ISACA®
Serving IT Governance Professionals

IT Governance Institute®
Leading the IT Governance Community

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*

17 December 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: Preliminary Staff Views—An Audit of Internal Control That Is Integrated With An Audit of Financial Statements—Guidance for Auditors of Smaller Public Companies—October 17, 2007

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 Guidance for Auditors of Smaller Public Companies.

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 Comments

ISACA is responding to the PCAOB questions principally from an information technology (IT) perspective.

We believe the proposed guidance will be useful to auditors of smaller public companies and congratulate the PCAOB on its accomplishments. In addition, portions of this proposed guidance may be applicable to audits of larger public companies that are not particularly complex.

Responses to PCAOB Questions

Based on our review of the proposed PCAOB guidance, our responses to questions 1 and 2 are as follows:

1. *Does the guidance in this publication, including the examples, appropriately consider the environment of the smaller, less complex company? If not, what changes are needed?*

Our response includes several suggestions that would add clarity to the document's objectives. (*Italicized words indicate modifications.)*

A. The section "Scaling the Audit of Internal Control," starting on page 6, should include an additional attribute along the lines of "relatively simple organizational structure with operations in only one country." Smaller companies may have operations in several countries, often with a corporate structure in each country in which they operate. This structure could introduce additional complexities due to adhering to different laws and regulations, managing within varying cultural aspects, operating with multiple IT systems including more extensive network configurations, etc. We suggest that companies having this additional attribute be excluded from consideration in this document.

B. This comment is directed to chapter 5, "Auditing Information Technology Controls in a Less Complex IT Environment," specifically to page 26, second bullet point "Software." Suggesting a company that uses off-the-shelf software "without modification" is a characteristic of a smaller, less complex company over-simplifies the issue. The wording may suggest an unintentional over-reliance on the implementation of off-the-shelf software as a basis for supporting the auditor's conclusion to reduce risk assessment conclusions and thus reduce review effort in this area.

   A proposed enhancement to this section is: Software: The company typically uses off-the-shelf packaged software without *programming and data flow modifications. While this reduces the risks associated with program development and changes, the auditor should recognize that system, table, processing, and control configuration settings need to be determined upon implementation and are subject to the risks and categories of IT controls discussed within this section.*

C. The section "End User Computing Controls" in chapter 5, page 32, should be modified to strengthen the impact these types of applications have in the smaller, less complex company.

   Currently the text (first paragraph of the section) reads: "End-user computing refers to a variety of user-based computer applications, including spreadsheets, databases, ad-hoc queries, stand-alone desktop applications and other user-based applications. These applications might be used as the basis for making journal entries or preparing other financial statement information. End-user computing is especially prevalent in smaller, less complex companies."

   A proposed enhancement is: End-user computing refers to a variety of user-based computer applications, including spreadsheets, databases, ad-hoc queries, stand-alone desktop applications and other user-based applications. *End-user computing is especially prevalent in smaller, less complex companies. The risk associated within this area is that these applications may be used as the basis for making manual journal entries or preparing other financial statement information. In smaller companies, data for such applications is frequently downloaded from other applications or manually entered or re-entered and these applications may be subject to informal or no controls. The auditor should clearly identify all end-user applications and categorize the applications by* *dollar-level effect/impact, owner, process input/source requirements (for control totals) and document significant logic criteria as to the creation and manipulation of data to obtain a result.*

2. *Are there additional audit strategies or examples that the staff should consider including in this publication? If so, please provide details.*

   A. We suggest adding an example about prepackaged software to dispel the common misperception of the software package mitigating any other risks than application development risk or expanding the example in 5.1 to include this. This example might cover a software package that handles billing and accounts receivable, accounts payable and disbursements, general ledger, fixed assets, etc., with risk and control considerations for the auditor to consider. These considerations might include the set-up of the chart of accounts, input editing parameters, pricing tables, customer terms, approval levels, and criteria for exception reports, access control profiles (which govern who can do what).

   B. We also suggest adding on page 33 an example illustrating adequate controls over a spreadsheet that directly affects entries to the general ledger, such as an analysis warranty claims.

   C. ISACA would be pleased to assist the PCAOB in developing these examples.

Other Comments

We have included additional, more detailed, comments and suggestions in the attachment, which we believe will help clarify the guidance.

* * * * *

With more than 65,000 members in more than 140 countries, ISACA (*www.isaca.org)* 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,* and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor (CISA) designation, earned by more than 50,000 professionals since inception; the Certified Information Security Manager (CISM) designation, earned by 7,000 professionals since it was established in 2002; and the new Certified in the Governance of Enterprise IT (CGEIT) designation.

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
Chair, Professional Issues Working Group
Past International President, 2005-2007
ISACA (*www.isaca.org*)
IT Governance Institute (*www.itgi.org*)

Attachment–Additional Comments and Suggestions

Page 9: Clarify the statement, “If none of the controls that are designed ..., the auditor can take that into account in determining the test of that control.” As written, it seems to imply that none of the controls designed to address a risk are effective, but they still need to be tested.

Page 11: Implies that the auditor is performing substantive tests before performing the risk assessment and determining the nature, timing and extent of evaluating controls. We suggest clarifying.

Page 13: In the paragraph immediately after “Evaluation of Entity-Level Controls and Testing of Other Controls,” the last line discusses evaluating the company’s control environment and period-end financial reporting process. We believe this is a good spot to note “including IT.”

Page 16: At the end of example 2.1, this statement is made: “she could reduce the direct testing of the reconciliation controls, absent other indications of risk.” It would be helpful if a bit more specificity could be added around “reduce.” In other words, the text would benefit from further clarification, maybe with an example, how direct testing might be reduced.

Page 25: In the “End-user computing” bullet, the definition says “which are used to process, accumulate, summarize, and report the results of business operations...” We suggest, from a consistency perspective, using “initiate, authorize, record, process and report.”

Page 28: Two paragraphs above “IT-Dependent Controls,” the last line says “controls over backups of data necessary for financial statement preparation.” It is difficult to support a statement that if you do not have backups, you would not have the data necessary for preparing financial statements. We appreciate that backups are critical in the event that a data file is corrupted or destroyed, but absent that happening, the lack of controls over backup of data would not appear to result in a situation where financial statements could not be prepared or their reliability would be affected.

Pages 28 and 32: The PCAOB defines IT-Dependent Controls and Other Automated Controls on page 28 and then defines Application Controls on page 32 as “automated or IT-dependent controls.” The discussion on these two pages is very similar and could be consolidated.

Page 29: In example 5-1 in the paragraph above Audit Approach, the term “correction of processing errors” is used. That could be interpreted as processing errors from a financial calculation perspective. Is it to reference errors from jobs being processed in the wrong sequence (based upon lack of controls over operations), or is it intended to identify application processing errors? We suggest this be clarified.

Page 30: Inside the box, and in the first bullet under the main bullet, the sentence reads “the data inputs into the report are accurate and complete.” We suggest it be changed to read “the data included on the report is accurate and complete.” Normally one would not think of inputting data into a report. If it is changed as we suggest, there may need to be a test over the application that generates the report in addition to considering the transaction inputs.

Page 30: The second bullet point says “This might be accomplished through testing controls over the initiation, processing and recording...” We suggest adding “authorization” to the list.

Page 31: Under “Computer Operations,” the last two lines of the first paragraph read “continuity of financial reporting data is maintained through effective data backup and recovery procedures.” We believe this overemphasizes the contribution (if any) of such procedures to reliable financial reporting. As we noted previously, such procedures generally are relevant only if there has been an incident requiring the recovery of data from backup files.

In the next paragraph, the last line reads “backup procedures tend to be manual.” We suggest this be clarified to indicate that backup procedures/programs are initiated manually vs. automatically.

Page 32: In the first line, we suggest rewording “process for testing new applications and updates” to “process for user testing of new applications and updates.” In the first paragraph under Application Controls, we suggest adding “manual” at the end of the first paragraph, i.e., “example of an IT-dependent manual control.”

In the first paragraph in the “Application Controls” section, the automated control description is built out and then there is one sentence for the IT-dependent manual control example. We believe IT-dependent controls warrant more verbiage. At the very least we suggest the sentence that currently reads “Management’s review and reconciliation of the exception report” be changed to “Management’s review and reconciliation of an exception report” as there is nothing to which “the” references back.

Page 49: The top of the page does not appear to read well. We suggest revising the second line “material misstatement **of** the financial statements” to “material misstatement in the financial statements.” We also suggest clarifying the meaning of the end of that sentence: “thus could inform the auditor’s risk assessments during the audit.” Specifically what is meant by the use of the word “inform”?