



LEADING THE IT GOVERNANCE COMMUNITY

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA

Telephone: 847.253.1545
Facsimile: 847.253.1443

Web Sites: www.isaca.org and www.itgi.org

27 April 2006

Ms. Nancy M. Morris, Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

and

Office of the Secretary
Public Company Accounting Oversight Board
1666 K Street NW
Washington, DC 20006-2803

Via e-mail to rule-comments@sec.gov and comments@pcaobus.org

RE: File Number 4-511

Dear SEC and PCAOB Board Members:

We very much appreciate the opportunity to provide comments and recommendations to the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) on lessons learned from the first two years of applying the Sarbanes-Oxley Act's internal control reporting requirements, including how the efficiency and effectiveness of those assessments and audits could be improved.

These comments and recommendations are offered on behalf of both ISACA and the IT Governance Institute (ITGI), international independent thought leaders on IT governance, controls, security and assurance. A brief description of the organizations is provided at the end of this letter.

ISACA Survey Results

In April 2006, ISACA conducted an online survey of its North American members, who are primarily IS audit and control professionals, and other individuals who participated in recent ISACA Sarbanes-Oxley symposia. The survey addressed issues surrounding their organizations' year-two experiences related to Sarbanes-Oxley compliance. Responses were received from approximately 740 individuals. The summarized findings of the survey form the basis of our comments and recommendations in this letter, and the full survey results are attached.

Primary Comments

Based on our review of the ISACA survey results, the following primary comments were identified:

- Additional guidance for management is needed.
- The risk-based, top-down approach had nominal impact.
- Further IT controls guidance is needed.
- Internal control sustainability is starting to grow as a benefit of Sarbanes-Oxley.
- Research on automating key controls is needed.

The following paragraphs summarize key findings from the survey in support of the primary comments listed above.

Additional Guidance for Management is Needed

The survey asked if the respondents perceived a need for additional management-focused guidance on Sarbanes-Oxley 404 compliance. More than 80 percent of the respondents either agreed or strongly agreed that such additional management-focused guidance is needed (question number 1). This area was further supported by the 73 percent who felt that the time is right for separate guidance for management of issuers and for public accountants (question number 3).

Recommendation: The SEC should work through COSO and other organizations to ensure additional management-focused guidance on Sarbanes-Oxley 404 compliance is developed and made available.

The survey respondents identified the following as the top four areas in which additional management-focused guidance is needed:

- IT controls (e.g., access, application, change and security)
- Testing (e.g., requirements, plans, methodologies and sample size)
- Scoping (e.g., risk assessment, relationship to other controls, processes and subprocesses)
- Various definitions (e.g., key controls, application and general controls)

Risk-based, Top-down Approach Had Nominal Impact

More than 60 percent of the respondents indicated that the SEC/PCAOB guidance issued in May 2005, recommending a risk-based, top-down approach, did reduce the scope of management's 404 work in year two (question number 2). However, 33 percent indicated that it did so by less than 5 percent. Nearly 17 percent reported that it actually increased the scope of management's work.

Recommendation: The SEC and PCAOB should work through COSO and other organizations to provide additional guidance, illustrations and best practices addressing how to apply the risk-based, top-down, approach.

This finding is consistent with several other surveys released recently by the CRA International¹ and Financial Executives International (FEI).² It appears that the overall resources required have been reduced in year two; however, the exact reasons why are not clear. It is apparent the level of work performed internally at many issuers is decreasing as they focus on Sarbanes-Oxley as part of

¹ www.crai.com

² www.fei.org

a process, and begin to look at their IT risks and controls in the broader context of their IT governance efforts.

Further IT Controls Guidance is Needed

Respondents were asked to identify their best source for addressing IT controls in year two (question number 4); more than 54 percent indicated that they relied on *IT Control Objectives for Sarbanes-Oxley*, published by the IT Governance Institute. Another 46 percent said they utilized an internally developed approach, while 34 percent used the advice of their external audit firm.

Recommendation: *The SEC and PCAOB should work through COSO to provide additional guidance on IT controls. The starting point for developing this guidance could be the broadly accepted ITGI publication, IT Control Objectives for Sarbanes-Oxley.*

When respondents were asked what IT governance/control framework was used for year two (question number 11), 58 percent indicated they relied on *Control Objectives for Information and related Technology* (COBIT) and 30 percent pointed to *IT Control Objectives for Sarbanes-Oxley*.³ COSO was used by 36 percent and internally developed approaches by 26 percent. More than 52 percent reported that their IT control framework was easy to use (question number 12).

Internal Control Sustainability is Starting to Grow as a Benefit of Sarbanes-Oxley

More than 57 percent of those responding to the ISACA survey indicated that sustainability was addressed as part of their year-two processes or as part of their year-three planning (question number 19). As a result of Sarbanes-Oxley compliance activities, enterprises are making internal control and sustainability a part of their business processes. Additionally, more than 54 percent reported that their overall sustainability efforts included the need for an IT control framework (question number 20). In the organizations' year-two efforts, more than 50 percent of their sustainability efforts considered business process, process controls and IT control changes (question number 21).

Recommendation: *The SEC and PCAOB should work through COSO and other organizations to support additional research into best practices and the benefits of sustainability, including a focus on continuous monitoring and auditing.*

Research on Automating Key Controls is Needed

Two-thirds of the respondents indicated that less than 25 percent of their key controls were considered automated in year two (question number 23). The possibility exists that the remaining 75 percent could achieve additional benefits by automating key controls. As more and more key controls are automated, the amount of work should continue to decline for testing and other compliance-related activities and the effectiveness of controls should increase. Looking at the issue slightly differently, 44 percent of respondents indicated that there was an overall increase in the automation of key controls from year one to year two (question number 24).

³ Both COBIT and *IT Control Objectives for Sarbanes-Oxley* are openly available to the general public from the ISACA and ITGI web sites, www.isaca.org and www.itgi.org. The draft of the second edition of *IT Control Objectives for Sarbanes-Oxley* will be posted on both sites for public exposure comments from 1 May to 30 June 2006.

Recommendation: *The SEC and PCAOB should work through COSO and other organizations to support additional research into best practices for automating key controls.*

A Summary of Additional Survey Findings

The following list summarizes key findings from the survey questions not already referenced in the paragraphs above. The list is organized by question number. Questions 22 and 25 were open-ended questions and generated a significant number of essay-type responses. Those results, which are under further analysis, are not included here.

5. Almost half of the respondents reported that no time or less than 5 percent of time was saved for the 404 attestation by having the organization's management work closer with its public accounting firm.
6. More than 50 percent of respondents reported that their public accounting firm took entity-level controls into account in determining their level of testing in year two (question 6.1). For 70 percent of those responding to the question, the reduction in work expended by the accounting firm by utilizing an entity level approach was less than 5 percent (question 6.2).
7. More than 40 percent of the responding organizations used software to assist with 404 compliance. Many respondents wrote in the name of the software program(s) they used, but no particular program(s) dominated the responses. In fact, the top three most often named constituted only 5 percent of the overall replies.
8. More than 40 percent of the respondents indicated that the year-two testing approach differed from the year-one testing approach with regard to scope and number of tests. This may explain why year-two costs have not decreased as much as anticipated.
9. E-mail systems are used by 84 percent of respondents to evidence approvals. Of that 84 percent, almost 60 percent did not include the e-mail system in the scope of Sarbanes-Oxley. Additional guidance is needed on the role of controls in these kinds of situations and the extent, if any, to which such controls need to be documented and tested by management and audited by the external auditor.
10. More than 78 percent of those who replied to the question asking about the organization's IT approach adopted the same level of IT control for smaller subsidiaries as for larger subsidiaries. (Note: This percentage is based on excluding the "not applicable" responses.) There may be an opportunity to use differentiated approaches based on size, top-down approach, risk and other factors. This could lead to potential cost reductions.
13. More than 56 percent stated that their staff obtained in-house training on using their IT control framework.
14. Of the 620 respondents who relied on external expertise to implement the IT control framework, 35 percent used a consultant, 35 percent used a Certified Information Systems Auditor (CISA) or Certified Information Security Manager (CISM), and almost 30 percent used an external auditor.
15. More than 37 percent of respondents changed their IT control framework from year one to year two.
16. More than 73 percent use spreadsheets as an integral part of the financial reporting process.
17. Almost 53 percent use software developed by end users as an integral part of the financial reporting process.
18. Only 15 percent use or adapt the nine-firm (public accounting firms) "Conclude framework" to address general computer controls and potential deficiencies.

26. In year two, more than 58 percent of organizations increased emphasis in testing application controls.
27. Additional comments related to their organizations' experiences in year two were provided by 237 respondents:
- More than 28 percent are concerned with external audit and inconsistent guidance.
 - More than 15 percent are concerned with cost.
 - More than 10 percent are concerned with testing.
 - More than 5 percent focused on framework issues.

With more than 50,000 members in more than 140 countries, ISACA is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*, develops international information systems auditing and control standards, and administers the CISA designation, earned by more than 44,000 professionals since inception, and the CISM designation, a groundbreaking credential earned by 5,500 professionals in its first three years.

The IT Governance Institute (ITGI) was established by ISACA in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. ITGI developed *Control Objectives for Information and related Technology* (COBIT), now in its fourth edition, and offers original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Thank you for this opportunity to relay our comments on the lessons learned from the first two years of applying the Act's internal control reporting requirements. Because ISACA and ITGI represent many of the individuals engaged in Sarbanes-Oxley compliance efforts and much of the guidance informing those efforts, we believe we are uniquely positioned to bring value to any future projects to address our recommendations. Please feel free to call on us if we can be of assistance in any way in task forces, committees or work groups. Representatives of ISACA and ITGI will be present at the SEC and PCAOB Roundtable meeting on 10 May in Washington and we look forward to the discussion of these issues.

Respectfully submitted,



Everett C. Johnson, CPA
2005-2006 International President
ISACA (www.isaca.org)
IT Governance Institute (www.itgi.org)

cc: Mr. Larry Rittenberg, Chairman, COSO Board, via e-mail to lrittenberg@bus.wisc.edu

Attach: ISACA survey results