

6-2011

Audit Committees Oversight of Information Technology Risk

Linda M. Hadden
Keene State College

Dana Hermanson
Kennesaw State University, dhermans@kennesaw.edu

F. Todd DeZoort
The University of Alabama, tdezoort@cba.ua.edu

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/facpubs>



Part of the [Management Information Systems Commons](#)

Recommended Citation

Hadden, Linda M.; Hermanson, Dana; and DeZoort, F. Todd, "Audit Committees Oversight of Information Technology Risk" (2011). *Faculty Publications*. 4165.
<https://digitalcommons.kennesaw.edu/facpubs/4165>

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Faculty Publications by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Audit Committees' Oversight Of Information Technology Risk

Linda B. Hadden (E-mail: lhadden@keene.edu), Keene State College
Dana R. Hermanson (E-mail: Dana_Hermanson@coles2.kennesaw.edu), Kennesaw State University
F. Todd DeZoort (E-mail: tdezoort@cba.ua.edu), The University of Alabama

Abstract

This exploratory study examines the role of the audit committee in overseeing information technology (IT) risk. We address the degree of audit committee oversight of specific IT risks, as well as factors associated with variations in audit committee IT oversight. Based on responses from 39 audit committee members, we found (1) little audit committee emphasis on oversight of IT risks, (2) audit committees involved with IT oversight focus on more traditional risks (e.g., monitoring), while very little attention is devoted to IT acquisition and implementation, and (3) the amount of IT oversight is positively associated with the responding members' auditing experience and prior familiarity with the COBIT model for assessing IT risks. Audit committee independence, diligence, and expertise, company size, and industry were not significantly associated with IT oversight.

1.0 Introduction

Increased reliance on information technology (IT) exposes companies to a variety of new risks. Managing these risks requires the efforts of various parties within the organization, including the board of directors (Horton et al. 2000; NACD 2001a). At the board level, the audit committee generally takes the lead in overseeing many key business risks (NACD 2000; POB Panel 2000). While expectations of audit committees have risen dramatically in recent years (e.g., BRC 1999; NACD 2000; Sarbanes-Oxley 2002), little is known about the audit committee's role in overseeing IT risks.

This preliminary study explores the audit committee's role in overseeing IT risks. We address the extent to which audit committees oversee the IT risk domain, the specific IT risks considered, and the factors associated with variations in oversight among audit committees. Using the COBIT model for addressing IT risks, we developed a survey to assess audit committee members' perceptions of their oversight of 34 specific IT risks.

Based on responses from 39 audit committee members, we found (1) little audit committee emphasis on oversight of IT risks, (2) audit committees involved with IT oversight focus on more traditional risks (e.g., monitoring), while very little attention is devoted to IT acquisition and implementation, and (3) the amount of IT oversight is positively associated with the responding members' auditing experience and prior familiarity with the COBIT model for assessing IT risks.

The remainder of the paper is organized as follows. The next section provides background information and our specific research questions. The third section describes our research method. The fourth section presents the results, followed by our conclusions and suggestions for future research.

Readers with comments or questions are encouraged to contact the authors via email.

2.0 Background and Research Questions

Prior research on IT risk identification and assessment has focused on the internal audit function. For example, Hermanson et al. (2000) found that internal auditors emphasized traditional IT risks and controls (e.g., safeguarding IT assets, processing applications, and ensuring data integrity, privacy and security). Alternatively, systems development and acquisition risks received the least attention from internal auditors. The authors found that several factors were associated with internal auditors' IT oversight, including "the nature of the audit objective, the prevalence of computer audit specialists on the internal audit staff, and the existence of new computerized systems" (39).

IT risk management research at the board level is scarce and limited in scope to a focus on information security risks. The National Association of Corporate Directors (NACD 2001a) surveyed corporate directors and board advisors to assess companies' reliance on IT and companies' experiences with information security breaches. The results revealed that many boards address information security, but that there was "room for improvement" (NACD 2001a, 3). The participants indicated that approximately half of the companies delegated responsibility for information security oversight to the audit committee. While these findings contribute to our understanding of board and audit committee oversight in this area, information security represents only one of several IT risks. The role of the board and its committees with respect to other IT risks remains unexplored.

As a subcommittee of the board of directors, the audit committee typically is charged with the risk oversight function of the corporation (NACD 2000). Specifically with regard to IT risks, the POB Panel on Audit Effectiveness (2000, 67) recommends that audit committees "promote candid discussions...on significant information system risks, including those related to any specific regulations or issues."

Although considerable research exists on audit committees (see DeZoort et al. (2002) for a synthesis of the literature) and the scope of audit committee oversight (e.g., Wolnizer 1995; DeZoort 1997), no study addresses the audit committee's role in monitoring IT risks. This study provides an initial examination of audit committee oversight in the area using the COBIT framework to organize the research.

Control Objectives for Information and Related Technology (COBIT 2000) is a comprehensive framework for addressing IT risks that is widely accepted in practice. First released in 1996 by the Information Systems Audit and Control Foundation, COBIT combines existing comprehensive business control models (e.g., COSO) with specialized IT control models (<http://www.isaca.org>). The COBIT framework includes 34 high-level control objectives and 318 detailed objectives developed through extensive research. COBIT is becoming internationally recognized as the authoritative source on IT governance, IT control objectives, and IT audit used in a variety of applications by private industry, public accounting firms, governments and academia (Lainhart 2000).

2.1 Research Questions

We address five research questions in this initial study of audit committee oversight of IT risk. First, we assess whether audit committees appear to provide any oversight in the IT domain. Second, we assess where audit committees focus their attention – for example, on "traditional" IT risks (e.g., monitoring) or on such areas as acquisition and implementation of IT.

Third, we evaluate whether audit committee independence, diligence, and expertise are related to perceptions of IT risk oversight within audit committees. Prior research on audit committees provides evidence that these three focal characteristics can affect audit committee activities and performance (e.g., McMullen and Raghunandan 1996; Beasley et al. 2000; DeZoort et al. 2002).

Fourth, we explore the effect of the responding audit committee members' expertise on perceived oversight of IT risks. Prior audit committee research (e.g., DeZoort 1998; DeZoort and Salterio 2001) highlights the importance of experience and knowledge on member oversight and task performance.

Finally, we explore the effects of company size and industry on perceptions of audit committee oversight of IT risk. Prior research on internal controls (e.g., DeAngelo 1981; Ivancevich et al. 1998) addresses the link between company size and focus on control, typically finding more extensive controls in larger companies. Researchers (e.g., Beasley et al. 2000; Carcello et al. 2002) also have explored industry effects on audit committee activity, finding relatively high levels of audit committee activity in industries such as financial services.

Stated formally, the research questions are:

1. To what extent do audit committee members perceive their audit committee provides oversight of IT risks?
2. Which specific IT risk areas receive the greatest attention from audit committees?
3. Does perceived audit committee oversight of IT risks vary with the independence, diligence, and/or expertise of the audit committee members?
4. Does perceived audit committee oversight of IT risks vary based on the expertise of the responding audit committee members?
5. Does perceived audit committee oversight of IT risks vary based on company size and industry?

3.0 Method

3.1 Survey

We developed a survey using the 34 high-level control objectives specified in the COBIT model (see Appendix). Audit committee members were asked to provide information regarding the largest public company on whose audit committee they served. We did not retain information that would allow us to identify the individual participants or the companies reflected in their responses.

A majority of the survey questions pertained to the members' perceptions of their audit committee's involvement in the oversight of IT risk. While the questions were based on the assumption that the audit committee provides IT risk oversight, the participants were given the opportunity to state whether the audit committee was formally responsible for monitoring this domain. Several questions focused on management's, the internal auditor's, and the external auditor's commitment to managing IT risk. In addition, the participants were asked to self-assess their qualifications for overseeing IT risk. The survey concluded with a demographics section.¹

3.2 Sample

The KPMG Audit Committee Institute mailed 1,000 surveys to directors and audit committee members on our behalf. A second mailing was sponsored by the Corporate Governance Center.² In an effort to maximize response rate, several procedures supported by Dillman (2000) were performed, including (a) offering a copy of the results to the participants, (b) using pre-stamped return envelopes and Likert scales to promote responses, and (c) having the study sponsored by (and cover letters included from) the KPMG Audit Committee Institute and the Corporate Governance Center.

We received 39 usable responses from audit committee members and had 50 sets of materials undeliverable. An exact response rate cannot be calculated because the ACI's confidential mailing list contained a mix of "non-audit committee member directors" (not of interest to us) and audit committee members (of interest to us). Based on additional information obtained from the ACI, it appears that audit committee members may comprise roughly 40% of the 1,000 person list. Accordingly, we estimate our response rate at approximately 10%.³

While some audit committee studies in the accounting literature (e.g., Kalbers and Fogarty 1993) have experienced response rates over 20%, we believe that the present study's response is reasonable given the length of the survey, the timing of the mailings (i.e., during 2002), and the likelihood of reduced interest because many audit committees apparently do not address IT risks in a specific manner. However, we do recognize the important potential limitation of the response and believe that the results should be interpreted with caution.⁴

3.3 Model

The following ordinary least-squares regression model is used to address Research Questions 3-5:

$$ACITOV = f(INDEP, FREQM, ACITEX, YRSAUD, COBEXP, LOGSALES, FINSVCS).$$

- **ACITOV (Audit committee IT oversight).** The dependent variable is measured using the COBIT model. A scale of 1 (no oversight) to 7 (heavy oversight) is used to assess the audit committee's perceived role in overseeing each of the 34 control objectives. The variable ACITOV is calculated using the mean of the 34 control objectives (another method is explored later).
- **INDEP (Audit committee independence).** This independent variable is measured as the percentage of members of the audit committee who are independent, outside directors (i.e., non-management, without other affiliations to the company).
- **FREQM (Frequency of audit committee meetings).** This independent variable is a measure of board diligence and refers to the number of audit committee meetings held in the most recent year as specified in the questionnaire.
- **ACITEX (Audit committee IT expertise).** This independent variable is a measure of the full audit committee's level of IT expertise. Participants rated fellow audit committee members' qualifications to oversee IT risks on a scale from 1 = not at all qualified to 7 = highly qualified, a perception-based measure.
- **YRSAUD (Years of audit experience).** This independent variable measures the responding audit committee member's years of auditing experience.
- **COBEXP (Prior exposure to COBIT model).** This independent variable measures the responding audit committee member's prior experience with the COBIT model on a scale from 1 = none to 7 = considerable.
- **LOGSALES (Natural log of sales).** This independent variable refers to company size. It is measured as the natural log of sales, expressed in millions.
- **FINSVCS (Financial services).** This independent variable refers to whether a company is classified within the financial services industry (1 = financial services, 0 otherwise).

4.0 Results

4.1 Demographics and Descriptive Statistics

Table 1 presents demographics and descriptive statistics on the model variables. The responding audit committee members generally are older males with nine years of audit committee experience. On average, the participants currently served on 1.80 audit committees.⁵

On average, audit committee oversight of IT risks appears quite limited (Research Question 1), as the mean of ACITOV was 2.38 on a scale from 1 = no oversight to 7 = heavy oversight. Overall, it appears that audit committees provide limited oversight of IT risks.

The companies' audit committees were primarily independent, and the average committee met five times per year. The participants rated their fellow audit committee members' IT expertise as moderate (mean of 3.54 on a scale from 1 = not at all qualified to 7 = highly qualified). The participants had an average of 2.97 years of audit experience, and most did not have prior familiarity with the COBIT model.

Finally, average revenues for the samples companies were \$819 million (mean of LOGSALES was 6.14). Thirteen percent of the companies were in the financial services industry.

Table 1: Demographics and Descriptive Statistics (n = 39)

Audit committee member age:	
Under 50	13%
50-59	36%
60-69	36%
70 or over	15%
Audit committee member gender	95% male 5% female
Mean total years of audit committee service	9.16
Mean number of audit committees on which participants serve	1.80
Means of model variables:	
ACITOV	2.38
INDEP	91.56
FREQM	5.00
ACITEX	3.54
YRSAUD	2.97
COBEXP	1.59
LOGSALES	6.14
FINSVCS	0.13

Legend:

ACITOV = Average level of audit committee IT oversight across 34 specific risk areas (scale from 1 = no oversight to 7 = heavy oversight)
 INDEP = Percentage of independent outside directors serving on AC
 FREQM = Number of AC meetings held in the most recent year
 ACITEX = Full audit committee’s level of IT expertise (scale from 1 = not at all qualified to 7 = highly qualified)
 YRSAUD = Responding audit committee member’s years of audit experience
 COBEXP = Responding audit committee member’s prior experience with COBIT (scale from 1 = none to 7 = considerable)
 LOGSALES = Company size measured as the natural log of sales, first expressed in millions
 FINSVCS = 1 if company is classified within financial services industry, else 0

4.2 Correlation Matrix

Table 2 presents a correlation matrix for the model’s dependent and independent variables. Four correlations were greater than 0.50. Audit committee IT oversight is positively correlated with the respondents’ prior familiarity with COBIT (0.67), the frequency of audit committee meetings (0.52), and audit committee IT expertise (0.52). In addition, companies with greater audit committee IT expertise had more frequent audit committee meetings (correlation of ACITEX and FREQM was 0.57).⁶

4.3 IT Oversight of Specific Control Objectives

The Appendix presents the mean rating for each of the 34 control objectives, as well as group means for each of the four business processes (Research Question 2). Overall, it appears that audit committees place the greatest emphasis on the Monitoring area (overall mean of 3.12) and the least emphasis on Acquisition and Implementation (mean of 1.99). This concentration of effort appears consistent with the focus of internal auditors. Hermanson et al. (2000) found that internal auditors primarily addressed more traditional IT risks, while systems development and acquisition received the least attention.

Table 2 Correlation Matrix (n = 39)

	ACITOV	INDEP	FREQM	ACITEX	YRSAUD	COBEXP	LOGSALES
INDEP	0.29						
FREQM	0.52	0.36					
ACITEX	0.52	0.26	0.57				
YRSAUD	0.28	0.06	0.18	0.05			
COBEXP	0.67	0.12	0.46	0.48	-0.05		
LOGSALES	0.17	0.15	0.11	-0.12	0.02	0.26	
FINSVCS	0.39	0.17	0.44	0.19	-0.06	0.45	0.01

Legend:

ACITOV = Average level of audit committee IT oversight across 34 specific risk areas (scale from 1 = no oversight to 7 = heavy oversight)
 INDEP = Percentage of independent outside directors serving on AC
 FREQM = Number of AC meetings held in the most recent year
 ACITEX = Full audit committee’s level of IT expertise (scale from 1 = not at all qualified to 7 = highly qualified)
 YRSAUD = Audit committee member’s years of audit experience
 COBEXP = Audit committee member’s prior experience with COBIT (scale from 1 = none to 7 = considerable)
 LOGSALES = Company size measured as the natural log of sales, first expressed in millions
 FINSVCS = 1 if company is classified within financial services industry, else 0

4.4 Regression Results

Table 3 presents the results of estimating the OLS regression model (Research Questions 3-5). The model has significant explanatory power (adjusted $R^2 = 53\%$, $F = 7.18$, $p = .00$). Two of the independent variables of interest (YRSAUD and COBEXP) were significantly related to ACITOV.⁷

Table 3 Regression Results, Dependent Variable = ACITOV (n = 39)

Variable	Estimate	t-stat.	p-value
Intercept	0.172	0.17	0.86
INDEP	0.008	1.11	0.28
FREQM	0.026	0.24	0.81
ACITEX	0.116	1.19	0.24
YRSAUD	0.051	2.47	0.02
COBEXP	0.498	3.47	0.00
LOGSALES	0.013	0.10	0.92
FINSVCS	0.170	0.72	0.48
Model F	7.18		
p-value	0.00		
Adj. R^2	0.53		

Note: All p-values are two-tailed.

Legend:

ACITOV = Average level of audit committee IT oversight across 34 specific risk areas (scale from 1 = no oversight to 7 = heavy oversight)
 INDEP = Percentage of independent outside directors serving on AC
 FREQM = Number of AC meetings held in the most recent year
 ACITEX = Full audit committee’s level of IT expertise (scale from 1 = not at all qualified to 7 = highly qualified)
 YRSAUD = Audit committee member’s years of audit experience
 COBEXP = Audit committee member’s prior experience with COBIT (scale from 1 = none to 7 = considerable)
 LOGSALES = Company size measured as the natural log of sales, first expressed in millions
 FINSVCS = 1 if company is classified within financial services industry, else 0

First, ACITOV is positively related to the participants' personal audit experience (YRSAUD, $p = 0.02$). Audit experience may sensitize audit committee members to the importance of risk assessment, particularly risks associated with computerized information systems. Such a focus on risks could influence the entire audit committee to focus greater attention on oversight of IT risks.

Second, the responding audit committee members' prior familiarity with COBIT (COBEXP, $p = 0.00$) was positively associated with ACITOV. This variable may reflect the participants' exposure to or knowledge of IT risk assessment, which may in turn influence the audit committee to focus greater attention on oversight of IT risks.

None of the other variables was significantly associated with ACITOV. As a result, prior linkages between internal control / audit committee oversight and such factors as audit committee independence, diligence, and expertise, company size, or industry do not appear to extend to the IT oversight domain. In this context, based on this one study, it appears that the responding audit committee members' expertise and experience are the primary factors associated with audit committee IT oversight.

4.5 Other Analyses

We performed four other analyses related to Table 3. First, the participants indicated whether the audit committee was expressly charged with oversight of IT risks. A variable coded 1 = audit committee has formal responsibility for IT oversight, 0 otherwise, was added to the model. The results in Table 3 were unaffected, and the new variable was not significantly associated with IT oversight ($p = 0.70$)

Second, we considered several other measures of the participants' expertise – self-assessed personal qualifications to oversee IT risks, years of IT experience, years of audit committee experience, years of accounting experience, and years of director experience. When added to the model, none was significantly related to ACITOV. The other results were fairly consistent with those presented in Table 3; however, in two cases the p -value on YRSAUD was greater than 0.05 (0.07 in one case and 0.15 in another). The 0.15 level occurred when years of accounting experience was added to the model.

Third, before addressing the 34 COBIT objectives, the participants were asked: (1) "What role does your audit committee play in overseeing IT risk?" and (2) "What role should your AC play in overseeing IT risk?" We ran two additional models, replacing ACITOV with the response to each of these questions. In both instances, the overall regression model was insignificant ($p > 0.05$).

Finally, in the COBIT model, the 34 individual control objectives are divided into four business processes (see Appendix). As an additional analysis, we ran four regression models, each time replacing the dependent variable ACITOV (the mean of the 34 control objectives) with the mean rating within one of the business processes. For example, the first model run used the mean of the 11 items in Planning and Organization as the dependent variable. YRSAUD and COBEXP each were significantly associated with oversight in three of the four models ($p \leq 0.06$). Overall, it appears that the results within the four business processes are reasonably consistent with the overall results presented in Table 3.

5.0 Discussion and Conclusions

This exploratory study examined the audit committee's role in overseeing IT risks. IT risks are a major component of risk management because an organization's information is among its most vital assets and is paramount to the organization's success (Horton et al. 2000). Although considerable research exists on audit committees and on IT risk (including a recent NACD study investigating board oversight of information security), no study to date addresses audit committee oversight in this domain.

Based on responses from 39 audit committee members, we found (1) little audit committee emphasis on oversight of IT risks, (2) audit committees involved with IT oversight focus on more traditional risks (e.g.,

monitoring), while very little attention is devoted to IT acquisition and implementation, and (3) the amount of IT oversight is positively associated with the responding members' auditing experience and prior familiarity with the COBIT model for assessing IT risks. Audit committee independence, diligence, and expertise, company size, and industry were not significantly associated with IT oversight.

This study has three important limitations. First, this initial study is exploratory. Rigorous future research is needed before definitive conclusions can be drawn about the audit committee's ability and willingness to provide effective IT risk oversight. Second, the results of this study rely on the perceptions of the participants regarding one of their audit committees' oversight of IT risk. The participants' perceptions may not accurately reflect the audit committee's true level of IT oversight. Finally, the relatively small sample size and response limit the ability to generalize the extent of audit committee oversight of IT risks.

We encourage additional, large-sample investigations of the role of the audit committee in overseeing IT risks. In particular, future research may examine the degree to which audit committees accept responsibility for IT oversight, how such committees enhance their IT expertise, and what other factors may be associated with greater IT oversight by the audit committee. 

Acknowledgements: We gratefully acknowledge financial and other support from KPMG's Audit Committee Institute and helpful feedback from Scott Reed of KPMG, Joseph Balloun, Mark Beasley, Dan Ivancevich, and John Sennetti.

References

1. Beasley, M. S., J. V. Carcello, D. R. Hermanson, and P. D. Lapedes. 2000. Fraudulent financial reporting: Consideration of industry traits and corporate governance mechanisms. *Accounting Horizons* 14 (December): 441-454.
2. Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees (BRC). 1999. *Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees*. New York: New York Stock Exchange and National Association of Securities Dealers.
3. Carcello, J. V., D. R. Hermanson, and T. L. Neal. 2002. Disclosures in audit committee charters and reports. *Accounting Horizons* 16 (December): 291-304.
4. COBIT. 2000. *COBIT – Governance, Control, and Audit for Information and Related Technology*. Information Systems Audit and Control Foundation. Available: <http://www.isaca.org>.
5. DeAngelo, L. E. 1981. Auditor size and audit quality. *Journal of Accounting and Economics* 3: 183-199.
6. DeZoort, F. T. 1997. An investigation of audit committees' oversight responsibilities. *Abacus* 33 (September): 208-227.
7. _____. 1998. An analysis of experience effects on audit committee members' oversight judgments. *Accounting, Organizations and Society* 23 (January): 1-22.
8. _____, D. R. Hermanson, D. Archambeault, and S. Reed. 2002. Audit committee effectiveness: A synthesis of the empirical audit committee literature. *Journal of Accounting Literature* 21: 38-75.
9. DeZoort, F. T., and S. Salterio. 2001. The effects of corporate governance experience and audit knowledge on audit committee members' judgments. *Auditing: A Journal of Practice & Theory* 20 (September): 31-47.
10. Dillman, D. A. 2000. *Mail and Internet Surveys: The Tailored Design Method* (2nd ed.). New York: John Wiley and Sons, Inc.
11. Hermanson, D. R., M. C. Hill, and D. M. Ivancevich. 2000. Information technology-related activities of internal auditors. *Journal of Information Systems* 14 (Supplement): 39-53.
12. Horton, T. R., C. H. Le Grand, W. H. Murray, T. R. Ozier, and D. B. Parker. 2000. *Information Security Management and Assurance: A Call to Action for Corporate Governance*. Altamonte Springs, FL: The Institute of Internal Auditors.
13. Ivancevich, D. M., D. R. Hermanson, and L. M. Smith. 1998. The association of perceived disaster recovery plan strength with organizational characteristics. *Journal of Information Systems* 12 (Spring): 31-40.

14. Kalbers, L. P., and T. J. Fogarty. 1993. Audit committee effectiveness: An empirical investigation of the contribution of power. *Auditing: A Journal of Practice & Theory* 12 (Spring): 24-49.
15. KPMG Audit Committee Institute. 2000. *Audit Committee Survey 2000*. Montvale, NJ: KPMG Audit Committee Institute.
16. Lainhart IV, J. W. 2000. COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems* 14 (Supplement): 21-25.
17. McKinsey & Company. 2002. *Director Opinion Survey 2002*. <http://www.mckinsey.com/practices/CorporateGovernance/Research/>
18. McMullen, D. A., and K. Raghunandan. 1996. Enhancing audit committee effectiveness. *Journal of Accountancy* 182 (August): 79-81.
19. National Association of Corporate Directors. 2000. *Report of the NACD Blue Ribbon Commission on Audit Committees: A Practical Guide*. Washington, DC: NACD.
20. _____. 2001a. *Information Security Oversight: Essential Board Practices*. Washington, DC: NACD.
21. _____. 2001b. *2001-2002 Public Company Governance Survey*. Washington, DC: NACD.
22. Public Oversight Board (POB) Panel on Audit Effectiveness. 2000. *The Panel on Audit Effectiveness Report and Recommendations*. Stamford, CT: POB.
23. Sarbanes, P. and M. Oxley. 2002. *The Sarbanes-Oxley Act of 2002*. Washington, DC: U.S. Congress.
24. Wolnizer, P. W. 1995. Are audit committees red herrings? *Abacus* 31: 45-66.

Appendix:

**34 Control Objectives from COBIT Model Sorted by Four Business Processes
(Scale from 1 = no oversight to 7 = heavy oversight)**

Planning And Organization: Includes strategy to identify best IT organization and structure.

Control Objective	Mean Rating
1. Define a strategic IT plan: includes periodic strategic planning sessions to develop short-term operational goals from long-term plans	2.64
2. Define the IT systems: includes an IT model with various systems designed to maximize information use	2.51
3. Determine the IT direction: includes an IT plan to attain specific technological products, services, and delivery systems	2.64
4. Define the IT organization and relationships: includes ideal size skilled organization with clearly defined and communicated individual roles and responsibilities subject to company strategy and control	2.69
5. Manage the IT investment: includes the development and approval of an IT budget	2.59
6. Communicate IT management aims and directions: includes communication of policies including specific standards to facilitate practical use	2.33
7. Manage IT human resources: includes fair and transparent IT personnel management practices (e.g., recruitment, training, promoting, etc.)	2.00
8. Ensure compliance with external IT requirements: includes compliance with external requirements relevant to IT	3.32
9. Assess IT risks: includes IT risk-identification and analysis; subsequently reducing risk subject to cost / benefit criteria	3.44
10. Manage IT projects: includes prioritizing projects and use of project management techniques	2.05

- 11. **Manage IT quality:** within established quality management standards including clearly defined deliverables and responsibilities 2.28

Business Process Mean

2.59

ACQUISITION AND IMPLEMENTATION: Represents identified IT solutions developed or purchased and implemented to meet IT objectives.

Control Objective	Mean Rating
1. Identify IT automated solutions: identify and analyze IT alternatives against user requirements	1.67
2. Acquire and maintain applications software: designed to meet specific user objectives possibly phased-in based upon clearly defined deliverables	2.05
3. Acquire and maintain IT systems: includes hardware and software acquisition, standardizing of software, evaluation of hardware and software performance, and consistent system administration	2.13
4. Develop and maintain IT procedures: systematic development of necessary IT manuals, service requirements and training materials	2.15
5. Install and accredit IT systems: an organizational plan to get the IT system up and running	1.92
6. Manage IT changes: a plan to facilitate IT changes including feed-back monitoring and follow-up	2.03

Business Process Mean

1.99

DELIVERY AND SUPPORT: Includes required IT services primarily relating to IT security and continued training, need to set up support, and actual processing of data by application systems.

Control Objective	Mean Rating
1. Define and manage IT service levels: formal service agreements indicating required quantity and quality of service	1.90
2. Manage IT third-party services: control procedures to determine effectiveness of existing IT agreements based upon organizational policy	2.08
3. Manage IT performance and capacity: relates to measuring system utilization and satisfaction of demand	2.10
4. Ensure IT systems security: relates to controls designed to limit access to systems, data, and programs to authorized users	3.21
5. Identify and allocate IT costs: a cost accounting system designed to accurately record and allocate IT costs based upon service provided	2.05
6. Educate and train IT users: a comprehensive IT training and development plan	1.90
7. Assist and advise IT customers: a help desk facility providing IT support and advice	1.77
8. Manage the IT inventory: controls which identify and record all IT hardware and software along with their physical location	1.92

9. Manage IT problems and incidents: the recording of all IT problems or incidents	2.21
10. Manage IT data: an effective combination of application and general controls over IT operations	2.05
11. Manage IT facilities: includes IT environmental and physical controls regularly reviewed to determine proper functioning	2.10
12. Manage IT operations: schedule of activities required	1.82
13. Ensure continuous service: making IT services available upon request, including a disaster recovery plan	3.03

Business Process Mean

2.16

MONITORING: The assessment of IT quality and compliance with control requirements over time.

Control Objective	Mean Rating
1. Monitor the IT process: identification of relevant IT performance indicators, systematic and timely reporting of performance and prompt follow-up on deviations	2.72
2. Assess IT internal control adequacy: commitment to monitoring IT internal controls, assessing their effectiveness at regular reporting intervals	3.51
3. Obtain IT independent assurance: independent IT assurance reviews carried out at regular intervals	2.92
4. Provide for IT independent audit: independent IT audits carried out at regular intervals, separate from financial audit	3.33

Business Process Mean

3.12

Endnotes

¹ The survey was pretested on academics and practitioners and revised based on their comments.
² The addition of an early/late response variable to the model has no effect on the results presented in Table 3. The early/late variable is not significant (p = 0.78).
³ Several recent surveys of directors or audit committee members have had limited responses. For example, in gathering data for its *2001 – 2002 NACD Public Company Governance Survey* (NACD 2001b), NACD mailed surveys to “CEOs, directors, and executive officers of all U.S. publicly held companies [approximately 15,000 companies].” NACD received 280 responses, reflecting 1.9% of the public companies. Similarly, KPMG’s Audit Committee Institute gathered data for its *Audit Committee Survey 2000* (KPMG 2000) in conjunction with *Corporate Board Member* magazine. KPMG mailed over 5,000 surveys and realized a 4.1% response rate. Finally, McKinsey & Company recently collaborated with *Directorship* magazine in gathering data for its *Director Opinion Survey 2002* (McKinsey 2002). McKinsey “sent surveys to about 2,000 directors, getting responses from nearly 200,” a response rate of just under 10%.
⁴ Some may argue that audit committee members most likely to respond to the present survey would be those whose audit committees are doing the most to oversee IT risks. If so, our results could overstate the typical audit committee’s IT oversight efforts. Despite this potential bias, the Results section discloses relatively low oversight levels among the responding audit committees.
⁵ Four participants did not indicate the number of audit committees currently served (although all indicated several years of audit committee experience). The results are unaffected if these four individuals are deleted. Also, one participant responded regarding only 33 of the 34 control objectives. Deletion of this individual has no effect on the results.
⁶ The variance inflation factors all are less than 2.10, indicating that multicollinearity is not a significant concern.
⁷ We recognize that it would be more desirable to have a sample size closer to 10 observations per independent variable. A reduced model, ACITOV = f (YRSAUD, COBEXP), yields consistent results.

Notes