What Can We Learn from
Critical Clusters of Internal Control Weaknesses?

Efrim Boritz
Louise Hayes
Jee-Hae Lim

University of Waterloo

September 2009

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

We wish to acknowledge the funding provided by the CAAA/CICA Research Program and the University of Waterloo Centre for Information Systems Assurance, sponsored by the Canadian Institute of Chartered Accountants, ISACA and CaseWare IDEA Inc.
Abstract

The Audit Analytics database identifies 21 categories of internal control weaknesses that appear in SOX 404 reports. Individual IT control weaknesses are not identified but are simply grouped together in one of these 21 categories (category code #20). To date there has been no systematic study of the various types of IT control weaknesses included under category code #20 to learn about which weaknesses occur and with what relative frequency, how they vary with various contextual factors and which weaknesses appear together frequently. In this research we address three main Research Questions (RQ).

1. RQ1: What are the most common clusters of IT control weaknesses?

2. RQ2: Are the most common clusters of IT control weaknesses associated with factors such as Year of report, Industry, Company Size, Auditor Type and Internal Control Quality?

3. RQ3: Are non-IT internal control weaknesses associated with IT control weaknesses or clusters of IT weaknesses?

Knowledge obtained through this research could help researchers, managers and auditors better understand which internal control weaknesses occur together and could help spur research to identify factors causing such co-occurrence and consequences of various clusters of weaknesses compared with other clusters or individual weaknesses.
What Do Critical Clusters Internal Control Weaknesses Tell Us About Financial Reporting Systems?

Introduction

For decades managers, auditors and regulators have recognized that effective internal controls are integral to reliable financial reporting. However, in their first four years of reporting on internal controls in accordance with SOX 404, hundreds of companies have reported material internal control weaknesses* indicating that, despite their importance, internal controls were not being implemented effectively in many public companies, exposing their financial reports to the risk of material misstatements. In the past, 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 evidence about the impact of internal control weaknesses on company performance. Now, however, the auditors’ reports on internal control are available through the 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.

* During the sample period of the proposed study, material weaknesses are those significant control deficiencies that result in more than a remote likelihood that a material accounting misstatement will not be prevented or detected (PCAOB Auditing Standard No. 2, 2004). The phrase “reasonably possible” replaced the phrase “more than remote likelihood” in this definition when Auditing Standard No. 5 replaced Auditing Standard No. 2 in 2007 (PCAOB Auditing Standard No. 5, 2007). Control deficiency is also a defined in these Auditing Standards.

† 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 required to certify executive management’s assessment. Section 302 requires executive management assert that they have disclosed significant control deficiencies, material weaknesses, significant changes in controls, and acts of fraud to their audit committees and independent auditors.

The results of the aforementioned studies indicate that internal control weaknesses have affected all of these factors to some degree. However, to our knowledge there has been no systematic study of the weaknesses themselves other than an early study by Gupta and Leech (2004) sponsored by the Financial Executives Research Foundation and the study by Doyle, et al. (2007a and 2007b) which distinguished company-wide and account-specific internal control weaknesses in their tests. Recently, many researchers have been relying on companies’ internal control weaknesses as reported in the Audit Analytics database which 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.

Internal control (e.g., COSO) and auditing publications (e.g., PCAOB (AS #5) discuss the distinction between various categories of IT controls such General Controls and Application Controls and within these categories 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 which companies report weaknesses in these categories and why. There is no published information that documents the attributes of companies in these categories and breaks the IT control weakness categories into finer sub-categories. Also, there is no published information about critical combinations or clusters of internal control weaknesses such as IT weaknesses, non-IT control weaknesses and frequently recurring combinations of material IT and non-IT internal control weaknesses.

The few studies that have attempted to investigate associations between IT control deficiencies identified in SOX 404 reports and other factors (Masli et al., 2009; Li et al. 2008) appear to have performed scans of the relevant reports manually, without the aid of content analysis software tools. In addition, those studies do not appear to recognize that virtually all companies with IT control weaknesses also have non-IT control weaknesses. The pattern of non-IT control weaknesses reported by companies without IT control weaknesses may be different than the pattern of non-IT control weaknesses reported by companies with IT control weaknesses. Thus, the reliability of manual scans and findings of studies of associations between IT control weaknesses and other factors are unknown and this represents an obstacle to reliably linking the presence of IT control weaknesses with other variables such as financial performance, audit fees and corporate and IT governance and determining implications of those associations.

To date there has been no systematic study of the various types of IT control weaknesses, to learn about the factors that may determine which weaknesses occur, which ones are identified in SOX 404 reports, which weaknesses appear together frequently and how clusters of weaknesses affect financial performance. We address several of these issues in this paper. Knowledge obtained through this research could help managers and auditors better understand which internal control weaknesses occur together and could help spur research to identify factors causing such co-occurrence and consequences of various clusters of weaknesses compared with
other clusters or individual weaknesses. Of interest to both practitioners and academics is whether and how time, industry, company size, auditor type (Big 4 vs. Other) and internal control quality are associated with various categories and clusters of internal control weaknesses.

**Research Questions:**

This study will address three main Research Questions (RQ).

4. **RQ1:** What are the most common clusters of *IT control weaknesses*?

5. **RQ2:** Are the most common clusters of *IT control weaknesses* associated with factors such as Year of report, Industry, Size, Auditor Type and Internal Control Quality?

6. **RQ3:** Are non-IT internal control weaknesses associated with *IT control weaknesses* or clusters of *IT weaknesses*?

**RQ1:** What are the most common clusters of *IT control weaknesses*?

Our preliminary analyses indicate that some internal control weaknesses are transient – they appear in a year and disappear - whereas other internal control weaknesses persist from year to year. We also have observed that a small number of IT control weaknesses seem to appear frequently together with a small number of non-IT weaknesses. Some clusters of control weaknesses such as weaknesses in IT controls can detrimentally affect an entity’s operations and increase audit fees, affecting both revenues and costs in addition to their other impacts as documented in other research. COBIT®, and other IT frameworks (e.g., CICA’s IT Control

---

\[COBIT®, Control Objectives for Information and related Technology (IT Governance Institute, 2007) outlines good practices that fit with and support the COSO, Committee of Sponsoring Organisations of the Treadway Commission’s, Internal Control Integrated Framework. The use of a combination of COBIT®, to assess IT related controls, and COSO, meets the SOX requirement that internal control be evaluated with a “suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment” (SEC, 2003).\]
Guidelines), provide high level guidance on what controls should exist in well-managed entities but do not detail actual IT weaknesses reported by companies, including the IT weaknesses that appear repeatedly and in combination with other IT and non-IT weaknesses.

To investigate RQ1, we will develop a ‘dictionary’ of words/phrases that may be used, in conjunction with Boolean logic and content analysis software, to identify IT control weaknesses in the SOX 404 Auditors’ reports. Table 2 provides entries in the “dictionary” we developed using the 274 companies reporting IT weaknesses in the period 2004-2006. Independent manual coding of a sample of 20 SOX 404 reports was used to assess the accuracy of the ‘dictionary’ and Boolean logic in IT control weakness identification.

Using the results of automated searches, we examined the associations between IT control weaknesses in the SOX 404 reports from 2004-2006. Cross-tabulations and proximity measures were used to identify “clusters” of IT control weaknesses.

RQ2: Are the most common clusters of IT control weaknesses associated with factors such as Year of report, Industry, Size, Auditor Type and Internal Control Quality?

The above effects (RQ1 and RQ2) may differ across years, industries, firm size, auditor type and internal control quality. According to Doyle et al. (2007a), industry type is one of the proxies for the incentives to discover and disclose internal control problems. 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

---

§ Boritz and Lim (2008) used the Audit Analytics database to identify all companies subject to SOX 404 regulations that reported material internal control weaknesses between 2004 and 2006. They supplemented their sample through manual review on the SEC’s Edgar database and validated 10-K filings in the Lexis-Nexis database using several IT-related keywords.
and separately report on management’s assertions. Thus, we consider different types of industries that may capture the tendency of material weaknesses to cluster by industry.

Compared to small firms, large firms have more expertise in deploying IT resources and controls because they can afford to hire major consulting firms to provide specialized services and offer expert advice. Large firms are also obligated to have more comprehensive internal controls and auditing systems in place (Klein 2002), which may further mitigate agency problems. Fourth, subsequent to the passage of SOX and the formation of the PCAOB the role of the auditor has undergone a significant change (Krishnan 2005; Raghunandan and Rama 2006). Prior literature suggests that Big 4 auditors have more resources and also tend to be more conservative than non-Big 4 auditors. Thus, Big 4 auditors are more likely to detect internal control weaknesses than non-Big 4 auditors.

Using cross-tabulation and chi-square tests of significance we test the association between the presence of IT control weaknesses with the following factors:

- Year of Report (2004-2006),
- Industry (SIC Codes),
- Company Size (Total Assets)
- Auditor Type (Big 4 vs. Other) and
- Internal Control Quality (number of weaknesses reported)

RQ3: Are non-IT internal control weaknesses associated with IT control weaknesses or clusters of IT weaknesses?

The Audit Analytics database identifies 20 non-IT internal control weaknesses (Figure 1) that appear in SOX 404 reports. Individual IT control weaknesses are not identified but are simply grouped together in one category (item 20 in Figure 1).
Using cross-tabulation and chi-square tests of significance conducted on the SOX404 reports of 2004-2006, we tested the association of IT control weaknesses/clusters with the 20 non-IT internal control weaknesses (Figure 1) identified for SOX 404 reports in the *Audit Analytics* database.

**Analysis**

**Data Sources**

Using *Audit Analytics*, we identified 1,343 companies that reported internal control weaknesses for fiscal 2004-2006. About 20% of the companies had both IT and non-IT control weaknesses and 80% had only non-IT control weaknesses. There were only two companies (one in 2004 and one in 2005) that reported only IT control weaknesses. Table 1 summarizes the number of companies reporting non-IT weaknesses and IT weaknesses by year. This table reports summary statistics for the 20 non-IT control weaknesses as reported by *Audit Analytics*. As mentioned previously, 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. Thus, it is as if there is only one IT weakness per company and the total number of IT weaknesses is identical to the number of companies with an entry for code #20.

Insert Table 1
Using the *Audit Analytics* database we obtained** the auditors’ SOX 404 reports for 263 companies reporting IT control weaknesses in 2004 – 2006 (i.e., those identified by Internal Control Weakness Code 20).†† We supplemented these 263 reports with 11 additional reports located by searching the *Lexis-Nexis* database using several IT-related keywords (Boritz and Lim 2008).

Instead of accepting the coding of IT weaknesses as given by *Audit Analytics* we used an automated content analysis tool‡‡ to independently perform key word searches of SOX 404 reports issued between 2004-2006 based on search strings such as those listed in Table 2 to break down the *Audit Analytics* code “20” into sub-categories of specific IT control weaknesses.

Insert Table 2

Therefore the number of weaknesses found and the number of companies for which weaknesses were identified differs from the counts obtained by simply relying on the presence or absence of an indicator in Code 20, depending upon the actual keywords/phrases and search criteria used in the automated search. Over the 2004-2006 time period, companies without IT weaknesses averaged three to four non-IT weaknesses each, whereas companies with IT weaknesses averaged five non-IT weaknesses plus three IT weaknesses each.

Table 2 reports the counts for keywords/phrases based on two different degrees of restrictiveness in our search criteria. Both search criteria counts a company as having an end user computing, masterfile, ERP and outsourcing IT weaknesses when any keyword/phrases listed in

** Searches in Audit Analytics are date dependent, since the database is continuously being updated. We extracted the data for this paper on May 22, 2009.
†† Although Audit Analytics lists 264 companies with IT weaknesses, we could not locate the SOX 404 report for Pain Care Holdings Inc. for 2006.
‡‡ QDA Miner from Provalis Research Inc.
the table associated with these weaknesses occur anywhere in the company’s SOX 404 audit report. The other IT weaknesses are identified by the less restrictive search criteria when keyword/phrases associated with these weaknesses occur within the same sentence as an “IT indicator”. The more restrictive search criteria require both that there be an “IT indicator” in the same sentence (listed at the bottom of the table) and that the sentence does not contain an “exclusion keywords/phrases.” The “IT indicator” and “exclusion keywords/phrases” are listed the bottom of the table.

Insert Table 2

Table 2 presents search results for two different search criteria – one more restrictive than the other – that we developed to search for occurrences of IT weaknesses using the content analysis software which identified IT weaknesses in 89% (244 out of 274) and 96% (263 out of 274) of the companies, respectively. Figure 2 is an illustrative example of a SOX 404 with IT weaknesses identified.

Insert Figure 2

The Appendix provides three illustrative examples of our search criteria applied to SOX 404 reports.

1. Example Report 1: This is an example of an auditors’ report which Audit Analytics identifies as having six non-IT weaknesses, two more weaknesses than any company classified as having less weak non-IT controls on the basis of a median split of non-IT control weaknesses.
2. Example Report 2: This is an example of an auditors’ report which Audit Analytics characterized as having IT weaknesses and five non-IT weaknesses but where our search criteria did not identify any IT-weaknesses.

3. Example Report 3: This is an example of a report with six IT-weaknesses, one more than any company with less weak IT controls and two associated non-IT weaknesses.

Reliability Checks

We read the reports of all companies for which the code “20” in the Audit Analytics database indicated that they had IT weaknesses but our automated searches failed to find any IT weaknesses and found only a very few reports for which we could not identify one or more IT weaknesses. We concluded that the code 20 indicator in Audit Analytics is reliable; merely less informative than the codes for non-IT weaknesses which offer more granular information to users of the database.

We also checked the accuracy of the automated content analysis for a random sample of 20 companies with 50 IT weaknesses and 20 companies with 68 non-IT weaknesses per Audit Analytics. For the sub-sample with IT weaknesses, the less restrictive search better identified the 50 IT weaknesses in the sample than the more restrictive search (78% vs. 64%, respectively). However, the less restrictive search produced almost twice as many false positives as the more restrictive search (29 vs. 16). For the sub-sample of companies without IT weaknesses there were no false positives by either search for 17 of the 20 companies. For three companies there was a total of five false positives – one for the more restrictive search and four for the less restrictive search. When search accuracy is computed as the correct identification of the presence
or absence of IT control weaknesses in the sample, the results were 90% and 89% for the more restrictive search and the less restrictive search, respectively. On the basis of these reliability tests we concluded that the search quality was sufficiently reliable for the analyses performed in this paper.

Table 3 reports the summary statistics based on two different groupings of the key-words in Table 2. One grouping involved reducing the number of categories in Table 2 by about half, to permit statistical analyses to be conducted on this data, since items with low counts lead to unstable results. The second grouping involved aggregating the weaknesses in Table 2 into four COSO categories. We could not distinguish the controls belonging to the Information and Communication category and the Activities category so we grouped these into a single category. It is important to note that the counts for the groupings in Table 3 differ by grouping because the grouping eliminated double counting. That is if the text in the SOX 404 report could be coded as several weaknesses in Table 2, when those weaknesses were grouped in Table 3 they would only be counted once if they were all classified in the same group.

Insert Table 3

**RQ1: What are the most common clusters of IT control weaknesses?**

We identified individual control weaknesses in three ways:

1. Based on the results of basic content analysis of SOX 404 reports that identified the following 17 control weaknesses (as summarized in Table 2).

   1. Policies
   2. Staffing and Competency
   3. Risk assessment
   4. Access
   5. Segregation
2. Based on grouping results of the content analysis into the following eight control categories with counts large enough to permit statistical analysis (as summarized in Panel A of Table 3):

1. Policies
2. Staffing & Competency
3. Risk Assessment
4. Access and Segregation
5. Design, Change and Documentation
6. End-user computing
7. Other Information & Communication
8. Monitoring

3. Based on grouping individual controls into the following COSO categories (as summarized in Panel B of Table 3):

1. Control Environment
2. Risk Assessment
3. Information, Communication, Activities
4. Monitoring

**RQ2: Are the most common clusters of IT control weaknesses associated with factors such as Year of report, Industry, Size and Auditor Type?**

Table 4 summarizes the IT weaknesses cross-tabulated in several ways: year, industry, company size, auditor size, and overall internal control quality.
Year

The number of companies reporting IT weaknesses dropped in 2006 compared to 2004 and 2005. However, the average number of weaknesses per company for companies with IT weaknesses did not change, being about 3 IT weaknesses per year with the more restrictive search criteria or 4 IT weaknesses per year with the less restrictive search criteria. The average number of weaknesses for companies with no IT weaknesses was consistently between 3 and 4 per company each year; however the average number of non-IT weaknesses for companies with IT weaknesses was higher, averaging about 5 non-IT weaknesses per company each year.

Industry

Using two-digit SIC codes we compared the weaknesses by industry. We created 12 industry groupings with IT weaknesses sufficient in number to perform statistical analyses. We found few industry differences. These differences are reported here as the industry group(s) with the lowest number of weaknesses since other than the groups identified here, the industries were very similar in the average number of weaknesses reported.

The companies in industries with SIC codes 60-71 (banks, insurance companies and real estate services) had the fewest IT weaknesses (p<.03). The average number of IT weaknesses was not significantly different for any other industry grouping across both search criteria. In contrast, companies with IT weaknesses in two-digit SIC codes 28-34 (chemicals, plastics, concrete, rubber, metal refining and fabricated metal products) had the fewest non-IT weaknesses compared with all other industry codes (p<.000). For companies without any IT

---

§§ SIC 10 -17; SIC 20-27; SIC 28-34; SIC 35; SIC 36; SIC 37; SIC 38; SIC39; SIC 40-49; SIC 50 – 59; SIC 60 – 67; SIC 72-87.
weaknesses, companies in two-digit SIC codes 38 (apparatus, instruments, meters, controlling
devices and photographic equipment) and 50-59 (wholesalers and retailers) had the fewest
weaknesses (p<.05).

Company size
Using a median split, based on median total assets of $498 million for all 1,343 companies with
internal control weaknesses, we classified the companies with internal control weaknesses into
larger and smaller companies: 60% of the companies with IT weaknesses were smaller and 40%
were larger, and the larger companies had significantly more non-IT weaknesses than smaller
companies (p=.013). For companies without IT weaknesses, the number of weaknesses did not
differ with company size. These overall findings must be interpreted in light of the interaction
between year, company size and auditor size discussed in the next section.

Auditor size
We classified companies’ auditors into two categories - Big4 and non-Big 4. Companies audited
by Big 4 audit firms reported more non IT weaknesses (p<.000) than companies audited by non-
Big 4 audit firms. However, the number of IT-weaknesses reported for companies audited by
Big 4 audit firms and those audited by non-Big 4 audit firms was only significantly greater
(p<.05) when the less restrictive search criteria were used to identify IT weaknesses.

We found an interesting interaction between auditor size and year for 2004. There was no
significant difference between the average number of IT weaknesses reported by the two groups
of auditors in 2005 and 2006.*** In 2004, the smaller companies with Big 4 auditors reported the

*** We excluded large companies with non Big 4 auditors from this discussion because of the small number of these
companies (9, 1 and 7 in 2004, 2005 and 2006, respectively) precludes reliable conclusions from being drawn.
largest number of IT weaknesses (on average) whereas the smaller companies with non-Big-4 auditors reported the smallest number of IT weaknesses (on average) (p=.026). The number of IT weaknesses reported by Big4 auditors did not differ significantly by company size in 2004.

Internal Control Quality

We split companies into groups based on the number of control weaknesses they reported. We classified companies into four categories based on their non-IT and IT internal control quality (ICQ), where the least weak ICQ had 4 or less non-IT weaknesses and 5 or less IT weaknesses and the weakest ICQ had 5 or more non-IT weaknesses and 6 or more IT weaknesses. We found the number of companies in each of the four categories differed significantly from the number expected by chance (p <.001):17% of the companies fell into the weakest ICQ category but had more than the median number of weaknesses in both non-IT and IT controls; 38% fell into the least weak ICQ category and had fewer than the median number of weaknesses in both non-IT and IT controls. The balance fell in the two middle categories: 5% had comparatively weaker IT controls, while 41% had comparatively weaker non-IT controls.

Proportionately more companies with IT weaknesses (57%) than those without (18%) had 5 or more non-IT weaknesses. In companies with a comparatively large number of non-IT control weaknesses, the companies with IT weaknesses had more non-IT weaknesses  (p<.000) and IT weaknesses (p<.002) For companies with four or fewer non-IT weaknesses, the number of non-IT weaknesses was not significantly different between companies with and without IT weaknesses.

RQ3: Are non-IT internal control weaknesses associated with IT control weaknesses or clusters of IT weaknesses?
We calculated pairwise associations between six IT and 20 non-IT weaknesses in our set of 244 or 263 companies, depending on the search used. The six IT weaknesses were based on the grouping of Panel A in Table 3 except that we had to omit the Risk Assessment Category and group the Policies and Staffing and Competency categories into the following six categories to have counts of sufficient size to perform meaningful statistical analyses.

1. Control Environment (Policies and Staffing and Competency)
2. Segregation & Access
3. Design, Change and Documentation
4. End user computing
5. Other Information & Communication
6. Monitoring

As Table 4 indicates, the pairwise associations between these IT weaknesses indicates that they are highly clustered, with over half of the 15 possible associations (12 for the more restrictive search and 8 for the less restrictive search) being significant at \( p < .05 \). This is quite different from the pattern observed for the pairwise associations between IT and non-IT weaknesses, where less than one sixth of the 120 possible associations (18 for the less restrictive search and 12 for the less restrictive search) are significant at \( p < .05 \).

The following seven of the 20 non-IT weaknesses coded in *Audit Analytics* had no statistical association with IT weaknesses (at a \( p \) value of \(< .10 \)) or had too few items in a cell for a meaningful statistic to be calculated.

5. Remediation of material weakness identified
12. Insufficient or non-existent internal audit function
14. SEC or other regulatory investigations and/or inquiries
16. Inadequate disclosure controls (timely, accuracy, complete)
17. Restatement of previous 404 disclosures
19. Ineffective regulatory compliance issues
21. IC-SAB 108 adjustments noted
Thirteen of the 20 non-IT controls had significant associations (p < .10) with between one and five of the six IT control groupings under at least one of the search criteria.

The following four non-IT weaknesses had the same pattern of significant associations with specific IT weaknesses across both the less and more restrictive searches:

2. Accounting personnel resources, competency/training was associated with Monitoring, End user computing and Control environment IT weaknesses (p<.10).
8. Material and/or numerous auditor /year-end adjustments was associated with Monitoring and End user computing IT weaknesses (p<.10).
11. Segregation of duties/ design of controls (personnel) was associated with Segregation and access and Other information and communication IT weaknesses (p<.001)
13. Scope (disclaimer of opinion) or other limitations was associated with Segregation and access IT weakness (p=.020)

The following five non-IT weaknesses had significantly associated IT-weaknesses in common under both search criteria, albeit the less restrictive criteria found additional significant associations:

4. Journal entry control issues was associated with Monitoring and End user computing under both search criteria (p<.10) and only with Other information and communication under the less restrictive criteria (p<.10).
6. Untimely or inadequate account reconciliations were associated with Monitoring and Other information and communication (p<.05) under both search criteria and associated with all but Segregation and access under the less restrictive criteria (p<.10).
15. Senior management competency, tone, reliability issues were associated with the Control environment (p< .05) and End-user computing, (p <.10) under both criteria and with Monitoring only under the less restrictive criteria (p<.05).
7. Management/Board/Audit Committee investigation(s) was associated with Monitoring (p<.10) under both criteria and with End user computing only under the less restrictive criteria (p<.10).
18. Ineffective or understaffed audit committee was associated with Other information and communication (p<.01) under both criteria and with Segregation and Access only under the less restrictive criteria (p<.10).

The significant associations of non-IT weaknesses with specific IT weaknesses shared no commonalities under both search criteria for the following four non-IT weaknesses:

1. Accounting documentation, policy and/or procedures (three significant associations under the less restrictive criteria, p<.10, and a different association under the more restrictive criteria p<.10).
3. Ethical and compliance issues with personnel (two associations under the less restrictive criteria, p<.10, and none under the more restrictive criteria).
9. Non-routine transaction control issues (three associations under the more restrictive criteria, \( p < .06 \), and none under the less restrictive criteria).
10. Restatement or nonreliance of company filings (one association, \( p < .05 \), under the less restrictive criteria and none under the less restrictive criteria).

Looking at it from a different perspective, the IT weakness that was most strongly associated with the non-IT weaknesses was Monitoring (respectively, six or seven significant associations with the more restrictive or less restrictive searches at \( p < .10 \)), followed by End user computing (respectively, four or seven significant associations with the more restrictive or less restrictive searches), Other Information & Communication (respectively, four or five significant associations with the more or less restrictive searches), Control Environment (respectively, three or four significant associations with the more or less restrictive searches) Segregation & Access (respectively, two or four significant associations with the more or less restrictive searches) and Design, Change and Documentation (one significant association under each of the search criteria).

Discussion & Limitations and Future Research

We believe that our study makes the following contributions to academe and practice.

- 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.

- We also hope to facilitate further study of IT controls by demonstrating the efficacy of using automated procedures to search SOX404 reports to identify IT control weaknesses.

- The sub-division of IT weaknesses based on content analysis can help researchers hampered by the lacking granularity of the coding in *Audit Analytics*.
• The identification of a small number of frequently-occurring clusters of IT control weaknesses and non-IT control weaknesses will lead to the development and testing of hypotheses concerning the differential effects of various control weakness clusters on financial performance.

• The identification of frequently occurring clusters of control weaknesses may provide managers, auditors, standard setters and regulators with relevant information about internal control issues to inform their respective policy considerations.

Our findings indicate that IT weaknesses do not occur in isolation. They generally occur in companies with a large number of non-IT weaknesses. The average number of internal control weaknesses for companies with IT weaknesses was consistently higher than the average. In particular, the average number of non-IT weaknesses for companies with IT weaknesses averaged about five non-IT weaknesses per company. Not only does the number of non-IT weaknesses figure prominently in companies with IT weaknesses but clusters of IT and non-IT weaknesses could figure prominently as well. Thus, researchers testing models using IT weaknesses as dependent or independent variables should take care not to omit non-IT weaknesses in their models.

Our findings also indicate that the IT weaknesses reported in 2004 may not be representative of the IT weaknesses reported in 2005 and 2006. Thus, researchers should exercise caution when including 2004 data on IT weaknesses, company size and auditor type in research models.

Selected industries have significantly lower numbers of IT weaknesses and these industries should be controlled for in research models as well.

In terms of specific control weaknesses, the three most frequent weaknesses were monitoring control weaknesses (138), followed by access control weaknesses (113), followed by end-user
control weaknesses (86). Considering the large number of weaknesses in all the other COSO categories, we were surprised that risk assessment weaknesses were infrequently reported. This warrants additional investigation.

A planned extension of this study is to track remediations of internal control weaknesses and, more specifically, identify particularly persistent weaknesses that are reported for two or three years running as compared with weaknesses that are not persistent. This would require obtaining additional data on reported weaknesses for 2007 and 2008 since our data relates solely to the period 2004-2006.

Another potential extension to this study would be to survey IT control and audit practitioners to obtain their reaction to our coding and our findings.

Another planned extension is to relate the IT and non-weaknesses and clusters of weaknesses identified in this paper to company financial performance.
References:


Canadian Institute of Chartered Accountants (CICA) 1998. IT Control Guidelines (Toronto: CICA.)


IT Governance Institute (ITGI). 2007. COBIT® 4.1 Rolling Meadows, IL. USA. Available online on May 12, 2009 at:


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
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.

***With the 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 the more restrictive search no IT weaknesses are found, because the sentence in which the IT weakness is described is excluded because of the presence of a non-IT indicator (generally accepted accounting principles). However, the two incorrectly identified weaknesses identified with the less restrictive search are also omitted.***
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.

/s/ Ernst & Young LLP

Tampa, Florida
April 29, 2005
Table 1 – Summary Statistics of SOX 404 reports with weaknesses\(^a\) reported in 2004, 2005 and 2006

Panel A – summary statistics when more restrictive automated search criteria are used to identify the companies with IT control weaknesses \(^b\)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Companies</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>reporting IT</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and non-IT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Weaknesses</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Number of companies</strong> (^b)</td>
<td>91</td>
<td>363</td>
<td>87</td>
<td>401</td>
</tr>
<tr>
<td><strong>Number of non-IT Control Weaknesses:</strong> (^a)</td>
<td>5.25</td>
<td>3.44</td>
<td>5.30</td>
<td>3.42</td>
</tr>
<tr>
<td><strong>Mean</strong></td>
<td>2.77</td>
<td>1.47</td>
<td>2.16</td>
<td>1.52</td>
</tr>
<tr>
<td><strong>Standard Deviation</strong></td>
<td>0.68</td>
<td>1.13</td>
<td>0.46</td>
<td>1.84</td>
</tr>
<tr>
<td><strong>Skewness</strong></td>
<td>0.06</td>
<td>1.10</td>
<td>0.65</td>
<td>1.10</td>
</tr>
<tr>
<td><strong>Range</strong>(^c)</td>
<td>0-14</td>
<td>1-10</td>
<td>0-11</td>
<td>1-13</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>478</td>
<td>1,247</td>
<td>461</td>
<td>1,370</td>
</tr>
</tbody>
</table>

\(^a\) 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. Thus, it is as if there is only one IT weakness per company and the total number of IT weaknesses is identical to the number of companies with an entry for code IC 20. This table reports summary statistics for the 20 non-IT control weaknesses as reported by *Audit Analytics*.

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

\(^c\) The range is the minimum to the maximum number of *Audit Analytics* database internal control weakness codes (of the 20 codes for weaknesses other than IT weaknesses) appearing in SOX 404 reports for each company.

\(^d\) There were only two companies (one in 2004 and one in 2005) that reported only IT control weaknesses.
Panel B – summary statistics when less restrictive automated search criteria are used to identify the companies with IT control weaknesses

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Companies</td>
<td>Companies</td>
<td>Companies</td>
<td>Companies</td>
</tr>
<tr>
<td></td>
<td>reporting IT</td>
<td>reporting only</td>
<td>reporting IT</td>
<td>reporting IT</td>
</tr>
<tr>
<td></td>
<td>and non-IT</td>
<td>non-IT</td>
<td>and non-IT</td>
<td>and non-IT</td>
</tr>
<tr>
<td></td>
<td>Weaknesses</td>
<td>weaknesses</td>
<td>Weaknesses</td>
<td>Weaknesses</td>
</tr>
<tr>
<td>Number of companies b</td>
<td>102</td>
<td>352</td>
<td>94</td>
<td>394</td>
</tr>
<tr>
<td>Number of non-IT</td>
<td>102</td>
<td>352</td>
<td>94</td>
<td>394</td>
</tr>
<tr>
<td>Mean</td>
<td>5.15</td>
<td>3.41</td>
<td>5.29</td>
<td>3.39</td>
</tr>
<tr>
<td>Standard Deviation</td>
<td>2.66</td>
<td>1.47</td>
<td>2.19</td>
<td>1.48</td>
</tr>
<tr>
<td>Skewness</td>
<td>0.75</td>
<td>1.20</td>
<td>0.46</td>
<td>1.82</td>
</tr>
<tr>
<td>Range c</td>
<td>0-14</td>
<td>1-10</td>
<td>0-11</td>
<td>1-13</td>
</tr>
<tr>
<td>Total</td>
<td>525</td>
<td>1,200</td>
<td>497</td>
<td>1,334</td>
</tr>
</tbody>
</table>

a. The *Audit Analytics* database codes internal control weaknesses appearing in SOX 404 reports using 21 identifiers, one of which (IC20) signifies all information technology (IT) control weaknesses. This table reports summary statistics for the 20 non-IT control weaknesses as reported by *Audit Analytics*.

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

c. The range is the minimum to the maximum number of *Audit Analytics* database internal control weaknesses codes (of the 20 codes for weaknesses other than IT weaknesses) appearing in SOX 404 reports for each company. There were only two companies (one in 2004 and one in 2005) that reported only IT control weaknesses.

---

*a. The Audit Analytics database codes internal control weaknesses appearing in SOX 404 reports using 21 identifiers, one of which (IC20) signifies all information technology (IT) control weaknesses. This table reports summary statistics for the 20 non-IT control weaknesses as reported by Audit Analytics.*

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

*c. The range is the minimum to the maximum number of Audit Analytics database internal control weaknesses codes (of the 20 codes for weaknesses other than IT weaknesses) appearing in SOX 404 reports for each company. There were only two companies (one in 2004 and one in 2005) that reported only IT control 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, 2005 and 2006

<table>
<thead>
<tr>
<th>IT Control Weaknesses</th>
<th>Keyword(s) Search (^a)</th>
<th>More restrictive search (^b)</th>
<th>Less restrictive search (^c)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Number of companies</td>
<td>% of companies identified by the search</td>
</tr>
<tr>
<td>Control Environment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policies</td>
<td>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*</td>
<td>59</td>
<td>24%</td>
</tr>
<tr>
<td>Staffing and Competency</td>
<td>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</td>
<td>26</td>
<td>11%</td>
</tr>
<tr>
<td><em>Total number of companies with either, or both, IT Control Environment weakness(es)</em></td>
<td></td>
<td>76</td>
<td>31%</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>analyze risk*; assess risk*; risk assess*; risk assessment</td>
<td>4</td>
<td>2%</td>
</tr>
<tr>
<td><em>Total number of companies with risk assessment weakness</em></td>
<td></td>
<td>4</td>
<td>2%</td>
</tr>
<tr>
<td>Information Systems and Communication and Control Activities</td>
<td>access; access rights; logical access; password*; physical access; security access; user identification</td>
<td>113</td>
<td>46%</td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
<td>Total number of companies with various weakness(es)</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Segregation</strong></td>
<td>incompatible duties; incompatible responsibility; segregate; segregation</td>
<td>79 32% 98 37%</td>
<td></td>
</tr>
<tr>
<td><strong>Total number of companies with either, or both, access or segregation weakness(es)</strong></td>
<td></td>
<td>135 55% 171 65%</td>
<td></td>
</tr>
<tr>
<td><strong>Design Issues</strong></td>
<td>accurate invoice*; assumption* used; audit trail*; complexity*; design*; disparate; do not appropriately address the requirements; functional business requirement*; functional complexity; incompatible application*; incompatible platform*; interface*; lack of adequate resources; lack of effective information system*; large number of manual process*; legacy; life cycle; manual intervention; manual performance*; manual process*; manual-intensive; non-integrated; open source; reporting limitations; reporting requirement*; track* change*; user dependence</td>
<td>79 32% 116 44%</td>
<td></td>
</tr>
<tr>
<td><strong>Development and Change</strong></td>
<td>acquisition; approval of change*; approval of the change; authorization of change*; change control; change management; changes to financial application*; changes to production application*; changes to program*; conversion; data conversion; data migration; deactivation*; development; implement*; implementation of computer application*; maintenance; maintenance control*; migration*; migrate changes to production; migration of system changes to production; placed into production; program changes; program development; set-up; system* conversion*; system* development; test*; timely deactivation</td>
<td>71 29% 109 41%</td>
<td></td>
</tr>
<tr>
<td><strong>Document</strong></td>
<td><em>adequate document</em>; <em>sufficient</em> document*; document* and test*; document* or test*; documentation; effectively document*; lack of document*; not document*; properly document*; unable to document</td>
<td>30 12% 62 24%</td>
<td></td>
</tr>
<tr>
<td><strong>Total number of companies with any, or all, design, development/change/test or document weakness(es)</strong></td>
<td></td>
<td>123 50% 174 66%</td>
<td></td>
</tr>
<tr>
<td><strong>End user computing</strong></td>
<td>cell protection; end user comput*; end-user comput*; spreadsheet*</td>
<td>86 35% 86 33%</td>
<td></td>
</tr>
<tr>
<td><strong>Total number of companies with end user computing weakness</strong></td>
<td></td>
<td>86 35% 86 33%</td>
<td></td>
</tr>
<tr>
<td><strong>General Controls</strong></td>
<td>configuration of certain settings; controls surrounding the use; deficiencies in controls over the operation of critical financial systems; effectively operated controls; general computer controls; general computing controls; general controls; ineffective information technology controls; ineffective IT controls; IT controls; IT general controls; ITC; ITGC</td>
<td>32 13% 40 15%</td>
<td></td>
</tr>
<tr>
<td><strong>Masterfiles</strong></td>
<td>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*</td>
<td>30 12% 30 11%</td>
<td></td>
</tr>
<tr>
<td><strong>Operations</strong></td>
<td>computer operation*; information systems operation*; IT operation*; operating procedure*;</td>
<td>18 7% 21 8%</td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>Operations Report*; Proper Operation*; Software Licenses*; Support Operation*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td>Backup*; Back-up*; Backup Media; Back-up Media; Disaster; Offsite; Off-site; Record* Retention; Record* Storage; Remote Location; Removable Media; Rotation Media</td>
<td>22</td>
<td>9%</td>
</tr>
<tr>
<td>Security (Other than Access)</td>
<td>Anti-virus; Encrypt*; Fire; Firewall; Network Vulnerability Assessment*; Physical Security; Uninterruptible Power</td>
<td>7</td>
<td>3%</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>Data Center*; Outsource*; 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</td>
<td>16</td>
<td>7%</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Business System; Enterprise Resource Planning; Enterprise Resource Platform; ERP; Manufacturing Resource Planning; Manufacturing Resource Platform; MRP; Oracle; SAP</td>
<td>13</td>
<td>5%</td>
</tr>
<tr>
<td>Total Number of Companies with Any, or All, General, Masterfile, Operations, Backup, Security (Other than Access), Outsourcing or ERP Weakness(es)</td>
<td>110</td>
<td>45%</td>
<td>120</td>
</tr>
<tr>
<td>Total Number of Companies with Information and Communication Control Weaknesses</td>
<td>238</td>
<td>98%</td>
<td>252</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Monitoring Adherence*; Complianc*; Dashboard*; Enforce*; Evaluate*; Examine*; IT Compliance; Monitor*; Oversight; Review*; Scrutiny; Supervise*</td>
<td>138</td>
<td>57%</td>
</tr>
<tr>
<td>Total Number of Companies with Monitoring Weakness</td>
<td>138</td>
<td>57%</td>
<td>179</td>
</tr>
<tr>
<td>Total Number of Companies with IT Weaknesses</td>
<td>244</td>
<td>263</td>
<td></td>
</tr>
<tr>
<td>Total of Detailed IT Control Weaknesses Identified Using QDA Miner Content Analysis Software</td>
<td>823</td>
<td>1098</td>
<td></td>
</tr>
<tr>
<td>Average Number of IT Control Weaknesses per Company</td>
<td>3.4</td>
<td>4.2</td>
<td></td>
</tr>
</tbody>
</table>

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

b. The more restrictive search criteria counts a company as having an end user computing, masterfile, ERP 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. The more restrictive search criteria counts a company as having the other IT weaknesses when keyword/phrases listed in the table associated with these weakness occur within the same sentence as an “IT indicator” and the sentence does not contain an “exclusion keyword/phrases”. 
c. The less restrictive search criteria counts a company as having an end user computing, masterfile, ERP and outsourcing IT weaknesses when any keyword/phrases listed as associated with these weaknesses occur anywhere in the company’s SOX 404 audit report. The less restrictive search criteria counts a company as having the other IT weaknesses when keyword/phrases associated with these weaknesses occur within the same sentence as an “IT indicator”.

d. 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; master data; master data file*; master file*; master record*; masterfile; master record*; 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 (accounting system*; application*; automated; automated process*; automated program*; computer*; computer based; computer generated; computer program*; computing; crm; data processing; end user computing; end-user computing; enterprise resource planning; enterprise resource platform; ERP; financial application*; financial application programs; financial reporting system*; general ledger system*; hardware; information processing; information system*; information technology; information technology application*; information technology systems; manufacturing resource planning; manufacturing resource platform; material resource planning software; mrp; open-source; Oracle; platform*; SAP; software; software licens*; spreadsheet*), (3) people related keywords/phrases (CIO; computing personnel; computing staff*; CTO; director of information technology; information technology personnel; information technology staff*; IT personnel; IT staff*; IT support staff*; programmer*), (4) processes and procedures related keywords/phrases (accounting process; billing process*; computer operation*; data center*; data entry; data input; information systems operation*; input; IT operation*; manual process*; operating procedure*; operations report*; outsource*; processing; processing file*; program change*; program development; proper operation*; reporting process*; SAS 70; service organization*; service provider*; Statement of Auditing Standards No. 70; support operation*; system generat*; third party organization; third party service organization; third-party organization; third-party service; transaction processing; transactional), and (5) computer control environment related keywords/phrases (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; rotation media; security access; security setting*;  

e. “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 Information and Communication 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 – IT Control Weakness Cluster Frequencies and Descriptive Statistics 2004 - 2006

#### Panel A

<table>
<thead>
<tr>
<th>IT Control Weaknesses by Grouping Categories&lt;sup&gt;c&lt;/sup&gt;</th>
<th>More restrictive search&lt;sup&gt;b&lt;/sup&gt;</th>
<th>Less restrictive search&lt;sup&gt;b&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of companies</td>
<td>% of companies</td>
</tr>
<tr>
<td>Policies</td>
<td>59</td>
<td>24%</td>
</tr>
<tr>
<td>Staffing &amp; Competency</td>
<td>26</td>
<td>11%</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>4</td>
<td>2%</td>
</tr>
<tr>
<td>Access and Segregation</td>
<td>135</td>
<td>55%</td>
</tr>
<tr>
<td>Design, Change and Documentation</td>
<td>123</td>
<td>50%</td>
</tr>
<tr>
<td>End-user computing</td>
<td>86</td>
<td>35%</td>
</tr>
<tr>
<td>Other Information and Communication</td>
<td>110</td>
<td>45%</td>
</tr>
<tr>
<td>Monitoring</td>
<td>138</td>
<td>57%</td>
</tr>
<tr>
<td>Total IT Control Weaknesses 2004-2006</td>
<td>681</td>
<td>100%</td>
</tr>
<tr>
<td>Number of Companies with IT weaknesses a</td>
<td>244</td>
<td>100%</td>
</tr>
<tr>
<td>Mean number of weaknesses per company</td>
<td>2.79</td>
<td></td>
</tr>
<tr>
<td>S.D.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skewness</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Panel B: IT Control Weaknesses 2004-2006 identified using content analysis software\textsuperscript{a}

<table>
<thead>
<tr>
<th>IT Control Weaknesses by COSO Categories\textsuperscript{c}</th>
<th>More restrictive search\textsuperscript{b}</th>
<th>Less restrictive search\textsuperscript{b}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of companies</td>
<td>% of companies</td>
</tr>
<tr>
<td>Control Environment</td>
<td>76</td>
<td>31%</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>4</td>
<td>2%</td>
</tr>
<tr>
<td>Information and Communication</td>
<td>238</td>
<td>98%</td>
</tr>
<tr>
<td>Monitoring</td>
<td>138</td>
<td>57%</td>
</tr>
<tr>
<td>Total IT Control Weaknesses 2004-2006</td>
<td>456</td>
<td>100%</td>
</tr>
<tr>
<td>Number of Companies with IT weaknesses\textsuperscript{a}</td>
<td>244</td>
<td></td>
</tr>
<tr>
<td>Mean number of weaknesses per company</td>
<td>1.87</td>
<td></td>
</tr>
<tr>
<td>S.D.</td>
<td>.77</td>
<td></td>
</tr>
<tr>
<td>Skewness</td>
<td>.39</td>
<td></td>
</tr>
</tbody>
</table>

The number of weaknesses found and the number of companies for which weaknesses were identified depends upon the keywords/phrases and search criteria used in the automated search. This panel presents search results for two different sets of automated search criteria labelled as Less Restrictive and More Restrictive (described in Table 2).
Panel C. IT weaknesses grouped within COSO groupings by year.

### More Restrictive Search Criteria details:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>% of companies</td>
<td>% of weaknesses</td>
<td>n</td>
</tr>
<tr>
<td>Control Environment</td>
<td>30</td>
<td>33%</td>
<td>17%</td>
<td>25</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>4</td>
<td>4%</td>
<td>2%</td>
<td>0</td>
</tr>
<tr>
<td>Information &amp; Communication</td>
<td>90</td>
<td>99%</td>
<td>52%</td>
<td>84</td>
</tr>
<tr>
<td>Monitoring</td>
<td>49</td>
<td>54%</td>
<td>28%</td>
<td>51</td>
</tr>
<tr>
<td>Total IT Weaknesses</td>
<td>173</td>
<td>100%</td>
<td>160</td>
<td>100%</td>
</tr>
<tr>
<td>Total number of companies</td>
<td>91</td>
<td>91%</td>
<td>87</td>
<td>87</td>
</tr>
<tr>
<td>Mean</td>
<td>1.90</td>
<td>1.90</td>
<td>1.84</td>
<td>1.84</td>
</tr>
<tr>
<td>S.D.</td>
<td>0.82</td>
<td>0.82</td>
<td>0.70</td>
<td>0.70</td>
</tr>
<tr>
<td>Skewness</td>
<td>0.56</td>
<td>0.56</td>
<td>0.23</td>
<td>0.23</td>
</tr>
</tbody>
</table>

### Less Restrictive Search Criteria details:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>% of companies</td>
<td>% of weaknesses</td>
<td>n</td>
</tr>
<tr>
<td>Control Environment</td>
<td>49</td>
<td>48%</td>
<td>22%</td>
<td>37</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>8</td>
<td>8%</td>
<td>4%</td>
<td>1</td>
</tr>
<tr>
<td>Information &amp; Communication</td>
<td>98</td>
<td>96%</td>
<td>44%</td>
<td>89</td>
</tr>
<tr>
<td>Monitoring</td>
<td>66</td>
<td>65%</td>
<td>30%</td>
<td>67</td>
</tr>
<tr>
<td>Total IT Weaknesses</td>
<td>221</td>
<td>100%</td>
<td>194</td>
<td>100%</td>
</tr>
<tr>
<td>Total number of companies</td>
<td>102</td>
<td>102</td>
<td>94</td>
<td>94</td>
</tr>
<tr>
<td>Mean</td>
<td>2.17</td>
<td>2.17</td>
<td>2.06</td>
<td>2.06</td>
</tr>
<tr>
<td>S.D.</td>
<td>0.92</td>
<td>0.92</td>
<td>0.73</td>
<td>0.73</td>
</tr>
<tr>
<td>Skewness</td>
<td>0.14</td>
<td>0.14</td>
<td>0.07</td>
<td>0.07</td>
</tr>
</tbody>
</table>
Table 4
Pairwise Associations Between IT and Non-IT Control Weaknesses in Companies with IT Weaknesses
Table Entries are p-values from Tests of Association Based on Chi-Squared

**More Restrictive Search**

| Control Environment | IT1 | IT2  | IT3 | IT4  | IT5  | IT6  | IC1  | IC2  | IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
|---------------------|-----|------|-----|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| IT1                 | 1.00| 0.013| 0.034| <.001| 0.005| 0.055| IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT2 Segregation & Access | 1.00| 0.005| <.001| 0.004| 0.047| IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT3 Design, Change and Documentation | 1.00| 0.012| 0.028| 0.096| 0.008| IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT4 End user computing | 1.00| 0.004| 0.047| IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT5 Other Information & Communication | 1.00| 0.064| IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT6 Monitoring | 1.00| 0.101| 0.076| 0.002| 0.059| 0.086| 0.029| IC1  | IC2  | IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |

**Less Restrictive Search**

| Control Environment | IT1 | IT2  | IT3 | IT4  | IT5  | IT6  | IC1  | IC2  | IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
|---------------------|-----|------|-----|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| IT1                 | 1.00| 0.003| 0.002| 0.048| 0.000| IC1  | IC2  | IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT2 Segregation & Access | 1.00| 0.061| 0.004| 0.001| IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT3 Design, Change and Documentation | 1.00| 0.012| 0.007| 0.021| IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT4 End user computing | 1.00| 0.003| 0.103| 0.069| 0.007| IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT5 Other Information & Communication | 1.00| 0.026| 0.062| 0.012| IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |
| IT6 Monitoring | 1.00| 0.000| 0.019| IC3  | IC4  | IC5  | IC6  | IC7  | IC8  | IC9  | IC10 | IC11 | IC12 | IC13 | IC14 | IC15 | IC16 | IC17 | IC18 |

Legend:

IC1. Accounting documentation, policy and/or procedures
IC2. Accounting personnel resources, competency/training
IC3. Ethical or compliance issues with personnel
IC4. Journal entry control issues
IC6. Untimely or inadequate account reconciliations
IC8. Material and/or numerous auditor /year-end adjustments
IC9. Non-routine transaction control issues
IC10. Restatement or nonreliance of company filings
IC11. Segregations of duties/ design of controls (personnel)
IC13. Scope (disclaimer of opinion) or other limitations
IC15. Senior management competency, tone, reliability issues
IC18. Ineffective or understaffed audit committee
Appendix

Illustrative Example Reports

Example Report 1

This is an example of an auditors’ report which Audit Analytics identifies as having six non-IT weaknesses (over and above IC20 that indicates IT weakness(es)), two more weaknesses than any company classified as having stronger non-IT control strength. Four of these six weaknesses - IC 2 Accounting personnel resources, competency/training; IC 6 Untimely or inadequate account reconciliations; IC 8 Material and/or numerous auditor/year-end adjustments; IC 11 Segregations of duties/design of controls (personnel) - are ones for which we found common associations with IT weaknesses across both search criteria. Consistent with this study finding, both search criteria found segregation, access, change management, end-user computing and monitoring IT weaknesses. These five IT-weaknesses, the number used to cut-off between companies with weaker and stronger IT-controls, occur in three of the four categories we found significantly associated with these four non-IT weaknesses. The policies weakness found by both search criteria and the documentation weakness found by the less restrictive criteria were ‘false hits’. The other two Audit Analytic identified non-IT weaknesses in this report, IC1 Accounting documentation, policy and/or procedures and IC9 Non-routine transaction control issues, we did not find to be significantly associated across both search criteria with the IT-weakness categories illustrated by this example.

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders
Sonic Solutions:

We have audited management’s assessment, included in the accompanying “Management Report on Internal Control Over Financial Reporting” at Item 9A.b, that Sonic Solutions did not maintain effective internal control over financial reporting as of March 31, 2005, because of insufficient qualified accounting and human resources personnel, ineffective controls over cash, fixed assets and the close process and inadequate controls over spreadsheets used in the financial reporting process, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Sonic Solutions’ 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:

The Company did not maintain sufficient personnel with an appropriate level of accounting knowledge, experience and training in the application of generally accepted accounting principles (GAAP) commensurate with its financial reporting requirements. The Company did not employ sufficient qualified personnel to plan, manage and execute the December 17, 2004 Roxio acquisition and the related purchase accounting. As a result, material errors occurred in the Company’s accounting for Roxio’s facility lease obligations and the related rent expense. In addition, material errors occurred in the Company’s classification of debt amounts in its consolidated balance sheet and in its consolidated statement of cash flows in its preparation of financial statements for the quarter ended December 31, 2004. Material errors also occurred in the Company’s consolidated statement of cash flows and footnotes in its preparation of financial statements for the year ended March 31, 2005. These errors in accounting were identified by us and were corrected prior to the filing of the Company’s financial statements on Form 10-Q for the quarter ended December 31, 2004 and on Form 10-K for the year ended March 31, 2005.

The Company did not maintain adequate controls to ensure appropriate execution of its integration plan to merge the accounting and financial reporting processes of the Roxio CSD into the Company’s existing processes. During the integration of the Roxio CSD, the Company did not maintain sufficient controls over existence, completeness and accuracy in its cash processes regarding authorization of disbursements and completion and review of bank account reconciliations; over accuracy of account balances in the close processes due to a lack of adequate review and approval of account postings and reconciliations; over accuracy of account balances related to accrued expenses; and over accuracy and completeness in its invoicing process related to shipment information received from third parties upon which the Company relies to record revenue within certain classes of customers. In addition, the Company had inadequate controls within the accounting and financial information systems over user access, segregation of duties and monitoring of information systems. As a result, material errors in accounting for accounts receivable, other current assets and accrued expenses occurred and were corrected prior to the issuance of the financial statements for the year ended March 31, 2005.

The Company did not maintain sufficient qualified personnel in its human resources and payroll functions. The Company did not maintain effective controls with respect to hiring of personnel; maintenance of employee records; payroll processing, including a lack of segregation of duties; and anti fraud measures including inadequate communication to employees of policies generally and with respect to the Company’s commitment to developing and maintaining effective internal control over financial reporting and compliance with its Code of Conduct and other corporate governance policies. As a result, material errors in accounting for compensation and related expenses could have occurred in the Company’s interim and annual financial statements.
The Company did not maintain adequate controls over accounting for the existence and valuation of fixed assets. The lack of adequate controls to ensure fixed assets records are supported by underlying invoices or other documentation, and the absence of tagging procedures and periodic physical counts, resulted in unsupported balances as well as inaccurate and incomplete data in the fixed assets listing resulting in a material error in accounting for depreciation expense for the year ended March 31, 2005. This error was corrected prior to the issuance of the financial statements for the year ended March 31, 2005.

The Company did not maintain adequate controls over spreadsheets used in its financial reporting process. The Company did not maintain sufficient controls regarding change management and access controls to prevent unauthorized modification of formulas and to detect errors in formulas. These spreadsheets are utilized to calculate and record entries to its records underlying the financial statements. As a result, material errors occurred in the allowance for returns and to the tax footnote disclosure in the annual financial statements. These errors were corrected prior to the issuance of the financial statements.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated balance sheets of Sonic Solutions and subsidiaries as of March 31, 2005 and 2004, and the related consolidated statements of operations, stockholders’ equity and comprehensive income (loss) and cash flows for each of the years in the three-year period ended March 31, 2005 and the related financial statement schedule. These material weaknesses were considered in determining the nature, timing, and extent of audit tests applied in our audit of the 2005 consolidated financial statements, and this report does not affect our report dated June 29, 2005 which expressed an unqualified opinion on those consolidated financial statements and related financial statement schedule.

In our opinion, management’s assessment that Sonic Solutions did not maintain effective internal control over financial reporting as of March 31, 2005, is fairly stated, in all material respects, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Also, in our opinion, because of the effect of the material weaknesses described above on the achievement of the objectives of the control criteria, Sonic Solutions has not maintained effective internal control over financial reporting as of March 31, 2005, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

We do not express an opinion or any other form of assurance on management’s statements referring to corrective actions taken after March 31, 2005, relative to the aforementioned material weaknesses in internal control over financial reporting.

(signed) KPMG LLP

San Francisco, California
June 29, 2005
Example Report 2:

This is an example of an auditors’ report where IT-weaknesses were not identified by search criteria which Audit Analytics characterized as having five non-IT weaknesses (over and above IC20 that indicates IT weakness(es)), one more than any company classified as having stronger non-IT controls. One reason for the lack of association of IT and non-IT weaknesses in this report is that the description of a possible IT-weakness, i.e., senior executives ability to override the controls and accounting system, does not detail IT-weaknesses that contribute to this vulnerability. Two of the non-IT weaknesses identified by Audit Analytics occurred for less than 1% of companies with IT weaknesses in the study years (IC3 Ethical and compliance issues with personnel and IC15 Senior management competency, tone, reliability issues). IC10 Restatement or nonreliance of company filings, an non-IT weakness identified by Audit Analytics for this report was not found to be significantly associated with any IT-weaknesses across both search criteria in this study. The other two non-IT weaknesses commonly occur in many of the reports (IC1 Accounting documentation, policy and/or procedures occurs and IC2 Accounting personnel resources, competency/training in 20% and 16% respectively).

Report of Independent Registered Public Accounting Firm

Board of Directors and Shareholders
BUCA, Inc. and Subsidiaries

We have audited management’s assessment, included in the accompanying management’s report on internal control over financial reporting, that BUCA, Inc. and subsidiaries (the “Company”) did not maintain effective internal control over financial reporting as of December 26, 2004, because of the effect of the material weaknesses identified in management’s assessment based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission. 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 opinions.

A company’s internal control over financial reporting is a process designed by, or under the supervision of, the company’s principal executive and principal financial officers, or persons performing similar functions, and effected by the company’s board of directors, management, and other personnel to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles (“GAAP”). 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 GAAP, 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 the inherent limitations of internal control over financial reporting, including the possibility of collusion or improper management override of controls, material misstatements due to error or fraud may not be prevented or detected on a timely basis. Also, projections of any evaluation of the effectiveness of the internal control over financial reporting to future periods are subject to the risk that the 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 significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected. The following material weaknesses have been identified and included in management’s assessment:

**Deficiencies Related to Design and Operation of Company-Level Controls as a Result of Tone Set by Senior Management.** The Company lacked an appropriate tone and a demonstrable commitment by former senior executives to set high standards of ethics, integrity, accounting, and corporate governance. These conditions resulted in a control environment that permitted the following deficiencies:

- inadequate policies and procedures to prevent senior executives from overriding existing controls and accounting systems
- inadequate procedures for proper corporate authorizations for certain expenditures and transactions, inadequate approval procedures, and poor documentation
- lack of safeguarding of the Company’s assets
- inadequate related-party and vendor procedures governing relationships, transactions, and related disclosures
- accounting practices that were not in accordance with GAAP
- lack of company policy to update accounting personnel position descriptions for proper qualifications based upon position responsibilities
- lack of company policy to review training requirements for accounting personnel on a periodic basis
- systems of internal controls and disclosure controls and procedures were not established nor were such policies and procedures communicated to employees
- assessment of financial reporting risks and monitoring of internal control did not operate effectively.

**Deficiencies Related to Design and Operation of Accounting Procedures and Application of GAAP.** Certain of the Company’s accounting control procedures, policies, and documentation were not sufficient to ensure that its financial statements were presented in accordance with GAAP. The following deficiencies were identified:

- lack of formal application of accounting policies and procedures
- lack of capitalization policy for fixed assets
- insufficient documentation to enable proper identification of certain of our disposed fixed assets
- lack of adequate procedures and oversight for appropriately assessing and applying critical accounting policies, estimates for insurance reserves and income taxes
- limited monitoring of changes to GAAP
- inadequate approval procedures and documentation
- lack of company policy to ensure significant events and transactions were brought to the attention of the accounting department for their review and, if applicable, the approval of the accounting treatment
• inadequate supervisory oversight to ensure proper application of the policies
• employees had not been trained to understand and apply the policies appropriately.

Due to (1) the material adjustments identified in the interim and year-end financial statements resulting in a restatement of the financial statements as described in Note 2 to the consolidated financial statements, (2) the significance of the deficiencies in the company-level controls and the financial closing and reporting process, and (3) the pervasiveness of the deficiencies identified in the company-level controls and financial closing and reporting process, there is a more than remote likelihood that a material misstatement of the interim and annual financial statements would not have been prevented or deleted.

These material weaknesses were considered in determining the nature, timing, and extent of audit tests applied in our audit of the consolidated financial statements as of and for the year ended December 26, 2004, of the Company, and this report does not affect our report on such financial statements.

In our opinion, management’s assessment that the Company did not maintain effective internal control over financial reporting as of December 26, 2004, is fairly stated, in all material respects, based on the criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission. Also in our opinion, because of the effect of the material weaknesses described above on the achievement of the objectives of the control criteria, the Company has not maintained effective internal control over financial reporting as of December 26, 2004, based on the criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission.

We have also audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated financial statements as of and for the year ended December 26, 2004, of the Company and our report dated July 25, 2005, expressed an unqualified opinion on those financial statements.

/s/ Deloitte & Touche LLP

Minneapolis, Minnesota
July 25, 2005
Example Report 3:

This is an example of a report with one more (6) IT-weaknesses than any company with stronger IT control and only two associated non-IT weaknesses, IC1 Accounting documentation, policy and/or procedures and IC11 Segregations of duties/ design of controls (personnel). The IT-weaknesses (related to segregation, access, change management, documentation, general controls and monitoring) were found by both search criteria. We found IC11 Segregations of duties/ design of controls (personnel) to be associated across both search criteria with segregation/access and other information and control IT-weaknesses, as is illustrated by this report.

Report of Independent Registered Public Accounting Firm
The Board of Directors and Stockholders of BioScrip, Inc.

We have audited management’s assessment, included in the accompanying Management Report on Internal Control Over Financial Reporting, that BioScrip, Inc. did not maintain effective internal control over financial reporting as of December 31, 2006, because of the effect of ineffective information technology controls, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (the COSO criteria). BioScrip, Inc.’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 weakness relating to information technology general controls has been identified and described in management’s assessment:

The Company identified a material weakness in internal control over financial reporting related to information technology general controls as a result of the aggregation of the following control deficiencies:

• Inadequate controls over the segregation of duties and restriction of employee access to applications, databases,
and operating systems;
• Ineffective controls over the documentation, testing, approval and migration of system changes to production environments; and
• Lack of monitoring controls over personnel in the information technology function with update access to the production databases supporting significant applications.

This material weakness affects the processing of information related to all significant accounts in the financial statements and could potentially result in a material misstatement to the financial statements.

This material weakness was considered in determining the nature, timing, and extent of audit tests applied in our audit of the 2006 financial statements, and this report does not affect our report dated March 15, 2007 on those financial statements.

In our opinion, management’s assessment that BioScrip, Inc. did not maintain effective internal control over financial reporting as of December 31, 2006, is fairly stated, in all material respects, based on the COSO criteria. Also, in our opinion, because of the effect of the material weakness described above on the achievement of the objectives of the control criteria, BioScrip, Inc. has not maintained effective internal control over financial reporting as of December 31, 2006, based on the COSO criteria.

/s/ Ernst & Young LLP

Minneapolis, Minnesota
March 15, 2007