ISACA®
Serving IT Governance Professionals

IT GOVERNANCE INSTITUTE®
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*

18 September 2006

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.:*** S7-11-06

Dear SEC Board Members:

We very much appreciate the opportunity to provide comments and recommendations to the Securities and Exchange Commission (SEC) Concept Release Concerning Management's Reports on Internal Control over Financial Reporting—**Release No. 34-54122; File No. S7-11-06.**

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.

Responses to Primary SEC Questions of Interest

Based on our review of the SEC Concept Paper, and the core competencies of ISACA and ITGI, the following SEC questions were our primary focus, and are addressed first:

28. How have companies been able to use technology to gain efficiency in evaluating the effectiveness of internal controls (e.g., by automating the effectiveness testing of automated controls or through benchmarking strategies)?
29. Is guidance needed to help companies determine which IT general controls should be tested?
30. Has management generally been utilizing proprietary IT frameworks as a guide in conducting the IT portion of their assessments? If so, which frameworks?
34. Is guidance needed about documentation for information technology controls?

28. How have companies been able to use technology to gain efficiency in evaluating the effectiveness of internal controls (e.g., by automating the effectiveness testing of automated controls or through benchmarking strategies)?

Although companies are striving to replace manual controls with automated controls, this is a task that requires a significant investment of capital to implement, and in some cases may necessitate overcoming certain cultural barriers. However, use of automated controls is emerging.

Once controls are automated, it will allow for automating tests of effectiveness through the use of continuous controls monitoring (CCM), which uses data analysis techniques to monitor all transactions for compliance with internal controls. CCM is not easily implemented, and successful implementation requires a detailed understanding of the transaction data and continued support from senior management. However, the efficiencies to be gained by the use of such technologies are significant and CCM can be used to efficiently monitor the ongoing effectiveness of controls. Adoption of technology to monitor the effectiveness of internal controls is gaining traction as a result of better harmonization of ERP systems, increased interest and support of corporations and their accountants, and significant improvements in the software required for automated monitoring of controls.

In addition, where companies have identified and implemented effective automated controls, benchmarking strategies can also be effectively applied.

29. Is guidance needed to help companies determine which IT general controls should be tested? How are companies determining which IT general controls could impact IT application controls directly related to the preparation of financial statements?

As a result of Sarbanes-Oxley Section 404, significant effort has been expended by management to determine whether specific IT general controls are in scope and which are not. We believe that guidance is needed, and there cannot be a one-size-fits-all solution. However, we have heard from a number of organizations who have found illustrative guidance, such as was provided in COSO's *Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting* and ITGI's *IT Control Objectives for Sarbanes-Oxley*,[1] to be very helpful. Providing guidance regarding a subset of IT controls that typically may affect the reliability of financial reporting, would be helpful to provide management guidance to determine which of their IT controls are relevant for Section 404 and should therefore be tested. The upcoming second edition of *IT Control Objectives for Sarbanes-Oxley* will provide additional clarification on which IT general controls are potentially important.

30. Has management generally been utilizing proprietary IT frameworks as a guide in conducting the IT portion of their assessments? If so, which frameworks? Which components of those frameworks have been particularly useful? Which components of those frameworks go beyond the objectives of reliable financial reporting?

An ISACA survey was conducted recently regarding year-two perspective on Sarbanes-Oxley.[2] When respondents were asked what IT governance/control framework was used for year two, 58 percent indicated they relied on *Control Objectives for Information and related Technology* (COBIT)[3] and 30 percent pointed to *IT Control Objectives for Sarbanes-Oxley.* COSO was used by 36 percent and internally developed approaches by 26 percent.

[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 draft of the second edition of *IT Control Objectives for Sarbanes-Oxley* was posted on both sites for an open public exposure period from 1 May to 30 June 2006.

[2] 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.

[3] COBIT is also available to the general public from *www.isaca.org* and *www.itgi.org*.

Additionally, a joint IMA/IIA survey conducted in 2006 sought out the opinions of controllers and chief audit executive early filers. There were slightly fewer than 3,000 respondents to the survey. When asked which framework was used to assess IT controls, 52 percent indicated they relied on *Control Objectives for Information and related Technology* (COBIT), 44 percent said they relied on COSO—1992, and 10 percent indicated ITGI's *IT Control Objectives for Sarbanes-Oxley.*

IT Control Objectives for Sarbanes-Oxley is a derivative of COBIT, and was created specifically to address the IT issues related to the financial reporting requirements of the Sarbanes-Oxley Act. 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.

34. *Is guidance needed about documentation for information technology controls? If so, is guidance needed for both documentation of the controls and documentation of the testing for the assessment?*

Yes, further guidance is needed on management's responsibility for documenting IT controls. *IT Control Objectives for Sarbanes-Oxley, 2nd Edition* begins to address this issue. Information technology controls are either process-driven, e.g., adding and removing users, or parameter-driven. The approach to process-driven controls is similar to the documentation and testing required for manual application controls.

For example, process documentation is required to show how a new authorized user is entered into a system. As an example of a parameter-driven control, password rules may be entered into the system requiring that passwords be eight alphanumeric characters in length and that they cannot be repeated.

Parameter-driven controls are tested during the system walkthroughs and a confirmation that they have not changed may be necessary near year-end. For example, during the system walkthrough, password rules may be viewed on a screen and printed out. Tests can be made to determine whether passwords that do not meet the rules are rejected. Provided the rules on the system correspond to management's password policy, no further testing would be required. Closer to year end, the password rules may be reviewed/tested again to ensure that they have not changed.

Responses to Select Other SEC Questions of Interest:
The following questions were evaluated, and responses prepared based on our overall perspective, as well as similar content covered in our May 2006 response to the SEC.

1. *Would additional guidance to management on how to evaluate the effectiveness of a company's internal control over financial reporting be useful? If so, would additional guidance be useful to all reporting companies subject to the Section 404 requirements or only to a sub-group of*

companies? What are the potential limitations to developing guidance that can be applied by most or all reporting companies subject to the Section 404 requirements?

Yes, additional guidance would be useful. Furthermore, any guidance issued will be utilized in the ever-expanding global business community. Consequently, we recommend that the SEC guidance be principles-based. Additionally, as recommended in the May 2005 SEC guidance, it should be top-down and risk-based. These recommendations have recently been endorsed by IFAC in its recent information paper on internal Controls.[4]

In response to the question of "potential limitations to developing guidance" for Section 404, we have firsthand experience. As worldwide organizations focusing on IT governance, ISACA and ITGI are interested in the global applicability of guidance. Prior to the passage of Sarbanes-Oxley, our international IT governance constituencies developed COBIT to address the full scope of internal control over IT. The IFAC document raises the issue of the scope of Sarbanes-Oxley internal control work, which focuses on one specific aspect of internal control, related to internal control over financial reporting. While COBIT is clearly accepted as the standard for IT governance frameworks, it is, not surprisingly, sometimes referred to as too broad for Sarbanes-Oxley. Consequently, we have developed a Sarbanes-Oxley-specific subset of COBIT, presented in our publication *IT Control Objectives for Sarbanes-Oxley*.

Sarbanes-Oxley is a US law, but legislators and regulators worldwide are considering governance, internal control and financial reporting guidance and standards. We understand that the SEC does not have the authority to change the law; however, the SEC guidance should consider these potential limitations.

5. *Would additional guidance in the format of a Commission rule be preferable to interpretive guidance? Why or why not?*

The additional guidance delivered through a SEC Commission rule would be preferred, for two reasons. The first deals with how prior interpretive guidance was received and utilized. Because it was in the form of FAQs, as opposed to a rule, many did not embrace and utilize it, which could have limited scope and reduced costs for a number of issuers. Second, if it were in the form of a rule, it would have higher standing and would help address managements' confusion over how they should or should not deal with AS2.

In practice, SEC interpretive guidance, such as that from May 2005, appears to have been applied very conservatively, resulting in increased costs being incurred by many companies. In many cases, management may have been focused solely on the interpretation the company's auditors and consultants, rather than performing their own interpretation of SEC guidance as the SEC was expecting.

9. *Should the guidance incorporate the May 16, 2005 "Staff Statement on Management's Report on Internal Control over Financial Reporting"? Should any portions of the May 16, 2005, guidance be modified or eliminated? Are there additional topics that the guidance should address that were*

[4] IFAC, *Internal Controls—A Review of Current Developments*, August 2006

not addressed by that statement? For example, are there any topics in the staff's "Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports Frequently Asked Questions (revised October 6, 2004)" that should be incorporated into any guidance the Commission might issue?

The May 2005 SEC guidance contained valuable management guidance to "reduce unnecessary costs and burdens without jeopardizing the benefits of the new requirements." We support the overarching message in the 2005 guidance, which stated that it is the responsibility of management, not the auditor, to determine the appropriate nature and form of internal controls for the company and to scope their evaluation procedures accordingly. This was also validated in the May 2006 Internal Control Roundtable.

One way to ensure that this guidance is heeded would be to ensure that it is incorporated into any management guidance issued by the SEC. This would also have the effect of eliminating any confusion between SEC management guidance and that of AS2—intended for the auditor for complying with Sarbanes-Oxley Section 404 (b), requiring the external auditor to review and report on management's assessment of internal control over financial reporting.

11. What guidance is needed to help management implement a "top-down, risk-based" approach to identifying risks to reliable financial reporting and the related internal controls?

Either principle-based guidance, with proper examples of the application of the principles, or actual implementation guidance would be highly appreciated by issuers.

In practice, it appears that management and auditors may have focused on the costly testing of control activities. At times, entity-level controls have been treated as activity-level controls, when in fact they include a robust risk assessment process, the monitoring of activities by many levels of management, and the documentation of how the board, CEO and CFO obtain and communicate the information required so that they can provide a 404 attestation. Additional guidance in this area would allow organizations to focus on the efficiencies that can be gained by more fully utilizing a top-down, risk-based approach.

The SEC should work through IFAC, COSO and other organizations to provide additional guidance, illustrations and best practices addressing how to apply the risk-based, top-down approach. ISACA/ITGI also would be very pleased to assist with the IT controls aspects of this guidance.

15. What guidance is needed about the role of entity-level controls in evaluating and assessing the effectiveness of internal control over financial reporting? What specific entity-level control issues should be addressed (e.g., GAAP expertise, the role of the audit committee, using entity-level controls rather than low-level account and transactional controls)? Should these issues be addressed differently for larger companies and smaller companies?

We believe that entity-level controls are very important in the assessment of internal control and boards should consider and act on company risks, including IT risks. Therefore, in the IT area we recommend principles-based IT control guidance, beginning at a high enterprise level, which will make the guidance appropriate for small to large organizations. This guidance should be directed to the board or audit committee level and begin with the principle that the board oversees the effectiveness of and controls over IT, with oversight from the financial organization.

Beyond high-level IT principles-based guidance, we believe there is a need to address implementation guidance differently for large and small companies, based on their degree of automation. Comprehensive IT governance frameworks, such as COBIT, exist, which allow companies to filter and select applicable control processes tailored to their individual scope and supporting judgment, supporting the one-size-does-not-fit-all principle. We would like to see guidance on when and how entity-level controls vs. low-level account and transactional controls should be used.

19. *What type of guidance would help explain how entity-level controls can reduce or eliminate the need for testing at the individual account or transaction level? If applicable, please provide specific examples of types of entity-level controls that have been useful in reducing testing elsewhere.*

Specific examples of entity-level controls that would successfully reduce or eliminate the need for testing at the individual account or transaction level would be most helpful. Instances where the SEC believes it would be improbable or impossible for an entity-level control to take the place of controls at the account or transaction level would also be beneficial. The role of IT general controls should also be addressed in this context.

Companies have effectively used entity-level controls over consolidation-level financial management reporting rather than transaction-level financial controls at decentralized and disparate geographically dispersed locations. By identifying and testing key controls at the consolidation level in one location, they have been able to limit the number of international entities in scope for Section 404 that had to perform testing locally.

Entity-level controls should always be reviewed in conjunction with some level of transaction- or detective-level controls review, as each serves as a check on the other. Entity-level controls make a statement about the “tone at the top” and create a “perception of monitoring” that helps deter conventional and collusive fraud. As an example, an IT control that addresses program changes sends the message that unauthorized changes to key processes are “on the radar” and a priority of management, but they do not, in most instances, guarantee that intentional or unintentional changes are not made. Transactional controls reviews, at some level, serve as a check on the effectiveness of the entity control and a further layer of control to prevent fraud.

As noted above, in many cases entity-level controls have been considered to be the equivalent of company-level controls. If entity-level controls were redefined as management controls, of which company-level controls would be a subset, then we could give good examples of how work at the transaction level could be reduced.

For example, program change is an area where companies often have deficiencies, e.g., a user has not signed off on a program change. It is also the area where a considerable amount of time is taken to test detailed controls. In many cases, companies use a help desk to collect statistics on program change errors and then report these statistics to management. Management then reviews the statistics and determines the underlying causes for program change errors and takes corrective action (monitoring control). As the monitoring control reduces the risk that a financially significant error could potentially occur, the amount of detailed control testing on how a program is tested and how a program change is moved to production (control activity) could be reduced. If the monitoring control were taken into account, the key control to ensure that a significant program error was not made would not be the user sign-off, but would instead be the management review of program change errors and subsequent corrective action. In practice, the monitoring control may be ignored by company management and accounting firms in determining their testing approach, creating a significant amount of time and effort in testing the program change control activities. Costs are then incurred to remediate control activity deficiencies.

20. Would guidance on how management's assessment can be based on evidence other than that derived from separate evaluation-type testing of controls, such as ongoing monitoring activities, be useful? What are some of the sources of evidence that companies find most useful in ongoing monitoring of control effectiveness? Would guidance be useful about how management's daily interaction with controls can be used to support its assessment?

Guidance focused on how ongoing monitoring activities can be used in management's assessment, as well as how management's daily interaction with controls can be used to support its assessment, would be useful. Today, management places much more reliance on monitoring controls, e.g., Six Sigma and performance metrics. It would be helpful if the information addressed instances where the SEC believes ongoing monitoring activities could be used vs. or in combination with separate evaluation-type testing. Some effective sources of evidence currently used by companies to indicate a strong control environment include:

- Type and number of calls to a whistleblower hotline
- 100 percent compliance with sign-off on the business code of conduct statement and evidence of reporting of conflicts and violations of the code of conduct to senior management and the audit committee
- Evidence of an effective internal audit function

Further direction and support for continuous control monitoring (CCM) technology is needed. The use of traditional auditing methods and programs will not provide the level of review needed to assure and reassure the investment community in the increasingly complex web of business. If the 2005 fraud report is even close to 5 percent revenue as the cost of fraud to the average company, it points out the large and growing need to invest in technology and reengineer audit plans for automation. The ability to address complex and collusive fraud will never be accomplished without the aid of existing, but seldom used, auditing/monitoring technology.

24. What type of guidance would be appropriate regarding the evaluation of identified internal control deficiencies? Are there particular issues in evaluating deficient controls that have only an indirect relationship to a specific financial statement account or disclosure? If so, what are some of the key considerations currently being used when evaluating the control deficiency?

Although we are confident we cannot get away from risk and careful enterprise risk management (ERM) processes as the best guidance for evaluating the impact and likelihood of control deficiencies, it would be beneficial for the SEC to address some of these issues in a more complete manner. For example, the SEC could issue an improved definition for a significant deficiency and material weakness to help companies more efficiently evaluate breakdowns in internal controls. Because the affect of IT is pervasive, each weakness in IT controls must be evaluated to see whether a significant deficiency or material weakness exists. General guidance currently provides that a deficiency in an important IT control, such as security, is at least a significant deficiency. Guidance from the SEC supporting this would be very helpful. Guidance regarding the conditions under which such a deficiency could ever, in isolation, rise to the level of a material weakness would also be extremely useful. Also, further guidance from the SEC could be helpful when a significant deficiency in IT control, which occurs repeatedly, and has not been resolved, should be classified as a material weakness.

Although some IT issues are directly tied to financial assertions, and it is easy to see why they cause a significant deficiency, other IT issues are not as clear-cut. For example, how could an issue in the network infrastructure or retention of backup data, which seems far removed from the direct financial reporting process of companies, ever be tied to a material weakness in a financial assertion? Guidance from the SEC in these areas would be useful in defining companies' in-scope internal controls and hence limit the cost going forward, as distance from the financial statement reporting process is being used by companies as a major consideration when evaluating such 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 48,000 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 Concept Release Concerning Management's Reports on Internal Control over Financial Reporting—**Release No. 34-54122; File No. S7-11 -06.** 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 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*)