2007

IT-Related Material Weaknesses in Internal Control: Initial Evidence from SOX Section 404 Reports

Dana Hermanson
Kennesaw State University, dhermans@kennesaw.edu

Daniel M. Ivancevich
University of North Carolina - Wilmington

Susan H. Ivancevich
University of North Carolina - Wilmington

IT-Related Material Weaknesses In Internal Control: Initial Evidence From SOX Section 404 Reports

Dana R. Hermanson, (E-mail: dana_hermanson@kennesaw.edu), Kennesaw State University
Daniel M. Ivancevich, (E-mail: ivancevichd@uncw.edu), University of North Carolina at Wilmington
Susan H. Ivancevich, (E-mail: ivancevichs@uncw.edu), University of North Carolina at Wilmington

ABSTRACT

Section 404 of the Sarbanes-Oxley Act (SOX) requires auditors and managers to assess public companies' internal control over financial reporting. Since some of the material weaknesses in internal control noted by auditors and management relate to IT issues, Section 404 reports offer a new opportunity to examine the types of IT-related control issues that public companies are struggling to address. This study presents a summary of the most commonly cited IT-related material weaknesses in internal control described in recent Section 404 internal control reports and describes the characteristics of companies with IT-related weaknesses. We also provide insights into companies' remedial actions to correct their IT control weaknesses.

INTRODUCTION

The Sarbanes-Oxley Act (SOX) was passed in 2002 to address a variety of problems in the U.S. financial reporting system, including questionable auditor independence, a lack of focus on internal controls, and weak corporate governance. These problems were most profound in companies such as Enron and WorldCom, which engaged in massive accounting frauds and shook the faith of U.S. investors.

One of the most meaningful and hotly-debated sections of SOX is Section 404 on internal controls. Effective for all but the smallest public companies as of November 2004, Section 404 requires external auditors to test their clients' internal control over financial reporting and to issue an audit opinion on internal controls.[1] If a client has a "material weakness" in its controls, then the auditor's opinion must describe the nature of the weakness. Management also issues a report on internal controls, discussing material weaknesses and often remedial steps taken to correct such weaknesses. Section 404 has proved to be quite costly for companies and their auditors, but many have argued that it has created substantial benefits.

From an IT perspective, the Section 404 reports offer a new opportunity to examine the types of IT-related control issues that public companies are struggling to address, since some of the material weaknesses noted by auditors and management relate to IT issues. Hoffman (2005) states that several IT experts expect many public companies to have IT-related material weaknesses in internal control, with more trouble in smaller companies. He also notes that a *Compliance Week* analysis of 2004 audit reports found that 3.5% of material weakness disclosures cited IT-related issues. While IT-related material weaknesses have received some attention in the business press, we are not aware of any academic research that has analyzed the specific categories of IT weaknesses cited in Section 404 reports and the characteristics of companies with such weaknesses.

This study presents a summary of the most commonly cited IT-related material weaknesses described in recent internal control reports and describes the characteristics of companies with IT-related weaknesses. We also

[1] Section 404 is not yet effective for "non-accelerated filers," essentially companies with public float under $75 million. These represent the smallest public companies.

provide insights into companies' remedial actions to correct their IT control weaknesses. We believe that the results will be of interest to IT professionals, auditors, and managers.

SOX SECTION 404 AND MATERIAL WEAKNESSES

Prior to the passage of SOX, external auditors expressed an opinion on the fairness of the company's financial statements, but they were not required to test the company's internal control over financial reporting. In other words, auditors tested the output of the financial reporting process (the financial statements), but not the process itself (the controls in place to promote reliable reporting). SOX Section 404 now requires the auditor to test and express an opinion on the client's internal control over financial reporting. Thus, the auditor now tests both the output and the process. The underlying logic is that companies with stronger internal controls should be less likely to commit fraud or have unintentional errors in their financial statements.

Under PCAOB Audit Standard No. 2 (the external auditor's guidance for how to comply with Section 404), auditors may identify three levels of internal control weaknesses as they test the client's controls (quoted from AS No. 2, PCAOB 2004):

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the company's annual or interim financial statements that is more than inconsequential will not be prevented or detected.

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.

Material weaknesses represent the most serious type of internal control problem. As a result, the details of material weaknesses are publicly disclosed in the auditor's report, as well as discussed in a companion report on internal controls from management. When companies have one or more material weaknesses, they receive an adverse audit opinion from the external auditor (i.e., signifying that the internal controls were not effective).

LITERATURE AND MOTIVATION

With the relatively recent implementation of SOX, there is little published research on material weakness disclosures. Ge and McVay (2005) examine material weakness disclosures in SOX Section 302 filings from August 2002 to November 2004.[2] Of the 493 material weaknesses analyzed, 14 (2.8%) reflected technology issues. The examples of technology issues related to access controls, documentation, and need for formal policies.

Raghunandan and Rama (2006) examine the relation between Section 404 disclosures in 2005 and external audit fees. While not the focus of their study, the authors disclose that seven (12%) of their 58 sample companies with material weaknesses have problems related to information systems.

These studies provide evidence that some companies have IT-related material weaknesses in internal control. However, neither study provides a detailed analysis of a large sample of IT-related weaknesses in Section 404 disclosures. Our goal is to provide such an analysis so that IT professionals and others can better understand the IT-related control challenges facing U.S. public companies.

[2] Section 302 was effective before Section 404 (August 2002) and requires management to describe material weaknesses in internal controls.

METHOD

To provide insight into the types of IT weaknesses cited in 404 reports, we conducted a search using the Audit Analytics database (http://www.auditanalytics.com). Specifically, we searched for adverse 404 audit reports that involved a material weakness(es) related to "information technology, software, security and access issues." Our search was conducted on January 30, 2006 and yielded 121 companies with IT-related material weakness disclosures, primarily involving 2004 fiscal year audits.

For these 121 companies, we consulted the companies' relevant 10-K to obtain the auditor's opinion on internal controls, as well as management's report on internal controls. We analyzed these reports to determine and classify the specific nature of the IT-related weaknesses. Each material weakness was classified into one of our categories (see Table 2 below), with care taken (a) to capture the most important element of the weakness and (b) to be consistent in coding similar weaknesses at different companies. While the coding is necessarily judgmental, it was performed by one of the co-authors with extensive experience in accounting systems education and research. The co-author took great care to ensure coding accuracy and consistency.

In a few cases, we excluded a company designated by Audit Analytics as an IT weakness firm because the 10-K did not disclose such issues. Apparently, Audit Analytics uses subsequent Section 302 disclosure control filings in classifying certain firms.[3] Our final sample includes 109 companies with 254 IT-related material weaknesses. For these 109 companies, we also gathered financial and other data from Audit Analytics ($n \leq 98$ for financial variables due to missing observations).

RESULTS

Description Of Sample

Table 1 presents descriptive information on our 109 sample companies. As shown in Panel A, the companies are relatively small, with median market value, revenues, and assets in the $200 million range (consistent with predictions in Hoffman (2005)).[4] The median company has a small net loss for the year.[5]

Panel B presents the industry distribution of the sample. We find a concentration of companies in the manufacturing and service sectors. Of particular note is that 19 companies are in the 737X SIC code (programming, software, and systems design). Most of the sample companies are audited by Big 4 or other large national CPA firms (see Panel C), with only 20 companies audited by other firms. Finally, the companies' audit fee typically is slightly over $1 million per year, with another $100,000 paid for non-audit services (Panel D).

Table 1
Sample Description
(n = 109)
Panel A: Financial Characteristics ($000s)

	Mean	Median
Market Value (n = 97)	702,211	213,153
Revenues (n = 98)	878,214	179,771
Assets (n = 98)	1,949,406	214,399
Net Income (n = 98)	-14,297	-1,478

[3] In addition, we consulted with Audit Analytics regarding some companies' weaknesses. Audit Analytics concluded that four companies were improperly coded in their database as having IT-related weaknesses.

[4] In the final sample of 109 companies, 82 have a 2004 year-end (80 of these are 12/31/04). The other 27 companies have 2005 year-ends, ranging from January to October.

[5] Note that companies with under $75 million in public float are not yet subject to Section 404, so our analysis addresses only companies over $75 million.

Panel B: SIC Codes

	N
1000-1999 Mining and Construction	2
2000-3999 Manufacturing	39
4000-4999 Transportation and Communication	14
5000-5999 Wholesale and Retail	12
6000-6999 Financial, Insurance, and Real Estate	9
7000-8999 Services	33
Total	109

Panel C: Audit Firm

	N
BDO Seidman	10
Deloitte and Touche	11
Ernst & Young	10
Grant Thornton	15
KPMG	21
PricewaterhouseCoopers	22
Other	20
Total	109

Panel D: Audit Fees ($000s)

	Mean	Median
Audit Fee (n = 104)	3,501	1,235
Total Non-Audit Fees (n = 104)	491	112

Table 2
Material Weaknesses In Internal Control
Panel A: Number Of Material Weaknesses Per Company

	Mean	Maximum
IT-Related Material Weaknesses	2.33	7
All Material Weaknesses	4.75	18

Panel B: Types Of IT-Related Material Weaknesses

	N
Access Controls	72
Change Management	32
Documentation	18
Spreadsheet Controls	16
Disaster Recovery Plan	15
Segregation of Duties	15
Application Controls	7
Other	79
Total	254

Analysis Of Material Weaknesses

Table 2 presents information on material weaknesses per company and on the most commonly-cited IT weakness categories. As shown in Panel A, most companies in the sample have multiple IT-related material weaknesses (average of 2.33 per company, with a maximum of seven per company). The sample companies also tend

to have other, non-IT material weaknesses as well. The average number of *total* material weaknesses per company is 4.75, with a maximum of 18 material weaknesses in one company.

Panel B of Table 2 presents the most common types of IT-related material weaknesses. Issues involving access controls dominate the list, followed by change management, documentation, spreadsheet controls, disaster recovery plans, segregation of duties, and application controls. Common problems and remedial steps in each of these areas are discussed below.

Access Controls

The overwhelming majority of access control weaknesses involved unauthorized access to applications, programs, and data. Employees often had access to systems, programs, and data outside of their assigned responsibilities, including the ability to initiate transactions inconsistent with their job responsibilities. Such instances were clear violations of proper segregation of duties.[6] Typically, the inadequate controls over access related to financial applications and data. In fact, several companies cited "unlimited access" to such areas. In some situations, inappropriate personnel were given system administrator rights to programs and data. Other violations noted were lack of periodic independent review of access, lack of policies and procedures over access, lack of independent monitoring of access, inadequate password control (e.g., not requiring regular password changes), lack of monitoring of security violations, failing to remove access rights for terminated employees, and lack of review of user access profiles. Computer Network Technology's report offers an interesting view of a material weakness because the weakness actually resulted in material financial misstatements:

The Company's information technology access controls were not designed to prevent Company personnel from accessing inventory accounting information and initiating erroneous accounting entries affecting amounts recorded as finished goods inventory. Specifically, this deficiency contributed to the aforementioned material misstatements in the Company's interim and annual financial information.

Remedial efforts to address access control weaknesses involved such steps as increasing executive involvement; improving segregation of duties; creating audit trails (logs of unauthorized access); limiting user access; enhancing monitoring; requiring regular password changes; implementing new systems, including ERP systems and associated controls; hiring new personnel (both high level and staff positions) to solidify internal control; periodically reviewing access rights; and establishing an IT infrastructure to ensure segregation of duties. Computer Network Technology offered the following remediation for its access control weaknesses:

Management has redesigned information technology access controls to restrict access to information technology programs and data that may be used to adjust finished goods inventory amounts. Implementation of this procedure will help ensure that potential inventory reconciling item adjustments are properly authorized.

Change Management

Many of the disclosures related to weaknesses in change management (changes to systems) broadly cited controls over change management. Of those disclosures providing greater detail, control over authorization and testing of changes was most commonly mentioned. Other cited weaknesses include change management policies not being well defined or well implemented, weaknesses in tracking and monitoring of changes to systems, and lack of proper documentation of the change management process. Descriptions of remedial efforts in the change management area addressed such items as tracking and monitoring of changes, improved controls to ensure changes are authorized and adequately tested, and better documentation. Many companies did not specifically describe their remedial efforts in this area.

[6] As noted above, each material weakness was classified into only one of our categories to reflect the primary element of the weakness. Access issues that also reflect segregation of duties typically were coded as access issues.

Documentation

Material weakness disclosures in this area all cited a lack of adequate documentation. Specific areas in which documentation was lacking include controls, business cycles, key processes, system usage and maintenance, financial reporting, IT policies and procedures, change management, access privileges, application systems, backup policies, general security, acceptable use policies, general IT controls, roles and responsibilities of IT function, security, and disaster recovery plans. Most companies did not specify remedial efforts in this area, but of those that did, each mentioned that the company was completing or updating its documentation.

Spreadsheet Controls

Most disclosures in this area referred generically to a lack of adequate controls (or ineffective controls) over spreadsheets, sometimes with reference to spreadsheets used in financial reporting. Other more specific disclosures cited such issues as inadequate controls related to calculation accuracy and prevention of unauthorized changes, inadequate controls regarding access to spreadsheets and changes made to spreadsheets, and problems with controlling versions of spreadsheets and protecting cells. Many companies did not describe their remedial actions, but some remedies included adding controls, converting to a new IT process, hiring outside help or additional employees, or implementing new end-user computing policies.

Disaster Recovery Plans

Disclosures in the disaster recovery plan (DRP) area cited such problems as a lack of a DRP, inappropriate backup and recovery processes, inadequate testing and documentation of the DRP, inadequate monitoring of backup and recovery processes to ensure the DRP is operating effectively, inadequate security over disaster backup and recovery, inadequate controls over backup and recovery, and keeping backups on site rather than offsite. IPIX Corporation was a particularly interesting example because the company did not perform monthly or yearly backups of its key systems, as noted below:

The Company did not maintain effective control related to its computer data backup and restore practices. The Company does not perform data backups onto removable media (e.g., tape or portable disk) which are then stored offsite. The Company did not perform and retain month-end or year-end data backups of any of its computer systems including the accounting and financial systems. This deficiency could result in the Company not being able to successfully restore critical databases to a recent point in time, thereby causing serious delays or even incorrect data in the financial reporting system.

Remedial activities in the DRP area included developing a formal disaster recovery plan, implementing / re-implementing disaster backup and recovery processes, adding a hot site to use in case of a disaster, adding document retention policies, improving the documentation of the DRP, and hiring additional IT personnel.

Segregation of Duties

The primary issue here was a lack of segregation of duties primarily in the IT and accounting functions. For example, the weakness at Annuity & Life Re (Holdings), Ltd. was described as follows:

The Company's Director of Information Technology serves as the Company's computer network administrator, possessing the highest level of security access over the Company's computer network. He also provides database support, including the electronic translation of data provided to the Company by its ceding companies, to the Company's Reinsurance Administration Actuary and Chief Actuary. Under the COSO Standards, this lack of segregation of duties is defined as a material weakness.

Zoltek Companies, Inc. had the following situation:

The Company did not maintain effective controls over segregation of duties (both manual and automated), including access to financial applications and data. Specifically, certain financial accounting, reporting and information technology personnel had unrestricted access to financial applications and data, without independent monitoring, that allowed the creation, review, and processing of financial data without independent review and authorization for (i) purchases and payables, (ii) payroll, (iii) debt and related interest expense, (iv) revenue and accounts receivable, (v) fixed assets, and (vi) inventory.

Many companies did not describe their remedial efforts, but some mentioned increasing their staffing and / or reassigning staff, implementing manual controls (review, approval, reconciliation, etc.), restricting access to systems, implementing an IT infrastructure, and hiring an outside consultant to improve controls.

Application Controls

Disclosures in this area either were generic, or they were specific to particular applications used by the company, such as billing, general ledger, and inventory. For instance, Warwick Valley Telephones had the following weakness:

The Company did not maintain effective controls over the design of its general ledger application. Specifically, the design of the general ledger application allows users to post adjusting journal entries to closed periods. This control deficiency did not result in audit adjustments to the Company's interim or annual consolidated financial statements. However, this control deficiency could result in a misstatement of significant accounts and disclosures that would result in a material misstatement to the Company's 2004 interim or annual consolidated financial statements that would not be prevented or detected.

While many companies did not specify remedies to weaknesses in application controls, those that did most often cited increased testing, improved processes and changes to controls.

CONCLUSION

SOX Section 404 reports provide important new insights into companies' internal control weaknesses, including material weakness related to IT. We examine disclosures of 109 companies' IT-related material weaknesses. We find that companies with IT-related material weaknesses are relatively small, often manufacturing or service companies, and typically are audited by Big 4 or national CPA firms. Analysis of specific deficiencies reveals particular problems with access controls and change management at many companies, and many of the companies appear to have responded vigorously to correct their IT-related material weaknesses.

We believe that the attention brought to IT-related weaknesses by Section 404 efforts ultimately will lead to stronger IT controls in U.S. public companies. Going forward, we encourage research on IT-related material weaknesses in the smallest public companies (non-accelerated filers) once Section 404 becomes effective for this segment of the market. In addition, we encourage smaller public companies to focus particular attention on access controls and change management, where many companies currently are struggling to ensure control effectiveness.

REFERENCES

1. Ge, W. and S. McVay. 2005. The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. *Accounting Horizons* (September): 137-158
2. Hoffman, T. 2005. IT role in Sarb-Ox problems is unclear. *Computerworld* (Feb. 7): 14.
3. Public Company Accounting Oversight Board (PCAOB). 2004. *Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Conducted in Conjunction With an Audit of Financial Statements*. Washington, DC: PCAOB.

4. Raghunandan, K. and D. V. Rama. 2006. SOX Section 404 material weakness disclosures and audit fees. *Auditing: A Journal of Practice & Theory* (May) : 99-114.
5. Sarbanes, P. and M. Oxley (SOX). 2002. *The Sarbanes-Oxley Act of 2002*. Washington, DC: U.S. Congress.

NOTES