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

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

Via e-mail to *rule-comments@sec.gov*
RE: ***File No.:*** S7-24-06

Dear SEC Commissioners:

We very much appreciate the opportunity to provide comments and recommendations to the Securities and Exchange Commission (SEC) for the Guidance for Management's Reports on Internal Control over Financial Reporting—**Release No. 34-8762; 34-54976: File No. S7-24-06**.

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
The SEC-proposed interpretive guidance can be considered a helpful beginning outline of a methodology to assist companies in complying with Sarbanes-Oxley *S*. 404. We believe the following would improve the document significantly:

- Expand the guidance to match the level of detail of the proposed PCAOB standard. We believe that management should have at least as much guidance as auditors.
- Consider how the guidance in SEC SAB 99 can be incorporated into this document, particularly in regard to materiality and material weaknesses and high, medium and low risk assessments.
- Clarify what should be considered a high risk, whether through fraud or error, a material weakness, and a significant deficiency. These should be consistent with the revised PCAOB definitions and other auditing standards, such as those relating to fraud.
- Provide more specific guidance and clarity on how specific controls can be eliminated from consideration for purposes of Sarbanes-Oxley *S.* 404.
- Provide additional clarity around the issue of how the assessment of risk relates to the sufficiency of evidence needed to support management's assessment of the effectiveness of ICFR.
- Provide more pragmatic examples and illustrations.

- Provide scenarios of when minimal or no testing is needed.
- Provide additional references to frameworks and guidance issued by other bodies, which will be helpful to management.

Without this additional focus we believe the proposed interpretative guidance may not accomplish the benefits the SEC desires, including making the Sarbanes-Oxley *S*. 404 processes less onerous on companies.

Responses to Primary SEC Questions of Interest
Based on our review of the SEC Management Guidance, and the core purpose of ISACA and ITGI, we have chosen to address SEC questions 1-5, 7 and 11 as our primary focus.

1. *Will the proposed interpretive guidance be helpful to management in completing its annual evaluation process?*

   The proposed SEC interpretive guidance will be a helpful addition, as management continues to implement Sarbanes–Oxley Act requirements. However, the guidance remains at a high level, so it will not be helpful for those who are looking for detailed management implementation guidance. This management need could be met by providing more detailed guidance, including implementation guidance or reference to helpful material (such references would be suggestive only and would not provide any endorsement of the material by the SEC). For example, one such additional reference related to IT controls that the SEC could include in the proposed management guidance is ITGI's *IT Control Objectives for Sarbanes-Oxley*.[1]

2. *Does the proposed guidance allow for management to conduct an efficient and effective evaluation? If not, why not?*

   Because the proposed guidance is at such a high level, it is difficult to determine if management's evaluation will be more efficient and effective. The addition of more detailed guidance, pragmatic examples and possibly a couple of brief case studies presenting some of the considerations, including financial statement assertions, could be very helpful to management of issuers.

3. *Are there particular areas within the proposed interpretive guidance where further clarification is needed? If yes, what clarification is necessary?*

   Yes, there is an area of the proposed interpretive guidance that could use further detail and clarification. The guidance addresses IT controls in only two paragraphs. We suggest that further detailed guidance would be helpful on the role of IT controls in a top-down approach, focusing on risk and suggestions on how IT controls impact the overall evaluation.

   Additional guidance for management on the nature and extent of tests of operating effectiveness of controls at various risk levels would be helpful. We have included one example of the type of

[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.

guidance that should be considered in the attachment. This guidance could replace the matrix on page 32, which we believe is of limited usefulness to management.

Also, the SEC's proposed interpretive guidance provides characteristics of a control framework, to assist registrants in selecting an overall framework (e.g., COSO) on which to base their Sarbanes-Oxley *S*. 404 evaluations, but does not give similar guidance in other areas. Since COSO and similar overall control frameworks provide very limited guidance regarding information technology risks and controls, and the role of information technology has grown in importance since COSO was developed, helpful additional guidance could include examples of acceptable control frameworks for IT controls (page 27, item d), such as ITGI's COBIT[2] framework and a companion book, *IT Control Objectives for Sarbanes-Oxley* (page 22 item a). We believe it would be extremely helpful to management to have illustrations of other literature to refer to; you might also consider including in the body of the guidance or in an appendix a listing of other authoritative, well-recognized and often-used reference documents such as COBIT and ITIL.

4. *Are there aspects of management's annual evaluation process that have not been addressed by the proposed interpretive guidance that commenters believe should be addressed by the Commission? If so, what are those areas and what type of guidance would be beneficial?*

Further guidance on the application of a top-down approach to IT controls would be helpful. Since the SEC's discussion on top-down approach presupposes the use of a risk assessment, additional examples of just how this would work inside a company would likely add further clarity and understanding of these important concepts.

Increased guidance on risk assessment would likely be helpful to management in addressing identification of controls. There are many references to risk and the need for self-assessment, and likely not enough reference to external documents, such as COSO, on how these concepts relate to the issue of enterprise risk management.

More specific guidance could be given concerning the risk of fraud. Fraud could be given a wide definition or could be interpreted as only fraud that would result in a misstatement of the financial statements. Investors may assume that all aspects of fraud have been addressed in a risk assessment, while management may address only fraud risks that could result in a misstatement of the financial statements.

It would be helpful to include guidance similar to that in the PCAOB standards draft, on how management could consider prior years' work in testing controls in the current year. Allowing management to rely on certain controls in the current year that have been tested in prior years could significantly reduce costs of compliance with Sarbanes-Oxley.

---

[2] COBIT is a comprehensive IT governance and control framework, and while the control objectives in COBIT are much more comprehensive than the control objectives of reliable financial reporting (i.e., COBIT also contains objectives related to risk management, governance, effectiveness and efficiency), organizations find that selecting those areas that apply to them provides the flexibility needed to address the wide-ranging complexities of IT—as their needs go beyond compliance with Sarbanes-Oxley Act. The *IT Control Objectives for Sarbanes-Oxley* publication includes a subset of the COBIT control objectives that are generally applicable to the reliability of financial reporting.

5. *Do topics addressed in the existing staff guidance (May 2005 Staff Guidance and Frequently Asked Questions [revised October 6, 2004]) continue to be relevant or should such guidance be retracted? If yes, which topics should be kept or retracted?*

   The May 2005 Staff Guidance and Frequently Asked Questions (revised October 6, 2004) have been useful for management in dealing with the requirements of Sarbanes-Oxley *S.* 404. We do not believe that the SEC should retract any guidance that currently exists.

7. *Considering the PCAOB's proposed new auditing standards, An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements and Considering and Using the Work of Others In an Audit, are there any areas of incompatibility that limit the effectiveness or efficiency of an evaluation conducted in accordance with the proposed guidance? If so, what are those areas and how would you propose to resolve the incompatibility?*

   We believe the guidance is basically compatible at the level of concepts, and there do not appear to be major areas of incompatibility in the SEC interpretative guidance that would limit the effectiveness or efficiency of management's evaluation. However, we believe the PCAOB guidance is at a more useful level of detail and is clearer than the proposed SEC guidance. We therefore suggest, as indicated in our response to question 1, that the level of interpretative guidance in the SEC document be expanded to reach the same level of guidance as in the PCAOB document.

   In addition, an item that the SEC's proposed guidance does not appear to address is the coordination of management's evaluation process with the public accounting firm's work. The SEC guidance could add an area on addressing how management and the public accounting firm could jointly plan their work to increase the effectiveness and efficiency of the entire process.

11. *Should compliance with the interpretive guidance, if issued in final form, be voluntary, as proposed, or mandatory?*

    The interpretive guidance should remain voluntary. The reason for this is centered on the ability of the SEC to use accumulated experience from its regulatory examination, requests for interpretive clarification, court rulings and legislative changes to be taken into account in the future. Management needs interpretive guidance, like that provided in 2005, to assist in the design and creation of an effective process for reporting on internal control over financial reporting.

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

- (page 28, paragraph 2) Document conditions in which you would expect management to include general IT controls outside of those areas listed, e.g., network controls.

- (page 28, paragraph 2) Provide some clarification to those functional areas covered by general IT control areas that should not normally be considered to be part of the scope of examination of internal controls for financial reporting, such as capacity management and disaster recovery.

- Use consistent terminology with the PCAOB. For example, the PCAOB document refers to "IT general controls" and the SEC document refers to "general IT controls."

- (page 33, paragraph 1) Consider adding further detail and information on materiality, such as material weakness and significant deficiency, as the PCAOB did in its proposed draft standard. Also, the relationship between management's materiality levels and those of the public accounting firm should be addressed.

- (page 32) Provide more guidance on how to assess risk levels, i.e., low, high and medium.

- (page 37, paragraph 1) Consider providing an explanation or illustration of what is a "lower risk area."

- (page 22, last paragraph) Provide more specific examples of "financial reporting elements" to aid in performing the top-down risk assessment.

- (page 23, paragraph 1) Consider providing examples of "financial reporting risks" to consider, or point to a document that lists examples of them.

- (page 22, paragraph 2) Consider providing additional information on assessing changes to risks and controls, and document when further testing is required.

- (page 22, paragraph 2) Consider providing additional information on how management can place reliance on the ongoing monitoring performed by internal audit to lower the overall cost of compliance.

- Consider providing specific examples of situations in which no control testing—solely a control self-assessment—would be appropriate for management purposes (e.g., in which the risks of material misstatement and control failure are low).

- Consider adding an explanation in the introductory section of the guidance indicating the following: "Management has a responsibility that goes beyond that required by the Sarbanes-Oxley Act, to establish and maintain an appropriate system of controls to ensure that the company not only has reliable financial reporting, but also that it achieves its objectives related to efficiency and effectiveness of operations and compliance with laws and regulations. This release provides interpretive guidance only with respect to management's responsibilities related to controls over financial reporting and not to other objectives of internal control."

* * * *

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 SEC Guidance for Management's Reports on Internal Control over Financial Reporting—**Release No. 34-8762; 34-54976: File No. S7-24-06.** Because ISACA and ITGI represent many of the individuals engaged in Sarbanes-Oxley compliance efforts and have produced 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 SEC 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 Testing of the Operational Effectiveness of Controls by Management

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	Minimum or No Testing	Minimum Testing	Minimum Testing
	Low	Medium	High

Risk of a Control Failure

Definitions[3]

No Testing—Once management has ascertained that the control has been suitably designed and placed in operation, no further testing or evidence of operating effectiveness is necessary.

Minimum Testing—Ordinarily, this would consist of walkthrough or a control self-assessment, 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 or control self-assessment. 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.

[3] 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.