

**WHAT DO AUDITOR'S REPORTS ON INTERNAL CONTROL TELL US
ABOUT IT CONTROL WEAKNESSES IN FINANCIAL REPORTING SYSTEMS?***

EFRIM BORITZ, *University of Waterloo*
LOUISE HAYES, *University of Waterloo*
JEE-HAE LIM, *University of Waterloo*

July 2010

Contact: Efrim Boritz
jeboritz@uwaterloo.ca
(519) 888-4567 x357774

*We wish to acknowledge the funding provided by the 2009 CAAA/CICA Research Program and the 2009 University of Waterloo Centre for Information Systems Assurance, sponsored by the Canadian Institute of Chartered Accountants, ISACA, and CaseWare IDEA Inc. We gratefully acknowledge the comments of four anonymous reviewers and participants at the 2010 Mid-Year Meeting of the Information Systems Section of the American Accounting Association, 2010 the Canadian Academic Accounting Association Annual Conference, the 2010 European Accounting Association Annual Congress 2010 and the 2009 University of Waterloo Symposium on Information Integrity and Information Systems Assurance, particularly those of Gary Baker and Ed O'Donnell.

Abstract

After five years and hundreds of SOX 404 reports of material control weaknesses, including information technology (IT) weaknesses, there are no published studies of IT weaknesses at a detailed level and their associations with non-IT control weaknesses and financial misstatements. This study contributes to our understanding of internal control by using content analysis to identify IT weaknesses as reported by auditors rather than managers and without grouping controls according to textbooks, professional standards, or other frameworks. Analysing auditor's SOX 404 reports for the five year period 2004-08 we find, contrary to the assumption implicit in studies that classify ITWs as 'company-wide', that not all ITWs reported are general control weaknesses having entity-wide, pervasive effects on applications. We demonstrate the advantages and limitations of using content analysis software to identify IT weaknesses and show that SOX 404 reports classified under a single code by Audit Analytics can be sub-divided into meaningful sub-categories based on content analysis. We identify a small number of frequently-occurring combinations of IT control weaknesses and non-IT control weaknesses in auditors' reports. We identify a significant change in auditors' SOX 404 reports after 2006, and differences in reported IT control weaknesses associated with industry, size, and auditor type. We also investigate differences in the persistence of non-IT and IT weaknesses. We present our content analysis dictionary of words and phrases, search logic, and findings to help other researchers hampered by the lacking granularity of the coding of IT weaknesses in *Audit Analytics*.

Key words: SOX 404, IT control weaknesses, Content analysis, relationship between IT and non-IT control weaknesses

1. Introduction

For decades managers, auditors, and regulators have recognized that effective internal controls over the use of information technology (IT) are integral to reliable financial reporting.

Organizations with weak IT controls are more likely to experience difficulty in consistently performing control activities, such as change management and access control. *General* controls are thought to have a “pervasive” effect on other IT controls (Public Company Accounting Oversight Board (PCAOB) Auditing Standard No.2). That is, if a relevant IT general control fails (e.g., a control restricting access to programs and data) it is expected to have a pervasive impact on all systems and the application controls that rely on it, the failure of which may lead to financial misstatements. In addition, it may be much more difficult to rapidly remediate weaknesses in IT controls (Canada et al., 2009), suggesting that IT control weaknesses may also be more persistent than other control weaknesses.

The Section 404 reporting requirements of the Sarbanes-Oxley Act (SOX)¹ that took effect in 2004 created a powerful setting in which to test these assertions. Section 404 requires that public company annual filings contain both management’s and an independent auditor’s assessment of the operating effectiveness of their internal control over financial reporting (SEC 2003). However, managements’ and auditors’ reporting of internal control weaknesses have not been identical. Interestingly, managements’ reports of internal control weaknesses often identify more weaknesses than auditors’ reports do. This has been attributed to an overabundance of conservatism on the part of management due to the penalties associated with failing to comply with SOX reporting requirements. Thus, an investigation of auditors’ reports enables researchers

¹ Section 404 of the Sarbanes-Oxley Act (SEC 2003) requires that the CFO and CEO of companies traded on US exchanges annually report on, and certify, the effectiveness of controls over financial reporting, including IT controls. External auditors are also required to attest to control effectiveness and, prior to a change in auditing standards in 2007, report on management’s internal control assessment.

to rely on the assessments of an independent third party of the effectiveness of a firm's internal control.

This study is particularly concerned about IT control weaknesses due to their special characteristics and the characteristics of the firms that report IT weaknesses and how IT weaknesses relate to non-IT weaknesses and the misstatements associated with the reported weaknesses. However, after five years and hundreds of SOX 404 auditors' reports of material control weaknesses, including IT weaknesses, there are no published empirical studies of the association between IT and non-IT control weaknesses² at a granular level. In some previous studies, IT controls have been treated simply as being a subset of internal control and differences in special characteristics of individual IT weaknesses have not been recognized or addressed. The *Audit Analytics* database identifies 21 internal control weaknesses (Figure 1) that appear in SOX 404 reports and tags company information with the item numbers of the weaknesses reported. IT control weaknesses (item 20) are all classified in one category. Researchers frequently rely on the single code provided in the *Audit Analytics*' database to indicate the presence or absence of IT weaknesses. Both the frequency and distribution of various non-IT weaknesses in companies with IT weaknesses is significantly different from those in companies without IT weaknesses (Klamm and Watson 2009). Thus, companies with IT weaknesses represent a distinct subpopulation of public companies that is worthy of research attention.

The few previous studies that have recognized the special nature of IT weaknesses have either treated IT weaknesses as a subset of company-wide internal controls (e.g., Doyle et al. 2007a, b) or studied the IT weaknesses on an aggregated basis, grouping weaknesses according to common practice (e.g., Masli et al., 2009) or in accordance with IT control frameworks published

² We relied on companies' non-IT internal control weaknesses as reported in the *Audit Analytics* database which identifies 20 non-IT internal control weaknesses (Figure 1) that appear in SOX 404 reports and tags company information with the item numbers of the weaknesses reported.

by professional associations such as COSO³ (e.g., Klamm and Watson, 2009) or COBIT⁴ (e.g., Li et al., 2008). However, these frameworks are not mandatory usage and their aggregated categories of controls may not fully represent the individual controls implemented by organizations or the specific weaknesses identified by management and auditors. This study complements previous studies by providing a more granular analysis of IT control weaknesses (ITWs) and how they are correlated with non-IT weaknesses (ICWs), accounting rule application failures and key factors such as time, industry, firm size, and auditor type. Following prior research (Moody's 2006; Goh 2009), we also examine differences in the remediation of various types of IT weaknesses.

The purpose of this study is to deepen our understanding of internal control by examining weaknesses reported in SOX 404 auditors' reports (as opposed to managements' reports) at a detailed level. Heeding Hunton's (2000) admonition that "a framework can lead us to believe that the framework is the world and this can inhibit our ability to think outside the box" we decided to use content analysis to identify IT weakness disclosures in SOX 404 auditors' reports, without referencing any particular control framework. Based on an automated content analysis of auditors' SOX 404 reports from 2004-08, we find auditors' terminology choices seldom reflect published IT frameworks. Also, associations of types of ITWs with ICWs and financial misstatements were not as simplistic as hypothesized. Reported IT control weaknesses often co-occur with a small number of other IT control weaknesses, factors such as industry, company size, and auditor type influence IT and non-IT weaknesses, or their reporting, differently. A downward trend in the number of IT

³SOX 404 requires management and auditors identify the framework used to assess the effectiveness of internal control over financial reporting. The framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) is the one most frequently used to meet the SOX requirement that internal control be evaluated with a "suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment" (SEC 2003).

⁴COBIT®, Control Objectives for Information and related Technology (IT Governance Institute 2007) outlines good practices that fit with and support the COSO Framework.

weaknesses reported from 2004 –08 and changes in control weakness associations have made more recent SOX 404 reports difficult to compare against earlier reports.

Our study makes several contributions with implications for academics, managers, and standard setters. First, this study adds to the academic and professional literature on internal control by using content analysis to identify IT weaknesses as reported by auditors rather than managers and without grouping controls according to textbooks, professional standards, or other frameworks. Secondly, we find, contrary to the assumption implicit in studies that classify ITWs as ‘company-wide’, that not all reported ITWs are general control weaknesses and they do not appear to have entity-wide, pervasive effects on applications. Taken together, these findings may indicate a need for testing the robustness of the results of previous internal control studies. Third, we identify co-occurring combinations of weaknesses representing an identifiable target for future research, education, and remediation. One such combination is IT monitoring and design weaknesses and non-IT weaknesses related to entry controls, period-end issues, and accounting resourcing. Another combination is IT access control and segregation of duties weaknesses and non-IT segregation of duties weaknesses. Fourth, we document a particularly significant change in the number and nature of IT weaknesses reported between 2004-06 and 2007-08 that appear to be associated with a change in regulation in 2007 (i.e., Auditing Standard No. 5 superseded Auditing Standard No. 2 effective November 15, 2007, with earlier adoption permitted after its acceptance by the SEC in the summer of 2007). This finding suggests that caution should be used when generalizing results of early SOX 404 studies to the present day. Further investigation of the possible differential effect of Auditing Standard No. 5 on auditors’ reports of IT and non-IT weaknesses may be warranted.

Finally, methodologically, this study demonstrates the advantages and limitations of using content analysis software in the study of narrative reports on the effectiveness of internal

control⁵. Until now, other researchers who have used SOX 404 reports to study IT control weaknesses have identified IT weaknesses through an arduous manual process. The resource demands of relying on experts to visually scan and identify IT weaknesses in text data sources impacts on research design decisions and represents an obstacle both to reliably linking the presence of IT control weaknesses with other variables - such as financial performance, audit fees, and governance - and to determining implications of those associations. Our 'dictionary' of keywords/phrases used in the automated identification of IT weaknesses provides a snapshot of IT-related terminology actually used by auditors (as contrasted with managers). This dictionary may help some researchers to speed development of text analysis approaches for studying internal control in other contexts.

This paper is structured into eight sections, of which this introduction is the first. The second section provides a review of existing research. The third section develops the proposed research questions. The fourth section outlines the methods employed in this study while the fifth section outlines the data sources. The sixth section indicates the results of the statistical analysis of the IT weaknesses combinations and their impact on financial reporting systems. The final two sections present discussion and a summary with limitations, conclusions, and recommendations for future research.

2. Literature Review

Researchers did not enjoy ready access to audited reports on internal control weaknesses until the Section 404 reporting requirements of the Sarbanes-Oxley Act (SOX) took effect in 2004. Thus, it was difficult to obtain direct evidence about the impact of internal control weaknesses on company performance. Now, however, the auditors' reports on internal control are available through the

⁵ While automated search technologies may be a useful additional research tool, researchers should not expect perfect identification and classification using automated search techniques,...

SEC's EDGAR system or more conveniently through the *Audit Analytics* database. This availability of internal control data enables researchers to investigate internal controls in a very detailed manner, and a number of studies addressing internal controls have been published, addressing reported weaknesses in tests of hypotheses about audit fees (Hoitash et al. 2008; Raghunandan and Rama 2006), audit committee quality (Krishnan 2005), financial performance (Boritz and Lim 2008), earnings management and accruals (Ashbaugh-Skaife et al. 2008; Cohen, Dey and Lys 2008), stock price and cost of capital reactions to the disclosures of internal control weaknesses (Beneish, Billings and Hodder 2008; Hammersley, Myers and Shakespeare 2008), executive turnover (Masli et al. 2009), and performance-based executive compensation (Jha, Kobelsky and Lim 2008).

The results of the aforementioned studies indicate that internal control weaknesses have affected all of these factors to some degree. However, to our knowledge, while guidance exists on what controls should exist in well-managed entities⁶, there have been few published studies of the IT weaknesses themselves other than an early study by Gupta and Leech (2005) sponsored by the Financial Executives Research Foundation and the study by Klamm and Watson (2009) that relates both IT and non-IT SOX 404 reported control weaknesses to the five components of the *Committee of Sponsoring Organization's (COSO) Internal Control-Integrated Framework* with IT weaknesses studied at an aggregate, not granular, level in *management's* SOX 404 reports issued in the first year of SOX reporting⁷. It is important to note that our study focuses on *auditors'*

⁶ COBIT®, Control Objectives for Information and related Technology (IT Governance Institute 2007) outlines good practices that fit with and support the Committee of Sponsoring Organisations of the Treadway Commission's (COSO), Internal Control Integrated Framework. The use of a combination of COBIT®, to assess IT related controls, and COSO, meets the SOX requirement that internal control be evaluated with a "suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment" (SEC 2003).

⁷ Until mid-2007 auditors were required to evaluate and opine on management's evaluation process and the control weakness descriptions in management and auditors' reports were usually similar, if not identical. Following the PCAOB acknowledgement that "at times, the related [audit]

reports whose content can differ from managements' reports, as will be discussed later in this paper. Also, our study covers the first five years of SOX 404 reporting, not just the initial period during which reporting of weaknesses was somewhat different from that seen in recent years, as will be discussed later as well.

It is also important to recognize that virtually all companies with reported IT control weaknesses also reported non-IT control weaknesses. This may be a consequence of the decision criteria and process commonly used by auditors to determine whether or not an IT weakness is reportable and the negotiations between auditors and management to determine which weaknesses to report (Wolfe et al. 2009). A common approach adopted by many companies would not identify an IT weakness unless it had caused an application control failure, was judged so pervasive as to undermine the control environment, or had not been remedied within a reasonable period of time (ITGI 2006). Accordingly, *general IT* control failures (e.g., a control restricting access to programs and data) that are thought to have a "pervasive" effect on other IT controls (Public Company Accounting Oversight Board (PCAOB) Auditing Standard No.2) that leads to financial misstatements would be reported. Furthermore, when the pervasive nature of such IT weaknesses makes it much more difficult to rapidly remediate them (Canada et al., 2009), IT control weaknesses are likely to be persistent and will be reported.

Insert Figure 1

3. Research Questions

Internal control (e.g., COSO) and auditing publications (e.g., PCAOB Auditing Standard No. 5) discuss the distinction between various categories of IT controls such as General Controls and

effort has appeared greater than necessary" and the elimination of the requirement to assess managements' evaluative process (May 24, 2007 PCAOB news release www.pcaob.com) differences in control weakness descriptions in management and auditor reports became more frequent.

Application Controls and sub-categories such as the subdivision of General Controls into Operations Controls, System Development and Maintenance Controls, and Security Controls. Our fundamental research interest is to examine IT weaknesses at a more granular level as reported by auditors in their SOX 404 reports with as little aggregation as possible.

The few studies that have investigated associations between IT control weaknesses identified in SOX 404 reports and other factors (Masli et al. 2009; Li et al. 2008; Klamm and Watson 2009) appear to have grouped detailed IT weaknesses before testing the association of the group(s) with other factors. Groupings differ amongst such studies⁸ so the results of those studies may be sensitive to the groupings used and their findings may not generalize to study setting in which sub-categories of IT weaknesses are mapped differently⁹.

It appears that to date researchers have relied on weakness identification performed by experts based on visual scans of the relevant reports, without the aid of content analysis software tools. Experts' awareness of the control categorization scheme to be used in a study may influence identification and characterization of IT weaknesses. A correspondence between the planned use of a categorization scheme and the headings and other descriptors (e.g., General IT controls, COSO component descriptors) that appear in many SOX 404 auditors' reports may influence the identification of IT weaknesses. Also, weaknesses identified through an analysis of auditors' reports may differ from those reported in managements' reports but previous studies have not

⁸ For example, Li et al. (2008) classify SOX 404 reports as with or without IT weaknesses based on the information effectiveness or integrity issues of COBIT 4.1. Klamm and Watson (2009) identify 12 IT material weaknesses in SOX 404 management reports and group these by the five components (control environment, risk assessment, control activities, information and communication and monitoring) of COSO's Internal Control-Integrated Framework. Masli et al. (2009) identify 25 material weaknesses in SOX 404 management reports and group these into seven categories (access controls, enterprise architecture, general IS/IT controls, IT capabilities, security and recovery, application controls and application development).

⁹ For example, masterfile, inadequate IT staffing, and undue reliance on manual processes are likely mapped to 'control activities' by Klamm and Watson (2009) but were likely mapped respectively to application controls, IT capabilities and Enterprise Architecture by Masli et al. (2009).

differentiated between the weaknesses identified in managements' reports and auditors' reports. If IT weaknesses at the sub-category (detailed) level frequently co-occur (e.g., monitoring and design IT weakness are frequently reported in the same SOX 404 reports), research results may not be robust to IT weakness grouping choices that divide these combinations¹⁰. This leads to our first research question:

RQ1: *What are the most common IT control weaknesses reported in auditors' SOX 404 reports and what terminology do auditors choose to describe them?*

The pattern of non-IT control weaknesses reported by companies without IT control weaknesses may be different from the pattern of non-IT control weaknesses reported by companies with IT control weaknesses. Omitting IT weaknesses commonly associated with non-IT weaknesses may lead to incorrect statistical inferences in studies involving these non-IT weaknesses and the misstatements associated with them. This leads to our second and third research questions:

RQ2: *Are non-IT internal control weaknesses associated with IT control weaknesses, and if so, how?*

RQ3: *Are IT control weaknesses associated with financial misstatements, and if so, how?*

Firm attributes and SOX 404 report characteristics may capture the tendency of control weaknesses to co-occur. Our analysis of the four factors (e.g., time, industry, size, and auditor type) influencing overall internal control quality should enhance our understanding of which particular IT control weaknesses are more frequently associated with various non-IT control weaknesses. First, over time, auditors' SOX 404 reporting may have changed. Their role underwent a significant change with the formation of the PCAOB (Krishnan 2005; Raghunandan

¹⁰ In the Method section we describe how we used automated search tools to identify IT weaknesses at a detailed level without reference to existing IT weakness classification frameworks. Such automated identification is consistent (as the process is rules based), replicable, scalable (as data sources expand), and transparent (when dictionaries and search criteria are made available).

and Rama 2006). Their reporting may have changed not only as auditors gained experience through their audits of internal control over financial reporting but also in response to the changes in regulatory guidance when PCAOB Auditing Standard No. 5 superseded Auditing Standard No. 2 effective for fiscal years ending on or after November 15, 2007 (PCAOB 2007)¹¹. Second, industry type is one of the proxies for the incentives to discover and disclose internal control problems (Doyle et al. 2007a)¹². Third, large firms have more expertise (or can afford to acquire specialized services and expert advice). Fourth, prior literature suggests that Big 4 auditors, having more resources and tending to be more conservative than non-Big 4 auditors, are more likely to detect internal control weaknesses than non-Big 4 auditors. In addition, the decision process commonly used by auditors to determine whether or not an IT weakness is reportable (Wolfe et al. 2009; ITGI 2006) may result in companies being more likely to report IT weaknesses if they are also reporting non-IT weaknesses. These observations lead to our fourth research question:

RQ4: *Do the most commonly reported IT control weaknesses differ across factors such as Time (Year of report), Industry, Company Size, Auditor Type, and Overall Internal Control Quality?*

Remediation of certain IT weaknesses (e.g., those requiring the acquisition and development or redesign of large, complex systems) may be difficult and time consuming; thus, IT weaknesses may persist over time, affecting SOX 404 reports in successive periods. Moody's has indicated that the existence of ongoing internal control problems can trigger negative rating action against the firm (Moody's 2006), emphasizing the need for the prompt remediation of internal control

¹¹ Earlier adoption was permitted with SEC approval on July 25, 2007. The auditing standard changes, developed in close consultation with the SEC to address the costs of SOX 404 implementation, were intended to reduce both management and auditor reporting effort by advocating a top-down, risk-based approach to evaluation of internal control over financial reporting and allowing management and auditors to adopt different testing approaches.

¹² For example, the Federal Deposit Insurance Corporation Improvement Act (FDICIA) of 1991 requires banks operating in the United States to file an annual report with regulators in which management attests to the effectiveness of their controls, and their independent public accountants attest to and separately report on management's assertions.

weaknesses to restore confidence in financial reporting, particularly control weaknesses with pervasive or entity-wide impacts. The prompt remediation of material internal control weaknesses presents a strong signal to the market that the firm is committed to and competent in ensuring credible financial reporting (Goh 2009). However, if in the following period a firm reports the same material internal control weakness or discloses a new material weakness, the deficiencies in the internal control system may be perceived as being more chronic than firms that are able to document improvements in their financial reporting process. Thus, our fifth research question is:

RQ5: *Do certain IT control weaknesses persist or are they remediated promptly?*

4. Method

To investigate the RQs, we developed a ‘dictionary’ of words/phrases that we used, in conjunction with Boolean logic and with text analysis software¹³, to identify IT control weaknesses in the SOX 404 auditors’ reports. As a consequence of our methodology, our study is replicable¹⁴, whereas earlier studies that relied on manual reading of the reports may not be able to be reliably replicated and are difficult to scale as future SOX 404 reports become available. The number of IT weaknesses and the number of companies for which IT weaknesses are identified depends on our dictionary and search logic. We developed the dictionary using frequency and key-words-in-context reports from the text analysis software, rather than using textbook and standards terminology. Accordingly, the dictionary of keywords/phrases provides a snapshot of IT terminology actually in use by auditors. We looked to professional guidance for topical headings by which to categorize the over 200 IT weakness dictionary keyword/phrases entries. However, we found that firms referenced COSO components, COBIT domains or the broad categories of

¹³ QDA Miner v 3.0.4 and WordStat 5.1 from Provalis Research Inc.

¹⁴ Such replication may be impacted by retroactive database updates that *Audit Analytics* makes. For example, *Audit Analytics* changed the coding of the auditor’s report in the Feb 13, 2007 10-K/A filing for Danka Business System’s March 31, 2006 year end from a report with IT weaknesses to one without sometime between November, 2009 and February 6, 2010.

“general IT controls” and “application controls” far less than we had expected¹⁵ consistent with Klamm and Watson’s (2009) observation that most firms report specific material weaknesses and do not classify by COSO component. Given this lack of adoption of high-level control framework terminology in auditors’ SOX 404 reports, we categorized synonyms and related IT weakness indicator keywords/phrases into 14 categories, trying to maximize the number of categories while ensuring identification of enough reports in each category to permit subsequent statistical analyses. The 14 categories, their keywords and the search logic are detailed in Table 2. The dictionary was reviewed by practitioners (Big 4 IT specialist partners) in the field of enterprise risk management, IT governance, and control assurance. We further validated the dictionary and search criteria by reading and manually coding a sample of SOX 404 reports (illustrated in Figure 2) to assess the accuracy of the ‘dictionary’ and the Boolean logic used in IT control weakness identification. The Type 1 and Type 2 errors committed using our automated search identification of IT weaknesses are summarized in the Data sources section.

Cross-tabulations, chi-square tests, and *t*-tests of significance were used to investigate the RQs. First we identified combinations of IT control weaknesses by testing the associations amongst the individual IT control weaknesses found using the automated search (RQ1). Next, we tested the association of these individual IT control weaknesses with the 20 non-IT internal control weaknesses listed by *Audit Analytics* in Figure 1 with which SOX 404 auditors’ reports in the *Audit Analytics* database are tagged (RQ2) and with the 26 financial misstatements coded by *Audit Analytics* (RQ3). Using cross-tabulations, chi-square tests, binomial tests of proportions and *t*-tests

¹⁵ Additional content analysis using frequency reports finds references to COSO components, other than monitoring, in sentences containing an IT indicator word/phrase are relatively infrequent: specifically (i) risk assessment (13 reports), (ii) control environment (50), (iii) information and communication (5), (iv) and control activities (14). The four COBIT 4.1 domains (“plan and organize”, “acquire and implement”, “deliver and support” and “monitor and evaluate”) are not referenced. The phrase “general controls” (and synonymous phrases “general computer controls” and “general computing controls”) was used in less than 15% (53) of the reports and in all but two of these 53 reports other IT weakness identifiers were also identified. The phrase “application control(s)” was used in less than 5% (18) of the reports.

we investigated RQ4, the association between the presence of IT control weaknesses and time (year of report: 2004-08), industry (SIC Codes), company size (Total Assets), auditor type (Big 4 vs. Other), and overall internal control quality (number of IT and non-IT weaknesses reported). To investigate RQ5, we defined control weakness persistence as weaknesses that were reported in two successive years. We then compared the mean counts of both IT and non-IT control weaknesses that persisted against those that did not persist and compared the ratio of persistent to total weaknesses for IT and non-IT weaknesses using a binomial test of proportions.

5. Data Sources

We used *Audit Analytics*, to identify 1,959 auditors' SOX 404 reports of internal control weaknesses for fiscal 2004-08. Based on 21 internal control weakness classifications (Figure 1)¹⁶, *Audit Analytics*' coded 429 of these reports as reporting both IT and non-IT weaknesses, only two reports¹⁷ (one in 2004 and one in 2005) as reporting only IT control weaknesses and 1,528 reports as reporting only non-IT weaknesses. Instead of accepting the coding of IT weaknesses as given by *Audit Analytics* we used automated searches to identify specific IT control weaknesses. We searched 441 reports in total - the 431 reports that *Audit Analytics* identified as reporting IT weaknesses plus 10 reports coded by *Audit Analytics* as reporting only non-IT weaknesses that were identified by searching the Lexis-Nexis database using several IT-related keywords (Boritz and Lim 2008). Our automated search identified one or more specific IT weaknesses in 380 of these 441 reports, the final population of reports with IT weaknesses used in our data analyses. - The initial selection of 441 reports included 51 reports which *Audit Analytics* coded as having an IT control weakness based on *management's* SOX 404 report. We restricted our study to the

¹⁶ Searches in *Audit Analytics* are date dependent, since the database is continuously being updated. We extracted the data for 2,062 auditors' SOX reports for this study on November 2, 2009 and eliminated 29 SOX 404 auditor's reports for companies reporting for fiscal 2009 and 74 reports for which amended reports for 2004-08 were included in the extraction.

¹⁷ Pegasus Communications Corp. (December 31, 2004) and Quixote Corp. (June 30, 2005).

auditors' SOX reports. Thus, the number of companies identified by our automated searches as having IT weaknesses could not be expected to match the count of those companies that were tagged by *Audit Analytics* as having information technology (software, security, access) issues based on managements' reports. The automated search successfully identified 97% of the 390 reports in which we expected to find IT weaknesses¹⁸. Figure 2 is an illustrative example of a SOX 404 auditor's report with IT weaknesses identified. Further, for the influencing factors (i.e., time, industry, company size, auditor type), we obtained fiscal year end information, four digit industry SIC codes, total assets¹⁹, and auditor type from *Audit Analytics*.

We performed additional procedures to gauge the success of our automated search in identifying auditors' reports with IT weaknesses and the extent of Type 1 and Type 2 errors committed by our automated identification of specific weaknesses. To gauge the extent of type 1 and type 2 errors committed in identifying the 14 specific weaknesses searched for with content analysis software we manually coded a random sample of 30 reports with one or more IT weaknesses and compared the manual coding to our automated search. The automated search correctly identified the presence or absence of IT control weaknesses in 87.14 percent of the 14 weaknesses in the 30 companies (420 total possible weakness instances). The automated search failed to identify 12 of the 73 IT weaknesses coded manually and falsely identified 42 weaknesses that had not been coded manually.²⁰ As an additional procedure to gauge the extent of type 1

¹⁸ An automated search of these 51 management reports was 95% successful in identifying IT weaknesses in managements' descriptions of weaknesses or recommendations for remediation involving changes to systems and software. While *Audit Analytics*' SOX 404 reporting documentation does not address using management report weakness descriptions when coding auditors reports, the Section 302 documentation explicitly states that software remediation evidences IT weaknesses.

¹⁹ We obtained asset value information that was missing from *Audit Analytics* from Compustat and EDGAR.

²⁰ We used two versions of our search logic, 'less' and 'more' restrictive, to identify IT weaknesses. To simplify presentation of findings, we consistently report descriptive statistics and results for only the less restrictive search which identified more weaknesses. The less restrictive search did not search for nearby non-IT context indicating words. The more restrictive search

errors committed by our automated weakness identification, we also ran an automated search for a sample of 30 companies that *Audit Analytics* did not tag as having IT weaknesses. The automated search falsely identified three companies as having IT weaknesses.²¹ However, the search also found one company²² which reported “issues in implementing the company’s new tax accounting system” that we would classify as an IT weakness but *Audit Analytics* did not. Automated search compares favourably with the 0.79 interrater reliability (0.73 for an independent third party) for agreement of experts’ ITW coding reported by Klamm and Watson (2009), the only study that we are aware of that reports inter-rater reliability of manual ITW coding.

6. Results

Table 1 summarizes the number of non-IT weaknesses and IT weaknesses identified by automated searches by year for companies with or without IT weaknesses. We performed an analysis of these two subpopulations of companies (untabulated) and found that seven of the 20 non-IT internal control weaknesses coded by *Audit Analytics* did not differ across the two subpopulations or did not have sufficient frequencies to permit meaningful statistical analyses, eleven were proportionately more frequent and two were proportionately less frequent in companies with IT weaknesses. Summary statistics for the 20 non-IT control weaknesses are based on *Audit Analytics*

logic checked for ‘exclusion’ words/phrases (i.e., tax, GAAP and other ‘exclusion’ words/phrases listed in Table 2 indicating a non-IT context) within the sentence and within 40 words (as determined by the content analysis software, QDA WordStat) of the possible IT weaknesses and, if found, did not count the IT weaknesses. In the sample of 30 companies used to check weakness identification accuracy, the less restrictive criteria identified more IT weaknesses than the more restrictive criteria (61 vs. 51 of the 73 IT weaknesses actually reported). However, the less restrictive search also falsely identified more weaknesses (42 vs. 20). The more restrictive search criteria correctly identified the presence or absence of IT control weaknesses in 90.00% of 14 weakness categories in the 30 companies (420 total possible weakness instances). For the total population of reports coded as having IT weaknesses, the more restrictive search identified 338 of the 390 reports (86.67%) as reporting IT weaknesses.

²¹ In one case, the misidentification was triggered by the word “software” in the company name. In another case, accounting for “software license revenue” was the trigger and in the third, “reporting process” was the trigger.

²² Alderwoods Group Inc. for the year ended January 1, 2005.

coding and summary statistics for the IT-weaknesses are based on the weaknesses identified in the 380 reports in which IT weaknesses were identified by our automated search.

Over the 2004-08 time period, companies without IT weaknesses averaged 3-4 non-IT weaknesses each, significantly fewer ($p < 0.001$) than companies with IT weaknesses which averaged 4-5 non-IT weaknesses plus 3-4 IT weaknesses each (panel A, Table 1). This is consistent with the observations of other researchers based on studies of early SOX data that companies with IT weaknesses have significantly weaker internal controls than other companies.

The pattern of changes in the average number of reported IT and non-IT weaknesses over the study period is not the same for companies with and without IT weaknesses. For the 1,579 reports for companies without IT weaknesses, the average number of reported weaknesses per year did not change significantly over the five years examined. However, in the 380 reports with IT weaknesses, both the average number of IT and non-IT weaknesses decreased between 2004 and 2008 ($p < 0.01$). Auditors reported an average of 4.26 IT weaknesses and 5.22 non-IT weaknesses (99 companies) in each report in 2004 and 2.32 IT weaknesses and 3.95 non-IT weaknesses (44 companies) in 2008. Between consecutive years, the average number of IT weaknesses in reports of Big 4 auditors was significantly less ($p < 0.01$) for 2007 than for 2006 and for companies audited by other auditors was significantly less for 2008 than 2007. Descriptive statistics for SOX 404 reports of Big 4 audits and other audits for 2004-06 and for 2007-08 are summarized in Table 1 panel B.²³ Big 4 auditors reported a higher average number of IT weaknesses (4.57) than other auditors (3.74) in 2004-06. Big 4 auditors reported fewer (2.29) IT weaknesses on average than other auditors (3.27) in 2007-08. Overall, the 269 companies with IT weaknesses with fiscal year

²³ We split the reporting into these two time periods based on the expectation that most auditors would opt for the more efficient top-down audit approach of Auditing Standard No. 5 and adopt the standard as soon as permitted. Adoption before the November 15, 2007 effective date was permitted after the SEC approved the Auditing Standard change on July 25, 2007. Only 15 (52) of the 67 (289) reports for 2007 in which both IT and non-IT (non-IT only) weaknesses were reported were for companies with year-ends prior to July 24th. Over 60 percent of the companies reporting weaknesses in 2007 had December 31st year-ends.

ends in 2004-06 had significantly more ($p < 0.001$) IT and non-IT weaknesses than the 111 companies with fiscal year ends in 2007-08.²⁴

Insert Table 1

Table 2 details the number of companies reporting 14 different IT weaknesses and the percentage of total IT weaknesses accounted for by each type. A SOX 404 report is counted as having an IT weakness when keywords/phrases listed in Table 2 associated with the weakness occur in the same sentence as “IT indicator” words. For example, an IT segregation weakness would be identified if “incompatible duties” occurred in the same sentence as “IT personnel”.²⁵

In decreasing order of frequency of reporting (Table 2), the 14 IT weaknesses identified by the automated searches are monitoring (66% of companies reporting IT weaknesses), access (53%), change and development (50%), design issues (42%), segregation (34%), end-user computing (31%), policies (27%), documentation (22%), staffing and competency (18%), masterfiles (11%), backup (9%), operations (7%), outsourcing (6%), and security - other than access (3%).

²⁴ A similar significant difference in the average number of IT and non-IT weakness is observed (not tabulated) when the average number of IT and non-IT weaknesses is compared for the 288 reports before and the 92 reports after the effective date of Auditing Standard No. 5, November 15, 2007.

²⁵ The keywords/phrases associated with end user computing, masterfile and outsourcing weaknesses are IT-specific enough that another IT indicator in the sentence is not required. Another, more restrictive, version of the search logic used in robustness checks, also searches for ‘exclusion’ words/phrases (i.e., tax, GAAP and other ‘exclusion’ words/phrases listed in Table 2 indicating a non-IT context) within the sentence and within 40 words of the possible IT weaknesses (as determined by the content analysis software, QDA WordStat) and does not count the IT weakness if such ‘exclusion’ words/phrases are found. Table 2 presents the keywords and search criteria used in both the less restrictive version of the automated searches and reported in the results section and tables, and the more restrictive version used for robustness checks and reported only in footnotes.

Consistent with a lower average number of IT weaknesses in 2007-08 than 2004-06, the frequencies of all types of IT weaknesses were lower in 2007-08 than in 2004-06. Details of IT weaknesses frequencies for both the 2004–06 and 2007-08 time periods are included in Table 4. For IT weaknesses for which counts are sufficient for binomial tests of proportions, test results (not tabulated $p < 0.05$) indicate Big 4 auditors (other auditors) identified proportionately more (fewer) IT weaknesses for companies with fiscal year ends before PCAOB Auditing Standard No. 5 became effective. While the frequency of IT weaknesses reported by Big 4 and other auditors differed, the relative ordering differed little (weakness counts greater than 10) from 2004-08²⁶.

Insert Table 2

We calculated pairwise associations between each IT weakness and other IT weaknesses in Table 3. As the results of Table 3 show, the pairwise associations between IT weaknesses indicate that they are co-reported frequently. Over 54 percent of the possible pairwise associations (39 of 71) between cells with expected cell counts that are large enough to permit statistical inference, and over 42 percent of all possible associations (39 of 91), are significant at $p < 0.05$ ²⁷. Six of the IT weaknesses (monitoring, access, changes, design, segregation, and policies) are associated significantly ($p < 0.05$) with more than half of the other 13 IT weaknesses. After 2006, consistent with a lower average number of IT weaknesses in 2007-08 than 2004-06, there were less than half as many significant pairwise associations (7 of 28 or 25%) between cells with expected cell counts that are large enough to permit statistical inference (not tabulated).

²⁶ The most notable difference is that Big 4 firms reported monitoring weaknesses in at least 15% more reports than access weaknesses in all years whereas other auditors reported proportionately more access weaknesses than monitoring weaknesses in 2005, 2006 and 2008.

²⁷ Proximity measures obtained with content analysis software analysis tools confirmed that IT weaknesses are highly clustered.

Insert Table 3

The pattern observed in Table 3 is quite different from the pattern observed in Table 4 for the pairwise associations between IT and non-IT weaknesses. In 2004-06 (panel A) almost 30 percent of the associations between cells with counts that are sufficient for chi-square tests of significance (45 of 156) and almost 16 percent of all possible associations (45 of 280), are significant at $p < 0.05$. In 2007-08 (panel B) less than 17 percent of the associations between cells with counts that are sufficient for chi-square tests of significance (9 of 53) and less than three percent of all possible associations (9 of 280), are significant at $p < 0.05$ ²⁸.

We calculated pairwise associations between each IT weakness and the non-IT weaknesses in Table 4 for 15 of the 20 non-IT control weaknesses.²⁹ A binomial test of proportions indicates that the panels are significantly different ($p < .001$).³⁰ For 2004-06 (panel A), the number of non-IT control weaknesses with which IT control weaknesses were significantly associated ($p < 0.05$) in decreasing order of the number of significant associations are: Monitoring (associated with 7 non-IT weaknesses), Design (7), End-user computing (6), Masterfiles (4), Policies (4), Outsourcing (4), Changes and Development (3), Documentation (3), Access (2), Operations (2), Segregation (1), Staffing & Competency (1), and Backup (1). It is also noteworthy that the most frequent associations are not simply those between the most frequently occurring IT

²⁸ We searched the 2007-08 SOX 404 management reports of IT weak companies using the same keywords and search criteria as used to identify IT weaknesses in the auditors' reports and found significant pairwise associations between IT and non-IT weaknesses reported in the management reports for 21% of the associations between cells with count that are sufficient for chi-square tests of significance (16 of 76).

²⁹ The following five of the 20 non-IT weaknesses coded in Audit Analytics had too few items in all cells for a meaningful statistic to be calculated; IC5 Remediation of material weakness identified; IC14 SEC or other regulatory investigations and/or inquiries; IC16 Inadequate disclosure controls (timely, accuracy, complete); IC19 Ineffective regulatory compliance issues; IC21 SAB 108 adjustments noted.

³⁰ Additional tests of differences between all pairs of years indicate that this difference is due to significant differences ($p < .05$) between 2004 and 2007 and 2008; between 2005 and 2007 and 2008, and between 2006 and 2008. We also found a significant difference between 2004 and 2006.

and non-IT weaknesses. For example, the most frequent non-IT weakness is IC1 with four significant associations ($p < 0.05$) with IT weaknesses, whereas IC6 which ranks fifth in frequency of occurrence has eight significant associations ($p < 0.05$) with IT weaknesses. It is noteworthy that associations between IT access and segregation of duties weaknesses and non-IT control weaknesses were comparatively few and isolated, despite the high frequency with which they were reported.

There were one-fifth as many significant ($p < 0.05$) associations between IT weakness and non-IT weaknesses in 2007-08 (9, panel B) as in years 2004-06 (45, panel A). Seven of the 12 non-IT weaknesses significantly associated with one or more IT weaknesses in 2004-06 continued to be significantly associated with IT weaknesses in 2007-08. IC4 Journal entry control issues, IC6 Untimely or inadequate account reconciliations, and IC11 Segregation of Duties accounted for 66.67 percent (6 of 9) significant associations in 2007-08 and 37.78 percent (17 of 45) in 2004-06. IC8 Material and /or numerous auditor/year-end adjustments which was associated with 6 IT weaknesses in 2004-06 was not significantly associated with any IT weakness in 2007-08.

In 2004-2006 (panel A), staffing and competency, documentation, and policies IT weaknesses, that are likely to be pervasive IT weaknesses that apply company-wide to all applications, were significantly associated with fewer non-IT weaknesses (three or less) than monitoring, design, and end-user computing IT weaknesses (six or more) that are less likely to affect all applications in the same way.

For companies with IT weaknesses, two combinations of IT and non-IT weaknesses are evident in both 2004-06 (panel A) and 2007-08 (panel B): IT access and segregation weaknesses with IC11 Segregation ($p < 0.01$) and IT monitoring and design with IC4 Journal entry control issues ($p < 0.05$). The second combination is a remnant of a larger combination observed only in 2004-06 (panel A): the three IT weaknesses (monitoring, design issues, and end-user computing) associations ($p < 0.05$) with four non-IT weaknesses (IC2 Personnel resources,

competency/training, IC8 Material and/or numerous auditor/year-end adjustments, IC6 untimely or inadequate account reconciliations, and IC4 Journal entry control issues in 2004-06³¹.

Insert Table 4

We also calculated the pairwise associations between the 14 IT control weaknesses and the 26 accounts that *Audit Analytics* uses to code financial reporting misstatements. Our objective was to see whether IT weaknesses were associated with particular accounting rule application failures. Panel A of Table 5 lists the IT weaknesses and the accounts in decreasing order of frequency of occurrence, respectively for 2004-06. Panel B of Table 5 presents the pairwise associations for 2007-08 in the same order as that used in panel A. A binomial test of proportions indicates that the panels are significantly different ($p < .001$).³² We see that the IT weaknesses are associated with a broad range of accounting issues in 2004-06 and few issues in 2007-08. Access control weaknesses, while reported frequently, do not appear to affect accounts as pervasively as would be expected from their theoretical characteristics.

Insert Table 5

Table 6 summarizes our tests of key influencing factors. The result shows the ranges of the average number of IT weaknesses (1 - 5) and the average number of non-IT weaknesses (2 - 6) at the overall company level are similar. However, we find some significant differences between

³¹ In supplementary analysis, we repeated chi-square tests of association between non-IT and IT weaknesses, using a more restrictive version of the search logic to identify the IT weaknesses. The more restrictive search logic did not count certain IT weaknesses found within forty words (as determined by QDA WordStat content analysis software) of an 'exclusion' words/phrases (e.g., tax and GAAP). The supplementary analysis supports our identification of critical combinations.

³² Additional tests of differences between all pairs of years support this finding. The only significant pairwise differences between years occur between the two panels.

the average number of IT and non-IT weaknesses depending on year of report (2004-08), industry (SIC Codes), company size (Total Assets), auditor type (Big 4 vs. Other), and internal control quality (number of weaknesses reported).

The downward trend observed in the average number of IT weaknesses from 2004 to 2008 (Table 1) was significant between 2006 and 2007 ($p < 0.05$).

The results of Table 6 show industry³³ differences in the average number of weaknesses. Some of these industry differences were significant. For example the average number of IT weaknesses reported by banks ($M = 3.16$; $SD = 2.10$) was one of the lowest and differed significantly ($p < 0.05$) from three of the other fifteen industries (not tabulated). Companies in the Industrial equipment sector had the largest number of IT weaknesses whereas companies in Miscellaneous equipment had the lowest number. In contrast, companies in the Services sector had the largest number of non-IT weaknesses whereas companies in the Transportation sector had the lowest number.

In addition, we found larger companies³⁴ had significantly more design weaknesses ($p < 0.05$ not tabulated) than smaller companies, but we found no difference in the overall average number of IT weaknesses per company. However, larger companies had significantly more ($p < 0.01$) non-IT weaknesses. The results also indicate that companies with IT weaknesses audited by Big 4 audit firms reported more IT-weaknesses than companies audited by non-Big 4 firms in both the 2004-06 ($p < 0.05$) and 2007-08 ($p < 0.01$) time periods and more non-IT weaknesses in the 2004-06 ($p < 0.001$). The average number of non-IT weaknesses did not differ with auditor type ($p > 0.1$) in the 2007-08 time period.

³³ We classified companies into 16 industries using the four-digit SIC codes (Doyle et al. 2007a).

³⁴ Using a median split based on total assets of companies both with and without IT weaknesses, we classified the companies with internal control weaknesses into larger and smaller companies: 58% of the companies with IT weaknesses were smaller and 42% were larger.

Overall, we found the quality of non-IT internal control was associated with the quality of IT control: ³⁵ companies that reported more non-IT control weaknesses also reported more IT control weaknesses ($p < 0.01$) and companies that reported more IT control weaknesses also reported more non-IT control weaknesses ($p < 0.01$).

Insert Table 6

Table 7 analyses persistence of IT and non-IT weaknesses which we defined as weaknesses that still remain unremediated in the year after being reported, a measure designed to permit study at the specific weakness level. This is somewhat different from Goh (2009) who measured persistence at the company level from the occurrence of at least one material weakness to the issuance of the first clean internal control opinion. The data in Table 7, panel C indicate that over the entire period analyzed, 24.36 percent of IT weaknesses took more than one year to remediate. This persistence affected 91 (27.00%) of the 336 companies in our test population of reports for which next year data is available to determine persistence. Most of the 14 listed IT weaknesses fall into a one quarter - three quarter proportion of unremediated/remediated over the time period considered; however, monitoring, access, design, and end-user computing weaknesses, the four weaknesses that exceed this three-quarter proportion (untabulated) are identified as IT-weaknesses that co-occur with non-IT weaknesses (Table 4).

The average number of weaknesses shown in panel A of Table 7 show that there are significantly more ($p < 0.05$) IT (non-IT) weaknesses in companies with one or more unremediated IT weaknesses in all years (2004) for which persistence can be measured (2009 data was not

³⁵ We split companies into groups based on the number of control weaknesses they reported. We classified companies where those with the stronger non-IT control quality had less than the median number (3) non-IT weaknesses and those with the stronger IT control quality had less than the median number (4) IT weaknesses.

available to determine persistence of weaknesses reported in 2008). However, a binomial test of proportions comparing the proportion of *persistent* IT weaknesses to all IT weaknesses to the proportion of *persistent* non-IT weaknesses to all non-IT weaknesses found no significant difference.

Insert Table 7

7. Discussion

Using the results of automated searches, we examined the associations between IT control weaknesses reported in the SOX 404 reports from 2004-08 and a number of factors of interest as described in our research questions. We add to the research on the associations of IT weaknesses with non-IT and financial reporting weaknesses (Klamm and Watson, 2009) by identifying sub-categories of IT weaknesses that may predict non-IT related weaknesses and accounting rule application failures. We identified sub-categories of IT weaknesses at a level of detail below that of the groupings commonly used in professional standards and other guidance such as the COSO framework. For example, our tests considered access, master file, and end-user computing weaknesses as separate weaknesses when these might all be studied as a single group (control activities) under a COSO grouping or as two groups (access controls and application controls) under another framework.

A question for future research consideration is the extent to which negotiations between management and auditors determine the reporting of the weaknesses listed in Table 1. Client-auditor confidentiality and other time-demands of audit partners and Audit Committee members involved in such negotiations limits researchers' study of this process. Another question raised by our findings is how it is possible for risk assessment controls over information technology to be comparatively strong in companies reporting numerous IT weaknesses and when risk assessment

is one of the five components of the COSO framework - the framework that is most frequently used to assess the effectiveness of controls. Further investigation of this issue is warranted.

We found that reported IT weaknesses are co-reported with other IT weaknesses and that co-reporting of IT with non-IT weaknesses is less pronounced than co-reporting within the IT category. However, we observed several significant associations that could be considered critical combinations of weaknesses. One such critical combination found in 2004-06 reports, is the association between IT weaknesses in monitoring, design, and end-user computing with non-IT weaknesses in journal entry controls, untimely or inadequate account reconciliations, material and/or numerous auditor/ year-end adjustments, and accounting personnel resources, competency and training. This combination captures almost one quarter of the associations (12 of 45) found in that time period. It is still unclear whether improvements in controls over financial reporting, the changes in the Auditing Standards in 2007 or some other reason explains why this combination is not as frequent in reports of recent years. Another noteworthy combination is the association between IT access control weaknesses and IT segregation weaknesses and non-IT segregation weaknesses; the association between IT staffing and competency and non-IT accounting personnel issues. These critical combinations of material weaknesses may be caused by factors at a higher level than is evident from the reported weaknesses, and if this is the case, then the weaknesses could be even more significant. A useful extension of this study would be to determine whether the capital markets are sensitive to such combinations.

Contrary to the assumption implicit in studies that classify IT weaknesses as ‘company-wide’, not all of the 14 IT weaknesses shown in Table 2 are likely to be general control weaknesses or have pervasive effects on applications: some (e.g. end-user computing and design IT weaknesses identified with keywords such as “spreadsheets”, “manual intervention”, “interface”, “inadequate design”, “functional business requirement”, “incompatible application”, “inadequate recording and reporting”) are likely to affect applications differentially, whereas

others are more likely to affect all applications (change and development, policies, documentation, staffing sufficiency and competency, backup and operations IT weaknesses) or to be either application specific or pervasive, depending on the circumstances (monitoring, access, segregation, outsourcing, security IT weaknesses). Our analysis of the association between IT weaknesses and financial reporting weaknesses indicated that some control weaknesses that would be expected to have pervasive effects do not have those effects, and that the pervasiveness of effects depends on the time period. This observation suggests several possibilities that could be investigated, ranging from a re-examination of the effects of controls and control weaknesses on accounting systems to an investigation of the process used to determine which weaknesses are reported when errors in accounts are identified and how the weaknesses that are candidates for being reported relate to the weaknesses that are ultimately reported.

In summary, for IT weaknesses we identified the following significant findings that may be relevant to future IT control studies:

- There is an overall downward trend in the number of IT weaknesses reported between 2004 and 2008, with a particularly significant change between 2006 and 2007, around the time auditing standards changed. This finding suggests that caution should be used when generalizing results of early SOX 404 studies to the present day.
- Big 4 auditors (other auditors) identified proportionately more (fewer) IT weaknesses and more non-IT weaknesses for companies with fiscal year ends before 2007, the year in which PCAOB Auditing Standard No. 5 became effective.
- The industries with the highest/lowest average number of IT weaknesses were not those with the highest/lowest average number of non-IT weaknesses. However, the companies with the highest average number of IT weaknesses were those with the highest number of non-IT weaknesses.

- For companies with IT weaknesses, larger companies had more (fewer) non-IT (IT) weaknesses than smaller companies.
- Larger companies had more design weaknesses but fewer change and development weaknesses than smaller companies.

During the five-year period (2004-08) we did not find evidence of differential internal control weakness persistence between IT and non-IT control weaknesses. This finding is consistent with the finding that frequently occurring IT and non-IT weaknesses co-occur. This issue merits further investigation of whether or not more pervasive IT weaknesses are comparatively more persistent than application-specific IT weaknesses and non-IT weaknesses.

8. Limitations and Concluding Remarks

We acknowledge certain limitations of our analyses. The first limitation of our analysis is the obverse side of a strength that we cited in the introduction: the weaknesses that we analyse are only the weaknesses that were reported by the entity's auditor as a result of a negotiation process with management that is thought to act as a screen that ensures that only the most severe weaknesses are reported³⁶. Therefore, the picture of financial reporting systems that these

³⁶ At the suggestion of an anonymous reviewer, we compared the number of weaknesses reported by dismissed/resigning auditors to the number of weaknesses reported by auditors continuing in the following year to see if weakness reporting is affected by the negotiation process: auditors' will likely be in a stronger negotiating position if they know they are not continuing. Based on a comparison of SOX 404 reporting dates and the departing/engaged auditor dates in the *Audit Analytics* database, we determined that 51 auditors who likely knew they were dismissed/resigning at the time of reporting, reported more ($p < 0.05$) IT weaknesses ($M=4.43$ $SD=2.48$) than continuing auditors ($M=3.68$ $SD=2.22$) lending support to the argument that the weaknesses reported are screened by the negotiation process. The number of non-IT weaknesses reported by dismissed/resigning ($M=5.02$ $SD=1.86$) auditors vs continuing auditors ($M=4.80$ $SD=2.41$) was not significantly different.

³⁸ With a less restrictive search we find segregation and access IT weakness (correctly) within the same sentence as an IT indicator ('IT applications' and 'data') but also incorrectly identify two weaknesses not related to IT: staffing (keywords: insufficient personnel) and monitoring (keyword: review). With a more restrictive search no IT weaknesses are found, because the sentence in which the IT weakness is described is excluded as it has not only an IT indicator, but

weaknesses portray may not be complete. Thus, a useful extension of this study would be to examine control deficiencies that were not considered significant enough to constitute material weaknesses. A second limitation is that the automated search is not perfect, resulting in both Type 1 and Type 2 errors in the data upon which our analyses are based. Although the automated search has the advantage of being transparent, replicable, and scalable, this research could be extended by supplementing the automated search with manual review. Just as subjectivity is involved in automated searches (choice of keywords, categorization and search criteria), a manual review would, of course, involve subjectivity in the identification and characterization of IT weaknesses, due to differences in authoritative guidance in this area. Another limitation of our analyses is due to our focus on a small number of factors to explain the frequency of reported internal control weaknesses such as time, industry, firm size, and type of auditor. Other explanatory factors such as IT intensity of the firm, the firm's state of IT governance, and reliance on IT experts could play a critical role in determining the co-occurrence of IT weaknesses and non-IT weaknesses. Examining such additional factors might be a fruitful research endeavour in the future. Last, our definition of weakness persistence only includes control weaknesses that recur in subsequent and successive years, and omits weaknesses that are remediated but are replaced by new weaknesses in the subsequent year.

Keeping in mind these limitations, we believe that our study makes the following contributions to academe and practice.

- We find evidence that SOX 404 auditor reported IT weaknesses have differential effects on non-IT weaknesses and financial misstatements: not all SOX 404 auditor reported IT weaknesses are general control weaknesses that have entity-wide pervasive effects. This

also a non-IT indicator (generally accepted accounting principles) within 40 words (as determined by the content analysis software, QDA Miner).

finding may have implications for the robustness of findings of research studies that classify all SOX reported IT weaknesses as company-wide.

- We demonstrate the efficacy of using automated text analysis procedures to search SOX404 reports and possibly other narrative control disclosures to identify control deficiencies and weaknesses. This may facilitate further study of internal controls in the U.S. and other jurisdictions.
- The sub-division of the single code for IT weaknesses in *Audit Analytics* into 14 sub-codes based on our content analysis can help researchers hampered by the lacking granularity of the coding of IT weaknesses in *Audit Analytics*.
- The “dictionary” of words/phrases that we created in this study to identify and categorize reported IT weaknesses may assist management and auditors in the reporting of future IT weaknesses.
- In our analysis we observed that in recent years the reporting of weaknesses seems to be potentially less informative compared to the early years of SOX 404 reporting. Thus, it is becoming more difficult to identify which types of weaknesses have occurred. Standard setters and regulators should investigate this pattern to determine whether the value of SOX 404 reporting is being undermined. They should consider whether a dictionary such as ours may help reverse this trend if managers and auditors use it to name internal control weaknesses in SOX 404 reports.
- The identification of a small number of frequently-occurring combinations of IT control weaknesses and non-IT control weaknesses may lead to the further development and testing of hypotheses concerning the differential effects of various control weakness combinations on financial performance. In this paper, we have identified how IT control weaknesses are associated with various accounts and the number of financial reporting

weaknesses. However, a more extensive analysis would be required to focus on how the co-occurrence of IT and non-IT weaknesses are associated with various accounts.

- The identification of frequently occurring combinations of control weaknesses may provide managers, auditors, standard setters and regulators with relevant information about internal control issues to inform their respective policy considerations. For example, IT weaknesses that co-occur with non-IT weaknesses may indicate that common factors cause both sets of weaknesses. Effective remedial action may need to be aimed at the common factors rather than the individual weaknesses. Weaknesses that are not remediated swiftly may indicate problems with organizational structure, limitations in human and financial resources allocated to internal control or incentives that are not aligned with maintaining effective internal control that should be investigated. Anomalies in patterns of weaknesses may also indicate problems in the way weaknesses are reported that require additional guidance to be provided by standard setters and regulators to managers and auditors.

As we noted earlier, companies with IT weaknesses have significantly weaker IT and non-IT internal controls than other companies. In addition, companies with IT weaknesses have a different distribution of non-IT weaknesses than companies without IT weaknesses. The internal control weaknesses reported by companies with IT weaknesses may be related to company-specific factors such as the quality of management and governance and these merit further investigation.

References

- Ashbaugh-Skaife, H., D. Collins, W. Kinney, and R. LaFond. 2009. The effect of SOX internal control deficiencies on firm risk and cost of equity. *Journal of Accounting Research* 47(1): 1-43.
- Beneish, D., M. Billings, and L. Hodder. 2008. Internal control weaknesses and information uncertainty. *The Accounting Review* 83 (3): 665-703.
- Boritz, E., and J.H. Lim. 2008. IT control weaknesses, IT governance and firm performance. Working paper, University of Waterloo.
- Canada, J., Sutton, S.G., Kuhn, J.R. Jr. 2009. The pervasive nature of IT controls: An examination of material weaknesses in IT controls and audit fees. *International Journal of Accounting and Information Management*, 17(1): 106 – 119.
- Canadian Institute of Chartered Accountants (CICA). 1998. *IT Control Guidelines*. Toronto: CICA.
- Cohen, D., E. Dey, and T. Lys. 2008. Real and accrual-based earnings management in the pre-and post-Sarbanes Oxley periods. *The Accounting Review* 83(3): 757–787.
- 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.

-----, 2007b. Accruals quality and internal control over financial reporting. *The Accounting Review* 82(5): 1141–1170.

Goh, B. W. 2009. Audit committees, boards of directors, and remediation of material weaknesses in internal control. *Contemporary Accounting Research* 26 (2): 549-579.

Gupta, P. and T. Leech, sponsored by the Financial Executives Research Foundation (FERF), the research affiliate of Financial Executives International (FEI). 2005. Control deficiency reporting: A review and analysis of filings during 2004. Available online at <http://www.financialexecutives.org>.

Hammersley, J.S., L.A. 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.

Hoitash, R., U. Hoitash, and J. Bedard. 2008. Internal controls quality and audit pricing under the Sarbanes-Oxley Act. *Auditing, A Journal of Practice and Theory* 27(1) 105-126.

Hunton, J. 2000. Discussant's Comments on Presentations by John Lainhart and Gerald Trites, *Journal of Information Systems*, 14(S-1): 33-36

ISACA. 2009. *CobiT® and Application Controls: A Management Guide*. Rolling Meadows, IL, USA: ISACA.

IT Governance Institute (ITGI). 2006. Appendix I sample deficiency evaluation decision tree. *IT control objectives for Sarbanes-Oxley: The role of IT in the design and implementation of internal control over financial reporting, 2nd Edition*. Rolling Meadows, IL. USA. ISACA.

-----, 2007. *COBIT® 4.1*. Rolling Meadows, IL. USA. Available online at <http://www.isaca.org> .

Jha, R., K. Kobelsky, and J.H. Lim. 2008. The impact of performance-based compensation on internal control. Working paper, Baylor University and University of Waterloo.

Klamm, B.K., and Weidenmier Watson, M. 2009. SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. *Journal of Information Systems* 23(2): 1-23.

Krishnan, J. 2005. Audit committee quality and internal control: An empirical analysis. *The Accounting Review* 80(2): 649–675.

Li, C., G. Peters, V.J. Richardson, and M. Weidenmier Watson. 2008. The consequences of poor data quality on decision making: The case of Sarbanes-Oxley information technology material weaknesses. Working Paper, University of Pittsburg.

Masli, A., V.J. Richardson, M. Weidenmier Watson, and R. Zmud. 2009. CEO, CFO & CIO engagement in information technology management: The disciplinary effects of Sarbanes-Oxley information technology material weaknesses. Working Paper, University of Arkansas.

Moody's. 2006. *The second year of section 404 reporting on internal control. Special Comment.*

New York: Moody's Investors Service, Global Credit Research.

Public Company Accounting Oversight Board (PCAOB). 2004. Auditing Standard No. 2 – An audit of internal control over financial reporting that is integrated with an audit of financial statements. Available online at <http://pcaobus.org>.

Public Company Accounting Oversight Board (PCAOB). 2007. Auditing Standard No. 5 – An audit of internal control over financial reporting that is integrated with an audit of financial statements. Available online at <http://pcaobus.org>.

Raghunandan K. and D. Rama. 2006. SOX Section 404 material weakness disclosures and audit fees. *Auditing: A Journal of Practice & Theory* 25(1): 99–114.

Securities and Exchange Commission (SEC). 2003. Final Rule: Management's report on internal control over financial reporting and certification of disclosure in Exchange Act periodic reports. Available online at <http://www.sec.gov/rules/final.shtml>.

Wolfe, C.J., E. G. Mauldin, and M. C. Chandler, 2009. Concede or deny: Do management persuasion tactics affect auditor evaluation of internal control deviations? *The Accounting Review* 84(6): 2013-2037.

Figure 1 Internal Control Material Weaknesses Identified by Audit Analytics

1. Accounting documentation, policy and/or procedures
2. Accounting personnel resources, competency/training
3. Ethical or compliance issues with personnel
4. Journal entry control issues
5. Remediation of material weakness identified
6. Untimely or inadequate account reconciliations
7. Management/Board/Audit Committee investigation(s)
8. Material and/or numerous auditor /year-end adjustments
9. Non-routine transaction control issues
10. Restatement or non-reliance of company filings
11. Segregations of duties/ design of controls (personnel)
12. Insufficient or non-existent internal audit function
13. Scope (disclaimer of opinion) or other limitations
14. SEC or other regulatory investigations and/or inquiries
15. Senior management competency, tone, reliability issues
16. Inadequate disclosure controls (timely, accuracy, complete)
17. Restatement of previous 404 disclosures
18. Ineffective or understaffed audit committee
19. Ineffective regulatory compliance issues
20. Information technology (software, security, access issues)
21. IC -SAB 108 adjustments noted

Figure 2 Illustrative SOX404 Auditor's Report^a*Report of Independent Registered Certified Public Accountants on Internal Controls
The Board of Directors and Shareholders of FindWhat.com, Inc.*

We have audited management's assessment, included in the accompanying Form 10-K/A, that FindWhat.com, Inc. (the Company) did not maintain effective internal control over financial reporting as of December 31, 2004, because of the effect of material weaknesses identified in management's assessment related to (i) purchase accounting, (ii) goodwill impairment, (iii) revenue recognition for private label agreements and other revenue agreements, excluding those related to FindWhat.com Network revenue (iv) personnel resources and technical accounting expertise, (v) quarterly and year-end financial statement close and review process, and (vi) segregation of duties, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (the COSO criteria). The Company's management is responsible for maintaining effective internal control over financial reporting and for its assessment of the effectiveness of internal control over financial reporting. Our responsibility is to express an opinion on management's assessment and an opinion on the effectiveness of the company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, evaluating management's assessment, testing and evaluating the design and operating effectiveness of internal control, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's 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.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

A material weakness is a control deficiency, or combination of control 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. The following material weaknesses have been identified and included in management's assessment: (i) insufficient controls over the determination and application of generally accepted accounting principles with respect to purchase accounting for certain 2004 acquisitions, (ii) insufficient controls over the determination and application of generally accepted accounting principles with respect to evaluating and measuring

impairment of goodwill, (iii) insufficient controls over the determination and application of generally accepted accounting principles with respect to revenue recognition for private label agreements and other revenue agreements, excluding those related to FindWhat.com Network revenue, (iv) insufficient personnel resources and technical accounting expertise within the accounting function to resolve non-routine or complex accounting matters, (v) insufficient controls over and review of the quarterly and year-end financial statement close and review process, and (vi) insufficient segregation of duties whereby financial accounting personnel had access to financial accounting IT applications and data and also performed incompatible duties with respect to the authorization, recording, and control activities. The first five of these material weaknesses affected several financial statement accounts, including accounts receivable and allowance for doubtful accounts, goodwill, deferred revenue, accrued expenses, stockholders' equity, revenues and various expense accounts. As a result of the first five identified material weaknesses, the Company recorded various adjustments to the consolidated financial statements as of December 31, 2004 and for the year then ended. The sixth material weakness affects all financial statement accounts, however we did not identify any adjustments to our financial statements as a result of this control weakness. These material weaknesses were considered in determining the nature, timing, and extent of audit tests applied in our audit of the December 31, 2004 consolidated financial statements, and this report does not affect our report dated March 16, 2005 on those financial statements.

As described in Management's Annual Report on Internal Control Over Financial Reporting, management's assessment of and conclusion on the effectiveness of internal control over financial reporting did not include the internal controls of Espotting Media, Inc., its wholly owned subsidiary that was acquired on July 1, 2004 and is included in the 2004 consolidated financial statements of the Company and constituted \$240.4 million and \$207.0 million of total and net assets, respectively, as of December 31, 2004 and \$57.3 million and \$3.4 million of revenues and net income, respectively, for the year then ended. Our audit of internal control over financial reporting of the Company also did not include an evaluation of the internal control over financial reporting of Espotting Media, Inc.

In our opinion, management's assessment that FindWhat.com, Inc. did not maintain effective internal control over financial reporting as of December 31, 2004, is fairly stated, in all material respects, based on the COSO control criteria. Also, in our opinion, because of the effect of the material weaknesses described above on the achievement of the objectives of the control criteria, FindWhat.com, Inc. has not maintained effective internal control over financial reporting as of December 31, 2004, based on the COSO control criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated balance sheets as of December 31, 2004 and 2003, and the related consolidated statements of operations, stockholders' equity, and cash flows for each of the two years in the period ended December 31, 2004 of FindWhat.com, Inc. and our report dated March 16, 2005 expressed an unqualified opinion thereon.

Ernst & Young LLP, Tampa, Florida, April 29, 2005

a. With a less restrictive search we find segregation and access IT weakness (correctly) within the same sentence as an IT indicator ('IT applications' and 'data') but also incorrectly identify two weaknesses not related to IT: staffing (keywords: insufficient personnel) and monitoring (keyword: review). With a more restrictive search no IT weaknesses are found, because the sentence in which the IT weakness is described is excluded as it has not only an IT indicator, but also a non-IT indicator (generally accepted accounting principles) within 40 words (as determined by the content analysis software, QDA Miner).

TABLE 1Summary statistics of SOX 404 auditors' reports with weaknesses^a reported 2004 – 2008**Panel A:** SOX 404 auditors' reports with weaknesses^a reported by all auditors 2004 – 2008

	2004		2005		2006		2007		2008		Total 2004 –08		
	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak	All Companies
Number of companies ^b	99	355	98	394	72	345	67	289	44	196	380	1579	1959
Non-IT Control Weaknesses:													
Number of non-IT Control Weaknesses: ^a	517	1206	524	1330	335	1150	285	1004	174	659	1835	5349	7184
Mean	5.22	3.40	5.35	3.38	4.65	3.33	4.25	3.47	3.95	3.36	4.83	3.39	3.67
Standard Deviation	2.75	1.45	2.18	1.50	2.12	1.53	1.99	1.62	2.06	1.30	2.33	1.49	1.78
Skewness	0.73	1.16	0.45	1.81	0.50	1.27	0.33	1.54	0.67	1.13	0.65	1.44	1.40
IT Control Weaknesses:													
Number of IT Control Weaknesses: ^b	422	n/a	420	n/a	285	n/a	207	n/a	102	n/a	1436	n/a	n/a
Mean	4.26	n/a	4.29	n/a	3.96	n/a	3.09	n/a	2.32	n/a	3.78	n/a	n/a
Standard Deviation	2.35	n/a	2.23	n/a	2.34	n/a	2.02	n/a	1.43	n/a	2.27	n/a	n/a
Skewness	0.45	n/a	0.61	n/a	0.61	n/a	0.91	n/a	1.32	n/a	0.69	n/a	n/a

TABLE 1 (Continued)

Panel B: SOX 404 auditors' reports with weaknesses^a reported by Big 4 and Other auditors 2004-06 and 2007-08

	Big4 Audits 04-06		Other Audits 04-06		All Audits 04-06		Big4 Audits 07-08		Other Audits 07-08		All Audits 07-08	
	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak	IT & non-IT weak	Non-IT only weak
Number of companies ^b	127	617	70	132	197	749	55	331	56	154	111	485
Non-IT Control Weaknesses:												
Number of non-IT Control Weaknesses: ^a	745	2,127	296	409	1,041	2,536	230	1,144	229	519	459	1,663
Mean	5.87	3.45	4.23	3.10	5.28	3.39	4.18	3.46	4.09	3.37	4.14	3.43
Standard Deviation	2.50	1.50	2.07	1.32	2.48	1.47	1.90	1.50	2.13	1.51	2.01	1.50
Skewness	0.69	1.63	0.22	0.70	0.63	1.51	0.59	1.55	0.38	1.32	0.45	1.47
IT Control Weaknesses:												
Number of IT Control Weaknesses: ^b	580	n/a	262	n/a	842	n/a	126	n/a	183	n/a	309	n/a
Mean	4.57	n/a	3.74	n/a	4.27	n/a	2.29	n/a	3.27	n/a	2.78	n/a
Standard Deviation	2.29	n/a	2.19	n/a	2.29	n/a	1.74	n/a	1.82	n/a	1.84	n/a
Skewness	0.31	n/a	0.97	n/a	0.52	n/a	1.68	n/a	0.85	n/a	1.13	n/a

a. Automated searches using keywords and search criteria described in Table 2 were used to identify IT weaknesses in the 2004-08 Auditors' SOX 404 reports coded in the *Audit Analytics* dataset as having one or more material weaknesses. The *Audit Analytics* database codes internal control weaknesses appearing in SOX 404 reports using 21 identifiers, one of which (IC20) signifies that there were information technology (IT) control weaknesses but does not specify their precise nature. This table reports summary statistics for the 20 non-IT control weaknesses as reported by *Audit Analytics* and the summary statistics for IT weaknesses as identified by the automated searches. The number of companies with IT and non-IT weaknesses identified by the automated searches differs from the count based on Audit Analytics IC20 code.

b. Table 2 describes the keyword/phrases and search criteria used to identify companies with IT weaknesses.

TABLE 2

Summary statistics of keywords/phrases and search criteria used to analyze content of SOX 404 reports with IT weaknesses ^a reported in 2004-08

IT Control Weaknesses	Keyword(s) ^a	Number of companies ^b	% of companies	% of IT weaknesses
Monitoring	adherenc*; complianc*; dashboard*; enforce*; evaluat*; examin*; IT compliance; monitor*; oversight; review*; scrutiny; supervis*	249	66%	17%
Access	access; access control*; access privilege*access rights; logical access; password*; physical access; physical security; security access; system privile*; user access; user identification	203	53%	14%
Change and Development	acquisition; accuracy of calculate*; approval of chang*; approval of the change; authorization of chang*; billing error; change control; change management; changes to financial application*; changes to production application*; changes to program*; configuration of certain settings; conversion; data conversion; data migration; deactivat*; development; implement*; implementation of computer application*; maintenance; maintenance control*; migrat*; migrate changes to production; migration of system changes to production; placed into production; program changes; program error; program development; proper calculation; set-up; software chang*; system chan*; system* conversion*; system* development; test*; timely deactivation; track* chang*	191	50%	13%
Design Issues	accurate invoice*; assumption*used; audit trail*; complexit*; design*; disparate; do not appropriately address the requirements; functional business requirement*; functional complexity; inadequate design; inadequate recording and reporting; inadequate system*; incompatible application*; incompatible platform*; insufficient information systems; insufficient system*; interface*; lack of adequate resources; lack of effective information system*; large number of manual process*; legacy; life cycle; manual intensive; manual intervention; manual performanc*; manual process*; manual-intensive; non-integrated; reporting limitations; reporting requirement*; user dependence	159	42%	11%

TABLE 2 (Continued)

IT Control Weaknesses	Keyword(s) ^a	Number of companies ^b	% of companies	% of IT weaknesses
Segregation	incompatible duties; incompatible responsibilit*; segregate; segregation	130	34%	9%
End user computing	cell protection; end user comput*; end-user comput*; spreadsheet*	119	31%	8%
Policies	acceptable use policies; access policies; adequate policies; backup policies; company policies; deficiencies in the company's policies; develop and enforce policies; did not have policies; documentation policies; enforce policies; establishment and maintenance of policies; ineffective policies; information technology polic*; IT policies; IT strategic plan; lack of effective policies; lack of policies; polic*; policies and procedures; security polici*; strateg*	103	27%	7%
Documentation	*adequate document*; *sufficient* document*; document* and test*; document* or test*; documentation; effectively document*; lack of document*; not document*; properly document*; unable to document	82	22%	6%
Staffing and Competency	adequate staffing; competenc*; experienc*; inadequate IT staff; inadequate IT support staff; inadequate personnel; inadequate staff*; knowledg*; lack* of competenc*; limited number of personnel; personnel limitation*; skill*; *sufficient complement of personnel; *sufficient number of; *sufficient personnel; training	67	18%	5%
Masterfiles	customer database; datafile*; employee database; master data; master data file*; master file*; master record*; masterfile; masterfile*; payroll changes; payroll data*; price table*; standing data; vendor database; vendor listing; vendor master file*	40	11%	3%
Backup	backup*; back-up*; backup media; back-up media; disaster; offsite; off-site; record* retention; record* storage; remote location; removable media; rotation media; uninterruptible power	34	9%	2%

TABLE 2 (Continued)

IT Control Weaknesses	Keyword(s) ^a	Number of companies ^b	% of companies	% of IT weaknesses
Operations	computer operation*; information systems operation*; IT operation*; operating procedure*; operations report*; proper operation*; software licens*; support operation*	25	7%	2%
Outsourcing	data center*; outsour*; SAS 70; service organization*; service provider*; Statement of Auditing Standards No. 70; third party organization; third party service organization; third-party organization; third-party service	23	6%	2%
Security (other than access)	anti-virus; electronic transmission; encrypt*; fire; firewall; information security; network vulnerability assessment*; security breach; vulnerability	11	3%	1%
Total number of companies with IT weaknesses		380		100%
Total of detailed IT control weaknesses identified using QDA Miner content analysis software		1,436		

a. Keywords/phrases were identified using content analysis software frequency and keyword-in-context reporting features in QDA WordStat from Provalis Research©.

b. A company is counted as having an end user computing, masterfile, and outsourcing IT weaknesses when any keyword/phrases listed in the table associated with these weaknesses occur anywhere in the company's SOX 404 audit report. A company is counted as having the other IT weaknesses when keyword/phrases listed in the table associated with these weaknesses occur in the same sentence as an "IT indicator" ^c. In supplemental analysis conducted using more restrictive criteria as a robustness check, IT weaknesses (except end user computing, masterfile, and outsourcing weaknesses) occurring within forty words (as determined by the QDA content analysis software) of "exclusion keyword/phrases" ^d are not counted.

c. The "IT-indicator" word(s)/phrases used in searches for IT weaknesses include: (1) data related keywords/phrases (computer-generated; customer data; customer database; data; data file*; database; datafile*; employee database; financial application programs and data; inut* to model*; master data; master data file*; master file*; masterrecord*; masterfile; master record*; model input*; payroll data; price table; set-up file*; source data; standing data; supplier data; system generat*; vendor database; vendor master file*), (2) systems and software related keywords/phrases (accounts payable system*; accounts receivable system*; accounting system*; application*; automat*; automated process*; automated program*; billing system*; computer*; computer based; computer generated; computer program*);

TABLE 2 (Continued)

c. (continued) computing; contract tracking system*; cost accounting system; costing system; crm; data processing; end user computing; end-user computing; enterprise business system*; enterprise resource planning; enterprise resource platform; ERP; financial application*; financial application programs; financial clos* system*; financial reporting system*; financial software system*; general ledger system*; hardware; information processing; information system*; information technology; information technology application*; information technology systems; inventory system*; inventory costing system*; legacy system*; manufacturing resource planning; manufacturing resource platform; material resource planning software; mrp; open-source; operating system; Oracle; payroll system*; People soft; perpetual inventory system*; platform*; reporting system*; SAP; software; software licens*; spreadsheet*; system generated), (3) people related keywords/phrases (CIO; computing personnel; computing staff*; CTO; director of information technology; information technology personnel; information technology staff*; insufficient information systems support; IT personnel; IT staff*; IT support staff*; programmer*), (4) processes and procedures related keywords/phrases (accounting process; accurately enter*; billing process*; close process*; closing process*; computer operation*; data center*; data entry; data input; financial close*; financial close and report*; financial close process*; financial statement* close* process*; financial statement reporting process*; information and communication control*; information systems operation*; information technology; input*; insufficient information systems support; inventory process*; IT operation*; manual process*; operating procedure*; operations report*; outsource*; payroll process*; period-end reporting process*; perpetual inventory records; process* to analyze; process* to record; processing; processing file*; program change*; program development; proper operation*; properly enter; properly record; reporting process*; SAS 70; service organization*; service provider*; Statement of Auditing Standards No. 70; software support; support operation*; system generat*; third party organization; third party service organization; third-party organization; third-party service; transaction processing; yield curve), and (5) computer control environment related keywords/phrases (access control*; access privilege; access rights; anti-virus; backup*; back-up*; backup media; back-up media; cell protection; computer environment controls; disaster; encrypt*; firewall; general computer controls; general computing control*; information and communication control*; information technology control*; IT controls; IT general controls; ITC*; ITGC; logical access*; offsite; off-site; password*; record* retention; record* storage; remote location; removable media; restricted access; rotation media; security access; security setting*; system privile*; user access; user identification; user security management)

d. “Exclusion keyword(s)/phrases are: accounting for; accounting policies; accounting principles; application of; application of generally; application of generally accepted accounting principles; audit test*; balances; business process policies and procedures; Committee of Sponsoring Organizations; GAAP; generally accepted accounting; impairment; in the course of its testing; income tax*; internal control integrated framework; maintain effective internal control; management’s assess*; method; our observation and testing; public company account*; reserves; SFAS; software development costs; source documentation; statement* of operation*; supporting documentation; tax; third-party subsidiaries. In order to minimize double-counting of certain IT weaknesses, exclusion words also included all word(s)/phrases itemized for end user computing, master files, and outsourcing (except when searching for policies, monitoring or risk assessment IT weaknesses).

TABLE 3

Significant pairwise associations between IT weaknesses in reports with IT weaknesses
Table entries are p-values from tests of association based on Chi-square

	Monitoring	Access	Changes and development	Design	Segregation	End User Computing	Policies	Documentation	Staffing and competency	Masterfiles	Backup	Operations	Outsourcing	Security (other than access)
Monitoring		0.031	0.019	<.001	0.002	0.005	0.002	0.007	0.010	0.017				a
Access			<.001	0.012	<.001	0.037	<.001				0.014	0.019	0.042	0.055
Changes and development				<.001	0.098	0.004	0.095	0.001	0.005		0.034	<.001	0.019	
Design					0.001	<.001	0.003		0.001	0.075		0.002	0.056	a
Segregation							0.002	0.037		<.001		0.018		a
End User Computing													0.078	a
Policies								<.001	0.003		<.001	<.001	0.068	a
Documentation									0.032		0.004	0.070	a	a
Staffing and competency												a	a	a
Masterfiles											a	a	a	a
Backup												a	a	a
Operations													a	a
Outsourcing														a
Security (other than access)														

a. the expected cell count is <5, too low for meaningful chi-square statistical inference

TABLE 4 (continued)**Panel B:** Association between IT and non-IT weaknesses for 111 reports with IT weaknesses 2007-08

	n	% of reports	IC1	IC2	IC8	IC11	IC6	IC4	IC10	IC9	IC15	IC13	IC3	IC12	IC7
Number of Companies	111	100%	110	83	68	35	42	23	18	24	11	2	7	14	2
Monitoring	56	50%	a	0.071				<.001		0.040		a	a		a
Access	45	41%	a			0.005			0.024			a	a		a
Changes and development	47	42%	a				0.014				0.019	a	a		a
Design	33	30%	a				0.005	0.033			a	a	a	a	a
Segregation	26	23%	a			<.001			a		a	a	a	a	a
End-user Computing	30	27%	a						a		a	a	a	a	a
Policies	18	16%	a					a	a	a	a	a	a	a	a
Documentation	15	14%	a	a				a	a	a	a	a	a	a	a
Staffing and competency	11	10%	a	a	a	a	a	a	a	a	a	a	a	a	a
Masterfiles	9	8%	a	a	a	a	a	a	a	a	a	a	a	a	a
Backup	9	8%	a	a	a	a	a	a	a	a	a	a	a	a	a
Operations	3	3%	a	a	a	a	a	a	a	a	a	a	a	a	a
Outsourcing	3	3%	a	a	a	a	a	a	a	a	a	a	a	a	a
Security (other than access)	4	4%	a	a	a	a	a	a	a	a	a	a	a	a	a

a. the expected cell count is <5, too low for meaningful chi-square statistical inference; the columns are truncated at the right for non-IT weaknesses IC16, IC14, IC5, IC19, and IC21 where all non-IT weakness counts are 6 or less and cell counts are too low to permit reliable Chi-square statistics to be calculated

IC1. Accounting documentation, policy and/or procedures

IC2. Accounting personnel resources, competency/training

IC8. Material and/or numerous auditor /year-end adjustments

IC11. Segregations of duties/ design of controls (personnel)

IC6. Untimely or inadequate account reconciliations

IC4. Journal entry control issues

IC10. Restatement or nonreliance of company filings

IC9. Non-routine transaction control issues

IC15. Senior management competency, tone, reliability issues

IC13. Scope (disclaimer of opinion) or other limitations

IC3. Ethical or compliance issues with personnel

IC12. Insufficient or non-existent internal audit function

IC7. Management/Board/Audit Committee investigation(s)

IC18. Ineffective or understaffed audit committee

IC17. Restatement of previous 404 disclosures

IC16. Inadequate disclosure controls (timely, accuracy, complete)

IC14. SEC or other regulatory investigations and/or inquiries

IC5. Remediation of material weakness identified

IC19. Ineffective regulatory compliance issues

IC21. IC -SAB 108 adjustments note

TABLE 5

Significant pairwise associations between IT weaknesses and accounting rule (GAAP/FASB) application failures

*Table entries are p-values from tests of association based on Chi-square**Columns are arranged in decreasing order of frequency of accounting rule (GAAP/FASB) application failure reported in 2004-06.***Panel A:** Associations between IT weaknesses and GAAP/FASB application failures for 269 reports 2004-06

	A23	A1	A21	A18	A22	A24	A14	A12	A19	A6	A4	A2	A11	A9	A10	A17	A20	A13	A8	A25
Number of companies	154	132	126	122	91	90	65	61	46	46	42	41	36	35	31	28	27	24	24	18
monitoring	0.001		<0.001		<0.001	0.033		0.001	0.072			0.004					0.037			
access				0.010			0.092	0.034		0.101		0.090								
changes	0.062				0.002	0.043		0.064	0.081	0.007	0.000	0.040					0.008	0.075		0.100
Design	0.001	0.006	0.003		<0.001	<0.001			0.006	0.006	0.001	<0.001			0.013	0.006	0.001	0.014		0.030
Segregation	0.008	0.025		0.006		0.056	0.086	0.027					0.025			0.087				0.003
End-user Computing	0.008		0.007		<0.001	<0.001	0.023	0.016	0.020	0.047	0.011		0.053	0.001	0.020		0.029	0.001		
Policies	0.013				0.022			0.085	0.024		<0.001	0.027	0.075		0.033	0.027	0.017			
Documentation	0.006										0.031	0.023			0.020					a
Staffing and competency					0.004	0.046			0.078	0.078	0.003	0.022					0.091	0.035		a
Masterfiles	0.005	<0.001	0.036	0.001	0.026	0.007		0.023					a	a	a	a	a	a	a	a
Backup			0.016						a	a	a	a	a	a	a	a	a	a	a	a
Operations									a	a	a	a	a	a	a	a	a	a	a	a
Outsourcing	0.095		0.091		0.038				a	a	a	a	a	a	a	a	a	a	a	a
Security (other than access)	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a

a. the expected cell count is <5, too low for meaningful chi-square statistical inference; the columns are truncated at the right for accounts A5, A3, A16, A15, A7 and A26 where all Accounting Rule Failure counts are 10 or less and cell counts are too low to permit reliable Chi-square statistics to be calculated

TABLE 5 (continued)**Panel B:** Associations between IT weaknesses and GAAP/FASB application failures for 111 reports 2007-08

	A23	A1	A21	A18	A22	A24	A14	A12	A19	A6	A4	A2	A11	A9	A10	A17	A20	A13	A8	A25
Number of companies	42	33	30	37	24	35	27	23	14	12	7	5	24	15	10	13	2	4	7	20
monitoring			0.099					0.039			a	a	0.024				a	a	a	
access											a	a			a		a	a	a	0.014
changes							0.041				a	a			a		a	a	a	
Design	0.053								a	a	a	a	0.003	a	a	a	a	a	a	
Segregation						0.067			a	a	a	a		a	a	a	a	a	a	
End-user Computing				0.023		0.037			a	a	a	a		a	a	a	a	a	a	
Policies			0.097		a		a	a	a	a	a	a	a	a	a	a	a	a	a	a
Documentation		a	a		a		a	a	a	a	a	a	a	a	a	a	a	a	a	a
Staffing and competency	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
Masterfiles	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
Backup	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
Operations	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
Outsourcing	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
Security (other than access)	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a

a. the expected cell count is <5, too low for meaningful chi-square statistical inference; the columns are truncated at the right for accounts A5, A3, A16, A15, A7, and A26 where all Accounting Rule Failure counts are 10 or less and cell counts are too low to permit reliable Chi-square statistics to be calculated

A23. Revenue recognition issues

A1. Accounts/loans receivable, investments & cash issues

A21. Liabilities, payables, reserves and accrual est failures

A18. Inventory, vendor and cost of sales issues

A22. PPE, intangible or fixed asset (value/diminution) issues

A24. Tax expense/ benefit/ deferral/ other (FAS 109) issues

A14. Foreign, related party, affiliated and/or subsidiary issues

A12. Financial statement / footnote / US GAAP, segment disclosure issues

A19. Lease, FAS 5, legal, contingency & commit issues

A6. Consolidation, (Fin46r/Off BS) & foreign currency translation issues.

A4. Capitalization of expenditures issues

A2. Acquisition, merger, disposal or reorganization issues

A11. Expense recording issues

A9. Deferred stock-based or executive compensation issues

A10. Depreciation, depletion or amortization issues

A17. Intercompany/ Investment w/ sub/affiliate issues

A20. Lease, leasehold and other FAS 13 (98) issues

A13. Financial derivatives / hedging (FAS 133) accounting issues

A8. Debt, quasi-debt warrants & equity (BCF) security issues

A25. Unspecified/ unidentified/ inapplicable FASB/GAAP issue

A5. Cash flow statement (FAS 95) classification errors

A3. Balance sheet classification of asset issues

A16. Income statement classification, margin and EPS issues

A15. Gain or loss recognition issues

A7 Debt and/or equity classification issues

A26. Other – Defective or unreliable accounting/ reporting records

TABLE 6

Comparison of range of average number of IT and non-IT weaknesses per report for reports with both IT and non-IT weaknesses by year, industry, company size, auditor type and internal control quality

Company attributes compared	IT Weaknesses				Non-IT Weaknesses			
	Highest Average		Lowest Average		Highest Average		Lowest Average	
	Company Attribute	Mean (SD)	Company Attribute	Mean (SD)	Company Attribute	Mean (SD)	Company Attribute	Mean (SD)
Year of report (2004 - 2008)	2005	4.29 (2.23)	2008	2.32 (1.43)	2005	5.35 (2.18)	2008	3.95 (2.06)
Industry (16 classifications) ^a	industrial equipment	4.78 (2.24)	banks & insurance	3.02 (2.16)	services	5.60 (2.90)	transportation	3.97 (1.93)
Company size (larger vs smaller) ^b	smaller	3.83 (2.21)	larger	3.71 (2.35)	larger	5.22 (2.68)	smaller	4.55 (2.01)
Auditor type (Big 4 vs other)	Big 4	3.94 (2.63)	other	3.56 (2.11)	Big 4	5.32 (2.41)	other	4.15 (2.04)
non-IT Internal Control quality (weaker vs stronger) ^c	weaker non-IT control quality	4.20 (2.31)	stronger non-IT control quality	2.80 (1.84)	weaker non-IT control quality	5.92 (1.88)	stronger non-IT control quality	2.28 (0.80)
IT Internal Control quality (weaker vs stronger) ^c	weaker IT control quality	4.31 (2.09)	stronger IT control quality	1.00 (<.001)	weaker IT control quality	5.02 (2.34)	stronger IT control quality	3.84 (2.05)

a. Industries with more than 15 companies are included in this comparison. We classified companies into sixteen industries using the four-digit SIC codes (Ge and McVay, 2007a) Agriculture 100–999; 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: 3500–3569, 3580–3659; Electrical: 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: 6000–6999; Services: 7000–7369, 7380–8999; Miscellaneous: 9000–9999.

b. Using a median split based on total assets, we classified the companies with internal control weaknesses into larger and smaller companies: 58% of the companies with IT weaknesses were smaller and 42% were larger.

c. We split companies into groups based on the number of control weaknesses they reported. We classified companies where those with the stronger non-IT control quality had less than the median number (3) non-IT weaknesses and those with the stronger IT control quality had less than the median number (4) IT weaknesses.

TABLE 7

Comparison of IT and non-IT weaknesses per company for companies with both IT and non-IT weaknesses by weakness persistence

Panel A: Remediated and non-remediated average number of IT and non-IT weaknesses per company in companies with IT weaknesses

	IT Weaknesses						Non-IT Weaknesses in Reports with IT Weaknesses					
	n	IT Weaknesses: One or More IT Weakness Persists into the Next Year		IT Weaknesses: All IT Weaknesses remediated		<i>p</i> -value of t-test	n	Non-IT Weaknesses: One or More non-IT Weakness Persists into the Next Year		Non-IT Weaknesses: All non-IT Weaknesses remediated		<i>p</i> -value of t-test
		N	Mean (SD)	N	Mean (SD)			N	Mean (SD)	N	Mean (SD)	
Persistence ^a												
2004	99	26	5.69 (2.33)	73	3.75 (2.16)	<.001	99	27	7.26 (2.92)	72	4.46 (2.27)	<.001
2005	98	31	5.13 (2.74)	67	3.90 (1.84)	0.028	98	34	6.00 (2.22)	64	5.00 (2.09)	0.030
2006	72	21	4.95 (1.86)	51	3.55 (2.41)	0.011	72	24	4.96 (2.14)	48	4.50 (2.42)	0.392
2007	67	13	4.38 (1.94)	54	2.78 (1.93)	0.009	67	17	4.65 (2.12)	50	4.12 (1.95)	0.349
2004-2007	336	91	5.14 (2.34)	245	3.53 (2.11)	<.001	336	102	5.86 (2.55)	234	4.54 (2.14)	<.001
larger companies	143	40	5.33 (2.25)	103	3.38 (2.20)	<.001	143	45	6.60 (3.05)	136	4.78 (2.35)	0.001
smaller companies	193	51	5.00 (2.42)	142	3.65 (2.05)	<.001	193	57	5.28 (1.92)	98	4.38 (1.96)	0.004
Big 4 auditor	201	56	5.32 (2.35)	145	3.65 (2.20)	<.001	201	62	6.48 (2.72)	139	4.99 (2.11)	<.001
Other auditor	135	35	4.86 (2.32)	100	3.37 (1.97)	<.001	135	40	4.90 (1.93)	95	3.89 (2.01)	0.008