment component.

H1f: A positive association is expected between a weak monitoring component and a weak control activities component.

One of the objectives of internal control is to provide reliable information. Thus, strong (weak) internal controls should lead to high (low) financial reporting reliability. Reliable financial reporting indicates that (1) firms follow generally accepted accounting principles (COSO 1992, 35), and (2) accounts are appropriately stated. A misstatement is the difference between the recorded and true value of an account line item. This difference may or may not be detected by the auditors and includes (unintentional) errors, misappropriation fraud, and misrepresentation fraud (Kinney 2000). Such misstatements decrease financial reporting reliability. According to COSO, if all components are not working effectively (i.e., detect or prevent the entry of erroneous or fraudulent data), the objective of financial reporting reliability may not be met, and accounts may be misstated. Thus, we expect that weak COSO components are positively related to misstatements, as stated in our second hypothesis:

H2: Weak COSO components are positively related to the number of misstated account balances.

Given that ‘‘IT is the foundation of an effective system of internal control,’’ IT controls have a pervasive effect on the achievement of control objectives as well as the firm's inherent risk of misstatements (ITGI 2004, 21, 6). Specifically, ineffective IT controls may lead to incorrect recording of transactions, which in turn may result in misstatements. Prior research finds firms with IT MWs have less accurate forecasts when compared to firms with non-IT-related MWs, indicating lower quality financial information for IT-weak firms (Li et al. 2008). Thus, we expect firms with IT-related MWs to have more misstated account balances, which leads to our third hypothesis:

H3: Firms with IT-related MWs report more misstated accounts than firms with non-IT-related MWs.

Using U.S. audit data from 1988 where 56 percent of the firms were ‘‘computerized’’ (Messier et al. 2004, 224), Bell et al. (1998, 14) find that ‘‘incorrect manual computations, improper recording of exchange documents, incorrect application of internal controls, and inadequate internal controls are *more likely* to be sources of problems when information systems are computerized’’ (emphasis in original). A decade later, using Norwegian audit data from 1997, Messier et al. (2004) examined a sample of firms: 62 percent were ‘‘computerized’’ in all business processes; 38 percent were ‘‘partially computerized,’’ e.g., business processes such as payroll leases and/or other activities were not computerized. They find that missing controls, poorly designed controls, and overworked accounting personnel are more likely to be the source of misstatements in computerized business processes as compared to noncomputerized business processes. Thus, the use of IT appears to historically be associated with more overall (non-IT) control problems.

Today, IT is inseparable from a firm's strategic and operational information systems, making ‘‘IT control competency in *all* of the COSO components’’ a necessity for COSO to be effective (ITGI 2004, 27, emphasis added). While effective IT controls support the entire COSO framework (ITGI 2004, 27), ineffective IT controls may still be associated with non-IT control problems given IT's growing role in the firm. Therefore, we examine whether firms with at least one IT-related internal control problem have more non-IT-related internal control problems, as stated in our fourth hypothesis:

H4: Firms with IT-related MWs report more non-IT-related MWs than firms with only non-IT-related MWs.

III. RESEARCH METHOD

Sample

Our initial sample consists of 602 firms that received an adverse opinion on their internal controls as reported by Audit Analytics. From this sample of accelerated filers (i.e., more than $75 million in public float) with fiscal year-ends from November 24, 2004, through November 23, 2005, we eliminate eight exempt firms and 104 firms because of missing financial data from Research Insight Compustat. Our final sample consists of 490 firms that reported one or more MW.

Table 1, Panels A and B, show our total sample by year and by industry, respectively. Because the sample period runs from November 2004 to November 2005, the number of firms is greater in 2004 as most firms have a December year-end. The distribution by industry is similar to that of Ge and McVay (2005), a SOX 302 study, with firms in the computer, banks, insurance, retail, and services industries making up the majority of our sample.

TABLE 1
Sample Distribution

Panel A: Distribution of Ineffective Control Sample by Year

Year	Firms with IT Weaknesses	Firms with No IT Weaknesses	Total
2004	95 (29%)	229 (70%)	324
2005	34 (20%)	132 (80%)	166
Total	129 (26%)	361 (74%)	490

Panel B: Distribution of Ineffective Control Sample by Industry[a]

Industry	Number of Firms with IT Weaknesses (% of industry)	Number of Firms with No IT Weaknesses (% of industry)	Total (% of total sample)
Computers	30 (32%)	64 (68%)	94 (19%)
Banks and Insurance	14 (20%)	56 (80%)	70 (14%)
Retail	12 (17%)	57 (83%)	69 (14%)
Services	16 (30%)	37 (70%)	53 (11%)
Drugs and Medical Equipment	4 (24%)	27 (87%)	31 (6%)
Transportation	9 (31%)	20 (69%)	29 (6%)
Industrial Equipment	7 (30%)	16 (70%)	23 (5%)
Miscellaneous Equipment	9 (43%)	12 (57%)	21 (4%)
Rubber, Leather, and Metal	5 (28%)	13 (72%)	18 (4%)
Textiles, Printing, and Publishing	4 (24%)	13 (76%)	17 (3%)
Utilities	6 (35%)	11 (65%)	17 (3%)
Refining and Extractive	5 (36%)	9 (64%)	14 (3%)
Electrical Equipment	3 (27%)	8 (73%)	11 (2%)
Mining	2 (20%)	8 (80%)	10 (2%)
Chemicals	1 (14%)	6 (86%)	7 (1%)
Food	2 (40%)	3 (60%)	5 (1%)
Other	0 (0%)	0 (0%)	1 (0%)
Total	129 (26%)	361 (74%)	490 (100%)

[a] Industry classifications are compiled using the following SIC codes (Ge and McVay 2005): Mining 1000–1299, 1400–1999; Food: 2000–2199; Textiles: 2200–2799; Drugs 2830–2839, 3840–3851; Chemicals: 2800–2829, 2840–2899; Refining 1300–1399, 2900–2999; Rubber: 3000–3499; Industrial Equipment: 3500–3569, 3580–3659; Electrical Equipment: 3660–3669, 3680–3699; Miscellaneous Equipment: 3700–3839, 3852–3999; Computers: 3570–3579, 3670–3679, 7370–7379; Transportation: 4000–4899; Utilities: 4900–4999; Retail: 5000–5999; Banks and Insurance: 6000–6999; Services: 7000–7369, 7380–8999; and Other 000–999.

Variables

Table 2 provides variable definitions. Table 3 provides our categorization of weakness types by COSO component. Most firms do not classify reported MWs by COSO component. Instead, firms report specific MWs, e.g., insufficient account reconciliations. Therefore, the authors mapped the reported IT-related and non-IT-related MWs to COSO components based on specific examples from the *Internal Control Integrated Framework* (COSO 1992),

TABLE 2
Definition of Variables

Variable	Description
SOX 404 Variables	
CTRLENV	1 if the firm reports a MW in its Control Environment component, 0 otherwise
RISKAS	1 if the firm reports a MW in its Risk Assessment component, 0 otherwise
CTRLACT	1 if the firm reports a MW in its Control Activities component, 0 otherwise
INFOCOM	1 if the firm reports a MW in its Information and Communication component, 0 otherwise
MONITOR	1 if the firm reports a MW in its Monitoring component, 0 otherwise
SCOPE	The number of (non-IT and IT) weak COSO Internal Control components [0,5]
ITCTRLENV	1 if the firm reports an IT-related MW in its Control Environment component, 0 otherwise
ITRISKAS	1 if the firm reports an IT-related MW in its Risk Assessment component, 0 otherwise
ITCTRLACT	1 if the firm reports an IT-related MW in its Control Activities component, 0 otherwise
ITINFOCOM	1 if the firm reports an IT-related MW in its Information and Communication component, 0 otherwise
ITMONITOR	1 if the firm reports an IT-related MW in its Monitoring component, 0 otherwise
ITSCOPE	The number of IT-related weak COSO Internal Control components [0,5]
ITMW	1 if the firm has an IT-related MW(s), 0 otherwise
MSTMT	The number of accounts misstated
MWNum	The number of MWs reported in the SOX 404 internal control report
NONITMWNum	The number of non-IT MWs reported in the SOX 404 internal control report
NCTRLENV	1 if the firm reports an non-IT related MW in its Control Environment component, 0 otherwise
NRISKAS	1 if the firm reports an non-IT related MW in its Risk Assessment component, 0 otherwise
NCTRLACT	1 if the firm reports an non-IT related MW in its Control Activities component, 0 otherwise
NINFOCOM	1 if the firm reports an non-IT related MW in its Information and Communication component, 0 otherwise
NMONITOR	1 if the firm reports an non-IT related MW in its Monitoring component, 0 otherwise
NSCOPE	The number of non-IT related weak COSO Internal Control components [0,5]
Financial Variables (all current year unless otherwise specified)	
ASSETS	Total assets (in millions)
BV	Common equity − liquidation value divided by common shares outstanding
FOREIGN	1 if amount in Research Insight variable A150, 0 otherwise
MERGER	1 if amount in Research Insight variable AQSF, 0 otherwise
MV	The share closing price multiplied by the common shares outstanding at year end (in millions)
RESTRUCT	1 if amounts in Research Insight variables A376, A377, A378, or A379; 0 otherwise

(*continued on next page*)

TABLE 2 (continued)

Variable	Description
ROA	Income Before Extraordinary Items – Available for Common, divided by the average of the current year's Total Assets and the prior year's Total Assets, multiplied by 100
SALES	Gross sales reduced by cash discounts, trade discounts, and returned sales and allowances for which credit is given to customers (in millions)

COBIT 4.1 (ITGI 2007), and *GTAG: Information Technology Controls* (IIA 2005).[2] Table 3 presents the result of this process, while the Appendix provides references used in the mapping process.

We use Audit Analytics to identify the MWs. Audit Analytics captures the number of MWs as reported by the firm in its SOX 404 Management's Report on Internal Controls and then categorizes the control MWs. A single MW may be coded into multiple types. For example, Vishay Intertechnology Inc. reported the following material weakness in its 2004 10-K:

> Management determined that certain of our operating locations have insufficient staffing of the accounting and financial reporting function. This inadequate level of staffing results in certain accounting processes not being performed on a timely basis. These issues, when combined with an inadequate level of finance staffing at our corporate headquarters, reduce the effectiveness of the corporate finance staff in its monitoring and evaluation of the financial position and operating results of the Company, increasing the risk of a financial statement misstatement.
>
> As a result of the items described above, we ... identified adjustments during the audit ... in accounting for accruals, purchase commitments, fixed asset account reconciliations, and intercompany reconciliations among our wholly owned subsidiaries.

Audit Analytics sets MW as 1 (our *MWNum* variable) and codes this MW into the following types: (1) accounting personnel resources, competency/training; (2) material and/or numerous auditor year-end adjustments; and (3) untimely or inadequate account reconciliations. We use Audit Analytics to identify our non-IT MW COSO components (see Table 3) and number of misstated accounts (e.g., three for Vishay-fixed assets, accruals, and intercompany).

Identifying IT MWs was a two-step process. We first identified firms with IT-related MWs using Audit Analytics, which (dummy variable 0/1) codes a firm having an IT MW if its 404 report mentions an MW related to systems or IT. It does not identify the specific number or type of IT MW (e.g., system documentation). Therefore, both authors individually read each Management's Report on Internal Controls to count and code the reported IT MWs (see Table 3). The initial Cohen's kappa for interrater reliability equaled 0.79 (0.73 for an independent third party). All discrepancies were then identified and resolved. Table 1, Panel A, shows the firms without IT MWs, 361 (74 percent) (hereafter, Non-IT-Weak firms), and with at least one IT-related MWs, 129 (26 percent) (hereafter, IT-Weak firms). In eight of the 16 industries, 30 percent or more of the firms report one or more IT-related MW (Table 1, Panel B).

[2] Given the clarity of the examples from the selected guidance, the authors were in complete agreement about the mappings.

TABLE 3
Percentage of Firms Reporting Types of SOX 404 Material Weaknesses by COSO Component

Weakness Types by COSO Component	Full Sample (n = 490)	IT Analysis: IT-Weak[a] (n = 129)	IT Analysis: Non-IT-Weak[b,c] (n = 361)
Control Environment (*CTRLENV*)			
Non-IT Related MWs			
personnel ethical, compliance, or training issues	50.8	76.0	41.8**
explicitly reported: weak control environment	11.6	31.8	4.4**
senior management issues	6.1	12.4	3.9**
mgmt/board/audit committee investigations	2.0	4.7	1.1*
ineffective or understaffed audit committee	1.0	3.1	0.3**
ineffective regulatory compliance	1.0	1.6	0.8
IT-Related MWs			
explicitly reported: weak IT control environment	4.1	15.5	NA
lack of systems training	1.6	6.2	NA
decentralized systems	0.8	3.1	NA
Risk Assessment (*RISKAS*)			
Non-IT Related MWs			
foreign or subsidiary issues	21.8	34.9	17.2**
acquisition, merger, disposal, or reorg issues	10.8	16.3	8.9*
explicitly reported: weak risk assessment	3.7	10.1	1.3**
IT-Related MWs			
explicitly reported: weak IT risk assessment	0.6	2.3	NA
Control Activities (*CTRLACT*)			
Non-IT Related MWs			
accounting documentation, policy, procedures	94.9	93.8	95.2
period end issues	54.8	65.1	51.0**
inadequate account reconciliations	33.4	58.9	24.4**
explicitly reported: weak control activities	25.9	38.0	21.6**
segregation of duties	22.0	57.4	9.4**
fraud	1.6	2.3	1.4
IT-Related MWs			
logical access issues	14.7	55.8	NA
other IT issues	13.3	50.4	NA
program change control issues	7.6	28.7	NA
spreadsheet issues	6.5	24.8	NA
lack of systems documentation	4.3	16.3	NA
security issues	4.1	15.5	NA

(*continued on next page*)

TABLE 3 (continued)

Weakness Types by COSO Component	Full Sample (n = 490)	IT Analysis: IT-Weak[a] (n = 129)	IT Analysis: Non-IT-Weak[b,c] (n = 361)
explicitly reported: weak IT control activities	3.7	14.0	NA
disparate, non-integrated systems	2.2	8.5	NA
coding/program errors	1.8	7.0	NA
ineffective or lack of disaster recovery plan	1.8	7.0	NA
functionally complex systems	1.2	4.7	NA
Information and Communication (*INFOCOM*)			
Non-IT Related MWs			
explicitly reported: weak information and communication	10.8	21.7	6.9**
IT-Related MWs			
explicitly reported: weak IT information and communication	1.6	6.2	NA
Monitoring (*MONITOR*)			
Non-IT Related MWs			
explicitly reported: weak monitoring	30.0	44.2	24.9**
lack of supervision or oversight	19.2	37.2	12.7**
insufficient or non-existent internal audit function	2.4	7.0	0.8**
SEC Investigation	1.0	2.3	0.6
IT-Related MWs			
explicitly reported: weak IT monitoring	6.7	25.6	NA

*, ** One-tailed tests were used indicating (two-tailed) significance at the 0.05 percent and 0.01 percent levels, respectively.
[a] IT-Weak = firms with one or more IT-related material weaknesses.
[b] Non-IT-Weak = firms reporting non-IT-related material weaknesses.
[c] Differences between IT-Weak and Non-IT-Weak firms was examined using a MANOVA followed by univariate ANOVAs and Tukey multiple comparison tests.

Method

To test H1, the association of weak COSO components, we first examine Spearman correlations followed by structural equation modeling (SEM), which simultaneously tests all of the correlations. We use five dummy variables to identify weak COSO components. We expect a significant positive association between the control environment (*CTRLENV*) and the other components (*CTRLENV* → *RISKAS*, *CTRLENV* → *CTRLACT*, *CTRLENV* → *INFOCOM*, *CTRLENV* → *MONITOR*), as well as the "building" relationships between the remaining components (*RISKAS* → *CTRLACT*, *CTRLACT* → *INFOCOM*, *INFOCOM* → *MONITOR*). We also expect a significant positive association between monitoring and both risk assessment and control activities (*MONITOR* → *RISKAS*, *MONITOR* → *CTRLACT*).

We analyze the relationship between weak COSO components and each dependent variable from two perspectives. Equation (1) examines the total number of weak COSO components, or *scope* of internal control problems. Equation (2) examines the *existence* of a specific weak component. We control for firm characteristics that may affect MWs. Specifically, extant research shows that smaller and less profitable firms are more likely to disclose an MW or have misstated accounts (Ashbaugh-Skaife et al. 2007; Caster et al. 2000; Doyle et al. 2007a; Eilifsen and Messier 2000). Also, firms reporting MWs are more complex (Ashbaugh-Skaife et al. 2007; Doyle et al. 2007a). Therefore, we include variables controlling for firm size (*MV*), profitability (*ROA*), and complexity as measured by the presence of foreign operations, acquisition/mergers, and restructurings (*FOREIGN*, *MERGER*, and *RESTRUCT*):

$$\begin{aligned} IC\ WEAK\ OUTCOMES = {} & \alpha_0 + \alpha_1 SCOPE + \alpha_2 SCOPE * ITMW \\ & + \alpha_3 log(MV) + \alpha_4 ROA + \alpha_5 FOREIGN \\ & + \alpha_6 MERGER + \alpha_7 RESTRUCT + \varepsilon \end{aligned} \tag{1}$$

$$\begin{aligned} IC\ WEAK\ OUTCOMES = {} & \beta_0 + \beta_1 CTRLENV + \beta_2 RISKAS + \beta_3 CTRLACT \\ & + \beta_4 INFOCOM + \beta_5 MONITOR \\ & + \beta_6 CTRLENV * ITMW + \beta_7 RISKAS * ITMW \\ & + \beta_8 CTRLACT * ITMW + \beta_9 INFOCOM * ITMW \\ & + \beta_{10} MONITOR * ITMW + \beta_{11} log(MV) \\ & + \beta_{12} ROA + \beta_{13} FOREIGN + \beta_{14} MERGER \\ & + \beta_{15} RESTRUCT + \varepsilon \end{aligned} \tag{2}$$

where the *IC WEAK OUTCOMES*:

MSTMT = number of misstated accounts reported in SOX 404 Management's Report on Internal Control; and

NONITMWNum = number of non-IT-related MWs reported in SOX 404 Management's Report on Internal Control.

Table 2 provides the definitions for the explanatory variables.

Equations (1) and (2) are run as Poisson regressions appropriate for our count dependent variables. Using *MSTMT* as the dependent variable for Equation (1), a positive α_1 indicates a positive association between the number of weak components and the number of misstated accounts. A positive α_2 provides evidence that firms with IT-related MW(s) have more misstated accounts than firms with non-IT MW(s). Equation (2) expands the analysis to the individual COSO components. Positive values for β_1–β_5 will show the specific weak components associated with the number of misstatements, while the values for β_6–β_{10} examine the incremental effect of IT. Using *NONITMWNum* as the dependent variable, a positive α_2 (Equation (1)) and positive β_6–β_{10} (Equation (2)) would show that IT-Weak firms report more non-IT-related MWs in total and by component than Non-IT-Weak firms.

IV. RESULTS

Univariate Analysis

Table 3 shows the percentage of firms reporting a particular type of MW by COSO component for the full sample and for IT-Weak and Non-IT-Weak firms. For the full sample, 30.0 percent of the firms *explicitly* report that they have weak "monitoring," 25.9 percent weak "control activities," 11.6 percent weak "control environment," 10.8 percent weak "information and communication," and 3.7 percent weak "risk assessment."

Within the control environment component, the type reported most frequently is personnel, ethical, or training issues (50.8 percent). For risk assessment, the most frequently reported type was foreign or subsidiary issues (21.8 percent). For control activities, Audit Analytics codes almost 100 percent of all firms as having accounting documentation, policy, and/or procedures issues. Thus, we assume that all firms have this MW and exclude it from the following discussion, construction of COSO variables, and subsequent analyses. The next highest reported type is period-end issues (54.8 percent).

For non-IT-related MWs, Table 3 reveals that, with the exception of ineffective regulatory compliance, fraud, and SEC investigation, the IT-Weak firms report significantly higher percentages of every MW type than Non-IT-Weak firms. For IT-related MWs, the most cited IT MW types are control activities-logical access issues (55.8 percent) followed by other/miscellaneous IT issues (50.4 percent), program change control (28.7 percent), spreadsheet (24.8 percent), and lack of systems documentation (16.3 percent). IT-Weak firms most frequently and *explicitly* identify weak IT monitoring as a weak COSO component (25.6 percent), followed by the IT control environment (15.5 percent), IT control activities (14.0 percent), information and communication (6.2 percent), and IT risk assessment (2.3 percent). All of these IT MWs could lead to misstatements. For example, logical access issues could lead to theft, destruction, unauthorized changes to data, or in the extreme case, fraud. Moreover, weak program change controls and spreadsheet errors could result in inaccurate account balances.

Compared with Messier et al.'s (2004) 1997 Norwegian sample, our sample reports higher levels of weak IT control environment (4.1 percent of overall sample versus 2.8 percent), more program change/development issues (7.6 percent versus 1.2 percent), more system documentation issues (4.3 percent versus 0 percent), and more logical access issues (14.7 percent versus 2.0 percent). Thus, our more recent U.S. sample provides a good opportunity to examine the role of IT in internal control effectiveness.

Table 4 presents descriptive statistics. On average, each firm reports 2.47 MWs (*MWNum*) and 2.32 misstated accounts (*MSTMT*) with 62 percent (304 firms) reporting a misstatement (not shown). IT-Weak firms fared significantly worse than Non-IT-Weak firms with respect to number of total and non-IT MWs reported (*MWNum*, 4.53 versus 1.74, $p < 0.01$; *NONITMWNum*, 3.18 versus 1.74, $p < 0.01$) as well as the number of misstated accounts (*MSTMT*, 3.33 versus 1.95, $p < 0.01$) and percentage of firms reporting a misstated account (84 percent versus 54 percent, $p < 0.01$, not shown). IT-Weak firms also report a greater *scope* and *existence* of total and non-IT-related internal control problems in every COSO component ($p < 0.01$).

A MANOVA followed by univariate ANOVAs and Tukey multiple comparison tests reveals that the two groups of firms are not significantly different in terms of size (*ASSETS*, *BV*, *MV*, *SALES*), but IT-Weak firms are significantly less profitable than Non-IT-Weak firms (*ROA*, $p < 0.01$). Consistent with Ge and McVay's (2005) SOX 302 MW firms, both groups have a negative *ROA*, indicating lower abilities and/or resources to implement controls-and even more so for the IT-Weak firms.

Table 4 reveals that 100 percent of the IT-Weak firms have a weak control activities component (*CTRLACT*), making the coefficient estimation of Equation (2) impossible. Hence, we exclude the control activities component from Equation (2), which is used to test the association of each COSO component to misstatements and non-IT-related MWs. In summary, Tables 3 and 4 indicate that IT-Weak firms appear to have more MWs and

TABLE 4
Descriptive Statistics[a,b,c]

Variables	Full Sample (n = 490)	IT Analysis: IT-Weak Firms (n = 129)	IT Analysis: Non-IT-Weak Firms (n = 361)
SOX 404 Variables			
CTRLENV	0.54	0.81	0.44**
RISKAS	0.31	0.48	0.25**
CTRLACT	0.76	1.00	0.68**
INFOCOM	0.11	0.24	0.07**
MONITOR	0.42	0.66	0.34**
SCOPE	2.14	3.19	1.77**
ITCTRLENV	0.06	0.24	NA
ITRISKAS	0.01	0.02	NA
ITCTRLACT	0.25	0.95	NA
ITINFOCOM	0.02	0.06	NA
ITMONITOR	0.07	0.26	NA
ITSCOPE	0.40	1.53	NA
ITMW	0.26	1.00	0.00
MSTMT	2.32	3.33	1.95**
MWNum	2.47	4.53	1.74**
NONITMWNum	2.12	3.18	1.74**
NCTRLENV	0.53	0.79	0.44**
NRISKAS	0.31	0.48	0.25**
NCTRLACT	0.75	0.95	0.68**
NINFOCOM	0.11	0.22	0.07**
NMONITOR	0.40	0.58	0.34**
NSCOPE	2.10	3.02	1.77**
Financial Variables			
ASSETS (M)	8,885	10,031	8,476
BV (per share)	7.96	7.17	8.25
FOREIGN	0.26	0.29	0.25
MERGER	0.19	0.21	0.19
MV (M)	2,599	1,453	3,009
RESTRUCT	0.27	0.28	0.26
ROA (%)	−2.27	−5.51	−1.11**
SALES (M)	2,352	1,511	2,653

** Indicates (two-tailed) significance at the 0.01 percent level.
[a] See Table 2 for variable definitions.
[b] A Chi-square test was used to examine differences for all 0/1 variables (*CTRLENV*, *RISKAS*, *CTRLACT*, *INFOCOM*, *MONITOR*, *FORCURR*, *ITCTRLENV*, *ITRISKAS*, *ITCTRLACT*, *ITINFOCOM*, *ITMONITOR*, *MERGER*, *NCTRLENV*, *NRISKAS*, *NCTRLACT*, *NINFOCOM*, *NMONITOR*, *RESTRUCT*). All other differences were tested using a MANOVA followed by univariate ANOVAs and Tukey multiple comparison tests.
[c] IT-Weak = firms with one or more IT-related material weaknesses; Non-IT-Weak = firms reporting non-IT-related material weaknesses

misstated accounts than do Non-IT-Weak firms. IT-Weak firms also have MWs related to more COSO components whether a *scope* or *existence* measure is utilized.

Interrelatedness of COSO Components

We hypothesize positive associations between a weak control environment and each of the other weak COSO components (H1a). We also hypothesize a positive association between the ''building'' relationships of the components (H1b–H1d) as well as a positive association between monitoring and both risk assessment and control activities (H1e–H1f). For an initial examination of H1, Table 5 presents Pearson and Spearman correlation statistics showing that a weak control environment (*CTRLENV*) is positively related to a weak risk assessment (*RISKAS*, Spearman $r = 0.2224$, $p < 0.01$), control activities (*CTRLACT*, $r = 0.3029$, $p < 0.01$), information and communication (*INFOCOM*, $r = 0.2451$, $p < 0.01$), and monitoring (*MONITOR*, $r = 0.1728$, $p < 0.01$). Significant positive correlations exist between the weak components (H1b–H1d). Weak monitoring is positively related to weak risk assessment (*RISKAS*, $r = 0.1042$, $p < 0.01$) and weak control activities (*CTRLACT*, $r = 0.1667$, $p < 0.01$). Thus, the correlation results support that the weak components are associated as hypothesized.

Figure 1 shows the SEM results. The model appears to be a reasonably "good" fitted model based on three measures: the Chi-square divided by the model's degrees of freedom (*CMINDF*) (5.8530), the comparative fit index (*CFI*) (0.9680), and the root mean square error of approximation (*RMSEA*) (0.0996).[3] Similar to the correlation results, the SEM results show that a weak control environment (*CTRLENV*) is positively related ($p < 0.01$) to each of the other weak COSO components. With the exception of the link between weak control activities and weak information and communication, each weak component is positively related to its weak successor ($p < 0.01$). Weak monitoring is also positively related to weak risk assessment ($p < 0.10$) and weak control activities ($p < 0.05$).

We extend Figure 1 to include the effect of an IT-related MW (*ITMW*). Specifically, this SEM model captures the effect of an IT MW on the *number* of non-IT-related MWs by weak COSO component. This model appears to be a reasonably "well" fitted model based on the *CMINDF* (1.0293), *CFI* (1.0000), and *RMSEA* (0.0077). Figure 2 shows that an IT MW is positively related to the number of non-IT-related MWs reported in each weak component except for information and communication. The insignificance could be the result of only two potential MW types for information and communication (see Table 3). Thus, similar to the univariate analysis results, SEM shows that having an IT-related MW appears to have a pervasive, negative effect on almost every weak COSO component. Moreover, in this SEM model, all of the "building" relationships are significantly positive.

The correlations and SEM support our hypotheses that a weak control environment is positively related to other weak components (H1a) as well as the "building" relation between the weak components (H1b–H1d). The results also support our hypotheses that weak monitoring is positively associated with weak risk assessment and weak control activities (H1e–H1f). Taken together, the results provide evidence that not only is the control environment the foundation of the internal control system, but MWs in one component can easily influence the presence of MWs in other components. Moreover, an IT MW has a negative pervasive impact on the entire control system.

Weak Components and IT

We examine which weak components are positively associated with misstatements as well as the impact of IT. Specifically, H2 tests the effect of ineffective controls, measured by weak components, on the number of misstated accounts. Hypotheses 3 and 4 test the effect of IT on the number of misstated accounts and non-IT-related MWs.

Table 5's correlations reveal that the *scope* (*SCOPE*) of the MWs is positively correlated with each weak COSO component. The same relationship holds for both IT and non-IT *scope* (*ITSCOPE*, *NSCOPE*, not shown) and weak COSO components. Table 5 also shows

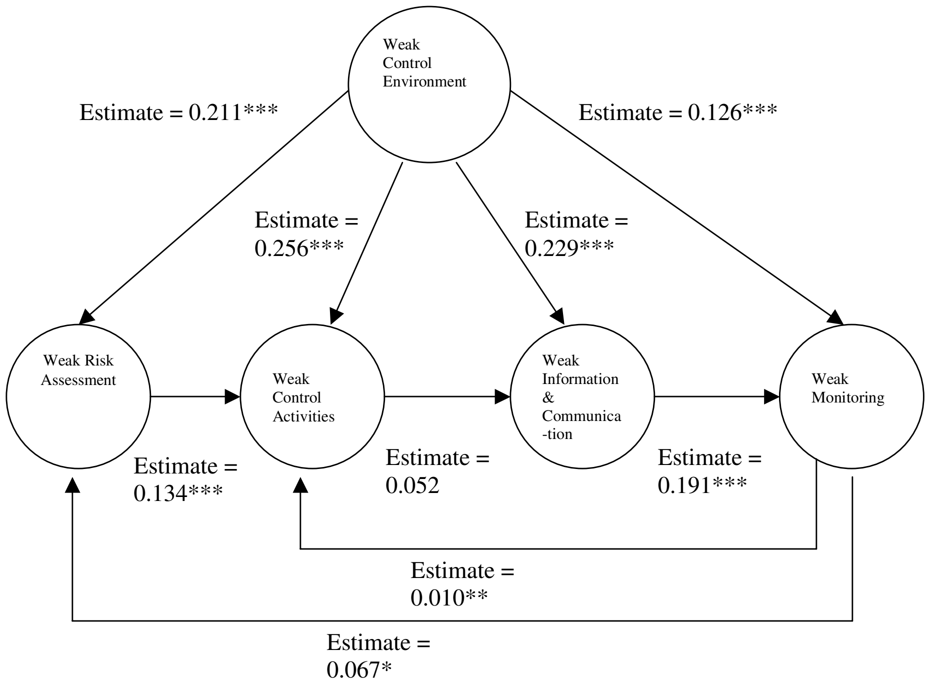
[3] Burney and Matherly (2007, 59, footnote 11) specify the guidelines for defining a reasonably well fitted model.

TABLE 5
Pearson/Spearman Correlations[a]
(n = 490)

Variables[a]		**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
CTRLENV	A		**0.2224**	**0.3029**	**0.2451**	**0.1728**	**0.3254**	**0.3680**	**0.3356**	**0.2780**	−0.0352	**−0.1601**	**0.6774**
RISKAS	**B**	**0.2224**		**0.2018**	**0.1732**	**0.1042**	**0.2172**	**0.3717**	**0.3606**	**0.2366**	0.0169	−0.0349	**0.5809**
CTRLACT	**C**	**0.3029**	**0.2018**		**0.1410**	**0.1669**	**0.3348**	**0.2835**	**0.2511**	**0.2166**	−0.0669	**−0.1037**	**0.6045**
INFOCOM	**D**	**0.2451**	**0.1732**	**0.1410**		**0.2269**	**0.2368**	**0.3950**	**0.3602**	**0.3360**	0.0004	−0.0877	**0.5248**
MONITOR	**E**	**0.1728**	**0.1042**	**0.1667**	**0.2269**		**0.2888**	**0.3232**	**0.2877**	**0.2562**	−0.0533	−0.0666	**0.5843**
ITMW	**F**	**0.3254**	**0.2172**	**0.3348**	**0.2368**	**0.2888**		**0.4758**	**0.2984**	**0.3527**	−0.0353	**−0.1103**	**0.4724**
MWNum	**G**	**0.4321**	**0.3746**	**0.4001**	**0.3327**	**0.3011**	**0.4970**		**0.9619**	**0.7080**	0.0337	**−0.2073**	**0.5772**
NONITMWNum	**H**	**0.3490**	**0.3426**	**0.2950**	**0.2891**	**0.2445**	**0.1966**	**0.8991**		**0.7016**	0.0329	**−0.2091**	**0.5288**
MSTMT	**I**	**0.2475**	**0.1927**	**0.1981**	**0.2667**	**0.2454**	**0.3331**	**0.6430**	**0.5924**		−0.0225	**−0.1234**	**0.4348**
MV	**J**	−0.0539	0.0511	**−0.1684**	0.0697	0.0661	−0.0763	**−0.1871**	**−0.1513**	−0.0282		0.0329	−0.0488
ROA	**K**	**−0.1373**	**−0.0976**	**−0.1373**	**−0.1451**	−0.0657	**−0.1249**	**−0.2904**	**−0.2850**	**−0.1671**	**0.3237**		**−0.1523**
SCOPE	**L**	**0.6962**	**0.5687**	**0.6153**	**0.4653**	**0.5797**	**0.4673**	**0.6110**	**0.4971**	**0.3738**	−0.0194	**−0.1849**	

[a] See Table 2 for complete variable definitions. The upper right-hand portion of the table presents Pearson correlation coefficients, while the lower presents Spearman correlation coefficients. Bold text indicates (two-tailed) significance of at least 0.05.

FIGURE 1
Structural Equation Model
Interrelatedness of the COSO Framework Components[a]



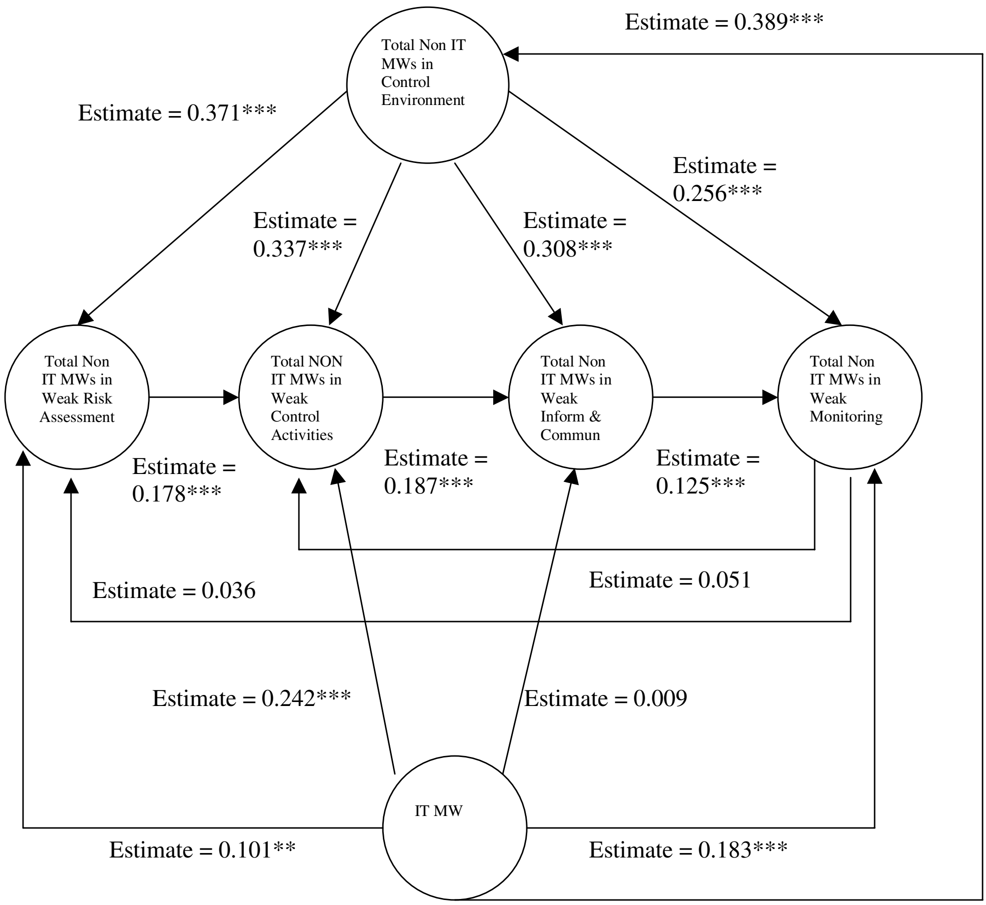
Chi-square divided by the degrees of freedom (CMINDF)	5.8530
Comparative Fit Index (CFI)	0.9680
Root Mean Square Error of Approximation (RMSEA)	0.0996

***, **, * Indicates significance at the 0.01, 0.05, and 0.10 levels, respectively. The estimates are the standardize path coefficients.
[a] Variables represent a weak COSO component (i.e., at least one IT or non-IT material weakness).

that misstatements (*MSTMT*) are positively related to the *existence* of a weak COSO component (*CTRLENV*, *RISKAS*, *CTRLACT*, *INFOCOM*, *MONITOR*), as well as the presence of an IT-related MW (*ITMW*). These results indicate that misstated accounts are positively associated with MW in *any* of the components, regardless of whether the MW is related to IT or not (correlation analysis not shown). We use regression analysis to further analyze these relationships.

Table 6 presents regression results for hypotheses 2, 3, and 4. With respect to H2, our *scope* Equation (1) shows a significantly positive association between the number of weak components (*SCOPE*, $p < 0.01$) and the number of misstated accounts (*MSTMT*), indicating that the more ineffective COSO components, the greater the number of misstated accounts. As shown in Equation (2) for *MSTMT*, the *scope* results are driven by the *existence* of MWs in control environment, information and communication, and monitoring. The excluded control activities component would, in a practical sense, contribute to the existence

FIGURE 2
Structural Equation Model
The Impact of Information Technology Material Weakness on Non-IT Material Weaknesses[a]



Chi-square divided by the degrees of freedom (CMINDF)	1.0293
Comparative Fit Index (CFI)	1.0000
Root Mean Square Error of Approximation (RMSEA)	0.0077

***, **, * Indicates significance at the 0.01, 0.05, and 0.10 levels, respectively. The estimates are the standardize path coefficients.
[a] IT MW equals 1 if a firm has at least one IT-related material weakness, 0 otherwise. The remaining variables are the number of non-IT related material weaknesses reported in the component.

of misstatements as evidenced by the positive correlation between misstatements and control activities (Table 5). Thus, combining the univariate and multivariate analyses, H2 is supported by the *scope* of MWs and *existence* of MWs in all components except risk assessment.

Table 6 shows that the interaction between *ITMW* and *SCOPE* is significantly positive for both misstatements (*MSTMT*, $p < 0.01$) and non-IT-related MWs (*NONITMWNum*, $p < 0.01$)—indicating that IT-Weak firms have more misstatements and more non-IT-related

TABLE 6
Multivariate Analysis of COSO Components: Non-IT-Weak versus IT-Weak Firms[a]
(n = 490)

		Dependent Variable			
		(1)	(2)	(1)	(2)
Equation		***MSTMT***	***MSTMT***	***NONITMWNum***	***NONITMWNum***
Intercept		0.2416*	0.4188***	−0.3659**	−0.0243
SCOPE	+	0.1555***		0.3331***	
CTRLENV	+		0.1431**		0.3846***
RISKAS	+		0.0790		0.4326***
INFOCOM	+		0.3314***		0.3751***
MONITOR	+		0.1758***		0.2191***
*SCOPE * ITMW*	+	0.0925***		0.0518***	
*CTRLENV * ITMW*	+		0.2479**		0.0062
*RISKAS * ITMW*	+		0.1914*		0.1328
*INFOCOM * ITMW*	+		−0.0150		−0.0204
*MONITOR * ITMW*	+		0.0086		0.2176**
Log(*MV*)	−	0.0147	0.0052	0.0324*	0.0167
ROA	−	−0.0018	−0.0016	−0.0060***	−0.0060***
FOREIGN	+	0.0988*	0.1081*	−0.0314	−0.0540
MERGER	+	−0.1008*	−0.0950	−0.0960	−0.1145*
RESTRUCT	+	0.0980*	0.0993*	0.0951*	0.0942*
Regression Type		Poisson	Poisson	Poisson	Poisson
Log Likelihood		−109.1247	−108.6489	−111.6091	−104.4526
Likelihood Ratio Chi-square		145.9908 (0.0001)	146.9425 (0.0001)	311.8290 (0.0001)	310.2548 (0.0001)

*, **, *** Indicates (one-tailed) significance at the 0.10 percent, 0.05 percent, and 0.01 percent levels, respectively.
Poisson regressions were checked for overdispersion and underdispersion. The control activity component is not included in the regressions because one hundred percent of the IT-Weak firms have a weakness in that component.
[a] See Table 2 for variable definitions.

MWs, supporting hypotheses 3 and 4, respectively. For misstatements, Equation (2) reveals that the IT *scope* results are driven by MWs in the control environment (*CTRLENV * ITMW*, $p < 0.05$) and risk assessment (*RISKAS * ITMW*, $p < 0.10$). For non-IT-related MWs, Equation (2) shows that the IT *scope* results are driven by MWs in monitoring (*MONITOR * ITMW*, $p < 0.05$). Thus, IT-Weak firms report more misstated accounts primarily due to the impact of additional MWs in the control environment and risk assessment components as well as more non-IT-related MWs primarily due to additional MWs in the monitoring component.

ROA ($p < 0.01$) is negatively associated with the number of non-IT-related MWs (*NONITMWNum*), but not misstatements (*MSTMT*), indicating that less profitable firms report more non-IT-related MWs. The presence of foreign operations (*FOREIGN*, $p < 0.10$) and restructuring (*RESTRUCT*, $p < 0.10$) have positive associations with misstatements (*MSTMT*), indicating that these operational and reporting complexities can increase the number of misstatements. Restructuring also has a positive association with non-IT-related

MWs (*NONITMWNum*, $p < 0.10$). Mergers (*MERGER*, $p < 0.10$) are associated with our dependent variables in the opposite direction as predicted, potentially signaling that firms extensively evaluate the internal controls of new acquisitions in this SOX environment.

Finally, market value (*MV*, $p < 0.10$) is only positively associated with the number of non-IT-related MWs (*NONITMWNum*), indicating that larger firms are more likely to report more non-IT-related MWs. To explore these results in more detail, we ran the regressions separately for IT-Weak and Non-IT-Weak firms. The results (not shown) reveal a significantly positive relationship between market value (*MV*) and both misstatements and non-IT-related MWs for IT-Weak firms only, signifying a greater number of misstatements and non-IT-related MWs for larger firms—the exact opposite relationship of earlier ‘‘error’’ studies and firm size (Bell et al. 1998; Eilifsen and Messier 2000). A potential explanation for our result is that today larger firms may have more complex systems, and because of the pervasiveness of IT, when they experience an MW, it has a greater impact on the number of misstated accounts and non-IT-related MWs.

Additional Analysis

Table 6 identifies which (total) components are significantly different between Non-IT-Weak and IT-Weak firms with respect to misstatements and non-IT-related MWs. To examine the control activities component, we extend this analysis to examine which Non-IT-Weak and IT-Weak components are related to misstatements. Table 7 shows that while all five Non-IT-Weak components contribute to misstatements, only the first three IT-weak components, control environment, risk assessment, and control activities, are positively associated with misstatements. These results further support the importance of the IT control environment, IT risk assessment, and IT control activities in establishing reliable financial reporting. Finally, the results do not change at the 5 percent significance level if different measures of size are used (i.e., book value, *BV*, log of *SALES*, or log of *ASSETS*) or *ITMW* is added as an additional control variable, indicating that the results are robust.

V. DISCUSSION

This study contributes to the post-SOX 404 internal control literature by (1) providing evidence on the interrelatedness of weak COSO components, (2) examining the effect of weak components on misstatements, and (3) analyzing the role of IT-related MWs. We employ two perspectives, *scope,* the number of weak COSO components, and *existence*, a control problem in a specific weak component, to analyze IT and non-IT MWs. Our analysis provides a basis for understanding the functionality of the *Framework* as well as the impact of weak components, IT and non-IT, on financial reporting reliability. Understanding these relationships is important to help managers, auditors, and regulators evaluate internal controls and the reported MWs; maintain investor confidence in the capital markets; and provide all stakeholders with insights about the role of IT in control effectiveness.

Multivariate analysis shows that a weak control environment is positively related to weak risk assessment, control activities, information and communication, and monitoring components. Also, a weak risk assessment component is positively related to a weak control activities component; MWs in the control activities component are positively related to MWs in the information and communication component; and a weak information and communication component is positively related to a weak monitoring component. Our results indicate (1) the need for an appropriate ‘‘tone at the top,’’ and (2) the impact of a component's MW on other components.

Our analyses show that IT-Weak firms not only have IT problems, but they also have more problems in general—more non-IT-related MWs, misstatements, and weak COSO

TABLE 7
Multivariate Analysis of COSO Components: Non-IT-Weak versus IT-Weak Components[a]
(n = 490)

		Dependent Variable *MSTMT*
Intercept		0.1977
NCTRLENV	+	0.1709***
NRISKAS	+	0.0980*
NCTRLACT	+	0.1895***
NINFOCOM	+	0.3221***
NMONITOR	+	0.1525***
ITCTRLENV	+	0.1585*
ITRISKAS	+	0.5174**
ITCTRLACT	+	0.2210***
ITINFOCOM	+	−0.1073
ITMONITOR	+	0.1027
Log(MV)	−	0.0170
ROA	−	−0.0017
FOREIGN	+	0.0894*
MERGER	+	−0.0735
RESTRUCT	+	0.1053**
Regression Type		Poisson
Log Likelihood		−116.5054
Likelihood Ratio		155.1663
Chi-square		(0.0001)

*, **, *** Indicates (one-tailed) significance at the 0.10 percent, 0.05 percent, and 0.01 percent levels, respectively.
Poisson regressions were checked for overdispersion and underdispersion.
[a] See Table 2 for variable definitions.

components. In addition, IT-Weak firms report a greater *scope* of internal control problems, i.e., internal control problems that involve multiple COSO components, as well as a greater negative effect for the *existence* of an IT internal control problem in selected COSO components. We find evidence that weak IT control environment, risk assessment, and control activities decrease financial reporting reliability. These results support the Information Technology Governance Institute's (ITGI) contention that "the reliability of financial reporting is heavily dependent on a well-controlled IT environment" (ITGI 2004, 5).

More than 90 percent of the firms reported MWs in the control activity of accounting documentation, policy, and procedures (see Table 3). Additionally, control activities consist of more MW types than any other component. Given the interrelatedness of the components, it would seem that the high frequency of control activity MWs would result in a higher number of MWs in other components as well. Several possible explanations exist. First, firms (and auditors) may be focusing their efforts on the control activities component, which coincides with ITGI's contention that many firms' documentation addresses only the control activity component (ITGI 2007, 40). Second, the other components may have significant deficiencies, but not MWs, and are not included in our analysis.

As with any sample-based research, care should be taken when generalizing our results to other firms and time periods. However, this paper provides a beginning point for research on the 1992 COSO *Internal Control Framework* and firms that fail their mandated SOX 404 report. Future research can expand the ''fail'' sample and evaluate it with respect to ''pass'' firms over time and/or by industry. Future research can examine different classifying schemes for IT and non-IT MWs, especially in the areas related to personnel and complexity. Finally, future research can identify systematic differences between firms with the same financial ability but different levels of internal control effectiveness.

APPENDIX

Examples of SOX 404 Weaknesses classified by COSO Component based on COBIT, COSO, and GTAG

COSO Component	SOX 404 Internal Control Weakness	Justification of COSO Classification
Control Environment (*CTRLENV*)	ineffective or understaffed audit committee	COSO Framework, p. 27: Board of Directors and Audit Committee identified as relevant to control environment effectiveness.
	lack of systems training	COBIT 4.1 DS7, p. 173: Educate and train users on the system primarily the control environment.
Risk Assessment (*RISKAS*)	foreign, subsidiary, acquisition, merger, disposal, or reorganization issues	COSO Evaluation Tools, pp. 26–27: Managing change includes handling foreign operations, corporate restructuring as well as new lines, products, activities, and acquisitions.
	weak (IT) risk assessment	Identified as weak by the firm.
Control Activities (*CTRLACT*)	inadequate account reconciliations and segregation of duties	COSO Executive Summary, p. 2: Control activities include approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
	logical access and security issues	COBIT 4.1 DS5, p. 173: Identifies ensure system security including access rights (p. 118) as primarily a control activity. COSO Framework, pp. 46–49: Identifies access to data as a control activity.
Information & Communication (*INFOCOM*)	lack of communication	COSO Executive Summary, p. 3: Indicates that effective communication is needed throughout the organization to have effective information and communication.
	inadequate information flow	COSO Framework, p. 58: States that information should be appropriate, timely, current, accurate, and accessible
	weak (IT) information and communication	Identified as weak by the firm.
Monitoring (*MONITOR*)	lack of supervision or oversight	COSO Executive Summary, p. 3: Monitoring includes supervisory activities. COSO Framework p. 68: States that ''supervisory activities provide oversight of control functions.''
	weak (IT) monitoring	Identified as weak by the firm.

COBIT 4.1 (2007) refers to the document released by the IT Governance Institute (ITGI). COSO *Internal Control-Integrated Framework* (1992) is divided into four different books: the Executive Summary, the Framework, the Evaluation Tools, and Reporting to External Parties. The appropriate book is referenced above. GTAG refers to the *Global Technology Audit Guide: Information Technology Controls* (2005) developed by the Institute of Internal Auditors. A complete list of the justification of the COSO mapping of the weaknesses in Table 3 is available from the authors.

REFERENCES

Ashbaugh-Skaife, H., D. W. Collins, and W. R. Kinney, Jr. 2007. The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. *Journal of Accounting and Economics* 44 (1/2): 166–192.

Bell, T. B., W. R. Knechel, J. L. Payne, and J. J. Willingham. 1998. An empirical investigation of the relationship between the computerization of accounting systems and the incidence and size of audit differences. *Auditing: A Journal of Practice & Theory* 17 (1): 13–38.

Beneish, M. D., M. B. Billings, and L. D. Hodder. 2008. Internal control weaknesses and information uncertainty. *The Accounting Review* 83 (3): 665–704.

Burney, L. L., and M. Matherly. 2007. Examining performance measurement from an integrated perspective. *Journal of Information Systems* 21 (2): 49–68.

Caster, P., D. W. Massey, and A. M. Wright. 2000. Research on the nature, characteristics, and causes of accounting errors: The need for a multi-method approach. *Journal of Accounting Literature* 19: 60–92.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1992. *Internal Control-Integrated Framework*. Jersey City, NJ: AICPA.

———. 2008. *Internal Control-Integrated Framework Guidance on Monitoring Internal Control Systems Exposure Draft* (June). Available at: http://www.coso.org/documents/VolumeI-ExecutiveSummary.pdf.

Doyle, J., W. Ge, and S. McVay. 2007a. Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics* 44 (1/2): 193–223.

———, ———, and ———. 2007b. Accruals quality and internal control over financial reporting. Working paper, Utah State University, University of Washington, and New York University.

Eilifsen, A., and W. F. Messier, Jr. 2000. The incidence and detection of misstatements: A review and integration of archival research. *Journal of Accounting Literature* 19: 1–43.

Ge, W., and S. McVay. 2005. The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. *Accounting Horizons* 19 (3): 137–158.

Geiger, M. A., S. M. Cooper, and E. J. Boyle. 2004. Internal control components: Did COSO get it right? *The CPA Journal* 74 (1): 28–31.

Hammersley, J., L. Myers, and C. Shakespeare. 2008. Market reactions to the disclosure of internal control weaknesses and to the characteristics of those weaknesses under Section 302 of the Sarbanes Oxley Act of 2002. *Review of Accounting Studies* 13 (1): 141–165.

Institute of Internal Auditors (IIA). 2005. *Global Technology Audit Guide: Information Technology Controls*. Altamonte Springs, FL: IIA.

IT Governance Institute (ITGI). 2004. *IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control over Disclosure and Financial Reporting*. Rolling Meadows, IL. Available at: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27526.

———. 2007. *COBIT 4.1: Framework Control Objectives Management Guidelines Maturity Models*. Rolling Meadows, IL: ITGI.

Jain, P. K., J. Kim, and Z. Rezaee. 2008. The Sarbanes-Oxley Act of 2002 and market liquidity. *Financial Review* 43 (3): 361–382.

Kinney, W. R. 2000. Discussant comments on research on nature, characteristics, and causes of accounting errors: The need for a multi-method approach. *Journal of Accounting Literature* 19: 93–101.

Kreutzfeldt, R. W., and W. A. Wallace. 2000. Discussants' comments on: The incidence and detection of misstatements: A review and integration of archival research. *Journal of Accounting Literature* 19: 44–59.

Li, C., G. Peters, V. J. Richardson, and M. W. Watson. 2008. The consequences of poor data quality on decision making: The case of Sarbanes-Oxley information technology material weaknesses. Working paper, University of Pittsburgh, University of Arkansas, and Mississippi State University.

Messier, W. F., Jr., A. Eilifsen, and L. A. Austen. 2004. Auditor detected misstatements and the effect of information technology. *International Journal of Auditing* 8 (3): 223–235.

Public Company Accounting Oversight Board (PCAOB). 2004. *An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statements*. Auditing Standard No. 2. Available at: http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_2.pdf.

———. 2007. An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statements. Auditing Standard No. 5. Available at: http://www.pcaobus.org/Rules/Docket_021/2007-05-24_Release_No_2007-005.pdf.