3701 Algonquin Road, Suite 1010 Telephone: 847.253.1545
Rolling Meadows, Illinois 60008, USA Facsimile: 847.253.1443 Web Sites: *www.isaca.org* and *www.itgi.org*

26 February 2007

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

Via e-mail to comments@pcaobus.org

RE: Rulemaking Docket Matter No. 021

Dear PCAOB Board Members:

We very much appreciate the opportunity to provide comments and recommendations to the Public Company Accounting Oversight Board (PCAOB) for the proposed Auditing Standard—An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements—**PCAOB Release No. 2006-007, December 19, 2006; Docket Matter No. 021**.

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

General Comment

ISACA is responding to the PCAOB questions principally from an information technology (IT) perspective. COSO and similar overall control frameworks provide very limited guidance regarding IT risks and controls. Meanwhile, the role and impact of information technology on risks and controls related to financial reporting has grown in importance since COSO was developed. Further, there is very limited guidance regarding the application of a risk-based, top-down approach in environments where IT is important. Accordingly, we believe that significant additional emphasis on such matters related to IT should be included in the PCAOB standard for it to be even more useful.

Responses to Primary PCAOB Questions of Interest

Based on our review of the proposed PCAOB guidance, and the core focus of ISACA and ITGI, PCAOB questions 1 to 6, 13 and14 are the primary focus of our comments:

1. *Does the proposed standard clearly describe how to use a "top-down" approach to auditing internal control?*

   We believe that the description of the top-down approach as it relates to IT application and IT general controls could be enhanced. This need could be met by providing more detailed guidance, particularly for IT general controls.

   We suggest adding descriptive material regarding IT risks and controls under a new separate heading titled "Effects of Information Technology on Internal Control over Financial Reporting." This section could be placed after paragraph 8. Content from AU 319.16 - .20 should be included in this section and modified to illustrate how the top-down approach would apply to IT.

   A brief case study describing the interaction of manual controls and IT controls using a top-down approach and how it could impact the overall evaluation of internal control would be useful.

   References to helpful external material also would be beneficial (such references would be suggestive only and would not imply any endorsement of the material by the PCAOB). One such reference could be ITGI's *IT Control Objectives for Sarbanes-Oxley*, particularly the IT compliance road map (pages 27 to 45) and IT general controls (appendix C – pages 57 to 81).[1]

2. *Does the proposed standard place appropriate emphasis on the importance of identifying and testing controls designed to prevent or detect fraud?*

   We believe that some examples of IT controls designed to prevent and detect fraud should be included. These might include the following:
   - A user has access to programmed functions that are incompatible with the user's duties and responsibilities and could then process transactions that result in potential misstatement to financial statements (such as an unrecorded funds transfer or misappropriation). This risk can be reduced by the proper implementation of controls over access to such programmed functions and related data (i.e., access to programs and data).
   - A programmer in a telecommunications company makes an unauthorized change to a computer program that causes revenues to be miscalculated and materially misstated. This risk can be mitigated by using security controls to restrict access to programs and ensuring that all program changes are reviewed and tested.

3. *Will the "top-down" approach better focus the auditor's attention on the most important controls?*

   We believe that a top-down approach will better focus the auditor's attention on the most important controls. A top-down approach will provide a better understanding of how an assessment of company-level controls could decrease risk and reduce the nature and extent of testing of controls at the control activity level. A bottom-up approach generally identifies a larger number of key controls and results in more detailed testing than a top-down approach. For example, a top-down approach may identify key controls that do not rely on IT. In this situation, IT general controls may not need to be tested. If key

[1] *IT Control Objectives for Sarbanes-Oxley* is openly available to the general public from the ISACA and ITGI web sites, *www.isaca.org* and *www.itgi.org.* The document, now in its second edition, has been downloaded more than a quarter of million times and referenced globally. The second edition was issued in 2006 after a public exposure process.

application controls are performed by IT or are IT-dependent, consideration can then be given to which IT general controls are important in the circumstances and the level of tests needed for such IT general controls.

Additional IT general control top-down considerations are discussed in the ITGI publication *IT Control Objectives for Sarbanes-Oxley*, particularly the IT compliance road map (pages 27 to 45) and IT general controls (appendix C, pages 57 to 81).

4. *Does the proposed standard adequately articulate the appropriate consideration of company-level controls and their effect on the auditor's work, including adequate description of when the testing of other controls can be reduced or eliminated?*

We believe that a top-down approach, including consideration of company-level controls, will better focus the auditor's attention on the most important controls. We have addressed this issue in question 3 above. However, it would be helpful to discuss the impact that very effective IT general controls would have on the need for testing other controls where the use of IT is very pervasive and such other controls are likely to be dependent on IT. For example, in a centralized IT environment with very effective program change controls, operations controls and access controls, reliance on IT application controls and IT-dependent applications controls across most applications may be possible. Accordingly, testing of IT general controls could significantly reduce the extent of testing of the related application controls across these applications.

5. *Does the proposed standard appropriately incorporate risk assessment, including in the description of the relationship between the level of risk and the necessary evidence?*

We believe that the description of the risk assessment as it relates to IT application and IT general controls could be enhanced. As noted in our response to question 1, we suggest adding descriptive material regarding IT under a separate heading titled "Effects of Information Technology on Internal Control over Financial Reporting." Consideration could be given to modifying the language from AU 319.19 and AU 319.20 for purposes of this guidance, to focus on how risk assessment would apply to IT and include it in this new section.

We have included "Illustrations of the Extent of Auditor Testing of the Operational Effectiveness of Controls" as an attachment to this letter. This table indicates how the auditor's assessment of risk might relate to the extent of testing of operating effectiveness of controls, including assessments in which no testing or a walkthrough only would be appropriate.

6. *Would the performance of a walkthrough be sufficient to test the design and operating effectiveness of some lower risk controls?*

Yes, in most cases we would agree that a walkthrough would be sufficient. For example, a walkthrough may be sufficient to assess the computer operations controls supporting a low-risk system with no history of problems. See also the attachment.

13. Can the auditor perform an effective audit of internal control without performing an evaluation of the quality of management's process?

The auditor can perform an audit of internal controls without performing an "evaluation" of the quality of management's process. However, the auditor will be able to perform a more efficient audit of the internal control system if the auditor has an overall understanding of the process management followed and the results of the management process. The guidance should indicate that the audit may be more efficient by obtaining an understanding of management's process, without necessarily making an evaluation of the process.

14. Will removing the requirement for an evaluation of management's process eliminate unnecessary audit work?

As noted in question 13 above, the auditor will be able to perform a more efficient audit of the internal control system if the auditor has an overall understanding of the process management followed and the results of the management process.

In addition, the guidance should include discussion addressing how management and the public accounting firm could jointly plan their work to increase the effectiveness and efficiency of the entire process.

Other areas the PCAOB might want to consider expanding for additional clarity include:

- Question 5—The release emphasizes the importance of the risk assessment. It would be useful to provide an example(s) of a risk assessment methodology, including examples of quantitative and qualitative risk factors.

- Questions 9 and 10—The draft states, "…any individual control does not necessarily have to operate without any deviation to be considered effective." (See PCAOB Release, Testing Controls, Relationship of Risk to the Evidence to be Obtained, point #53, p. A1-22.) Guidance would be helpful to assist in the determination of what level of deviation would be acceptable and still evaluate the control as effective.

* * * * *

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 50,000 professionals since inception, and the CISM designation, a groundbreaking credential earned by 6,000 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 regarding the PCAOB Guidance**.** 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 to the PCAOB in any way including task forces, committees, work groups or just for reference purposes.

Respectfully submitted,

Everett C. Johnson, CPA
2006-2007 International President
ISACA (*www.isaca.org*)
IT Governance Institute (*www.itgi.org*)

Attachment

Illustrations of the Extent of Auditor Testing of the Operational Effectiveness of Controls

Consequences of a Control Failure ↑			
Possible Material Weakness	Moderate Testing	Moderate to High Testing	High Testing
Possible Significant Deviation	Minimum Testing	Moderate Testing	Moderate to High Testing
No Significant Deviation	No Testing	Minimum Testing	Minimum Testing
	Low	Medium	High

Risk of a Control Failure

Definitions[2]

No Testing—No testing or evidence of operating effectiveness is necessary.

Minimum Testing—Ordinarily, this would consist of walkthrough and inquiry, without further testing or evidence of operating effectiveness.

Moderate Testing—Ordinarily, this would consist of obtaining evidence of operating effectiveness in addition to performing a walkthrough and inquiry. Such additional evidence could be obtained by performing monitoring procedures or examining the results of such monitoring procedures, by observing the operation of the control, by reviewing the evidence of the operation of controls (such as follow-up on exception reports), and similar activities. Such activities ordinarily would be performed on a test basis.

High Testing—Ordinarily, these tests would be more extensive than those described under Moderate Testing and would include tests as of period-end dates for controls that operate at that time.

[2] These definitions apply to the registrant's annual assessment for complying with the provisions of the Sarbanes-Oxley Act of 2002 for financial reporting purposes. They do not apply to the normal, periodic review, assessment and testing of the internal control systems for operational efficiency and for compliance with laws and regulations.