

February 26, 2007

Office of the Secretary
Public Company Accounting Oversight Board
1666 K Street, N.W.
Washington, D.C. 20006-2803

Response e-mailed to: comments@pcaobus.org

Re: PCAOB Rulemaking Docket Matter No. 021

PROPOSED AUDITING STANDARD – AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS AND RELATED OTHER PROPOSALS

Dear Sir/Madam:

The Institute of Internal Auditors (The IIA) welcomes the opportunity to comment on the referenced proposals. Our comments are based on in-depth analysis and discussions, harnessing the experience of a core team of prominent chief audit executives from major U.S. corporations who serve on The Institute of Internal Auditors' Professional Issues Committee.

The following are our principal observations. Detailed responses to each of the questions contained in the proposals can be found in Attachment A.

1. The proposed standard is a clear improvement to the existing guidance in Auditing Standard Number 2 (AS2). However, we do recommend revising the order of the steps in the top-down approach as noted below.
 - Determine materiality level for planning purposes (what would constitute a material misstatement of the consolidated financial statements).
 - Identify significant accounts and locations.
 - Identify relevant assertions.
 - Assess the control environment and related risk of management override.
 - Identify and assess other company-level controls, including the period-end financial reporting process.
 - Identify major classes of transactions and significant processes.
 - Identify key controls.

The top-down approach is continued for IT General Controls:

- Determine which key controls of those identified in the last step above involve critical IT functionality (e.g., automated controls, key reports, or other functionality such as calculations, updates, and interfaces) relied upon to prevent or detect a material misstatement.

- Identify in-scope financially significant applications: applications containing critical IT functionality, or where an unauthorized change to data is at least reasonably likely not to be detected and result in a material misstatement of the financials.
 - Identify risks with IT general controls processes and related control objectives that provide assurance over the consistent operation of the automated controls or which protect the data from unauthorized change.
 - Identify key IT General Controls.
2. We believe the use of *judgment* is insufficiently emphasized in the proposed Standard. The Standard should require the auditor to always exercise professional judgment and ensure a true and fair assessment of the quality of the system of internal control.
 3. We recommend that “significant deficiency” should be redefined as a condition (generally one or more control deficiencies) that the auditor believes represents a risk to the business of such significance that it should be reported to the audit committee. This enables items to be classified and discussed with the audit committee that do not meet the test of representing a reasonable risk of significant error in future financial statements.

This change in the definition would allow the auditors to bring issues of importance to the attention of the audit committee without implying there is an unacceptable risk of error in the financial statements. To this end, we believe this recommended change to the definition of a significant deficiency will allow both appropriate communications to the audit committee and a realistic assessment of the quality of the system of internal control as of the assessment date.

4. As stated in our responses to the SEC in May and September 2006, The IIA continues to believe the intent and the benefit of the Sarbanes-Oxley Act¹ are met with only two attestations – namely, management’s attestation, and the external auditor’s attestation over management’s attestation.

We further believe that the third attestation – the auditors own report on internal control over financial reporting – represents a fundamentally unrealistic and unfair expectation on the part of the auditors, which in turns leads to operating inefficiencies and costs. The essence and sole responsibility of auditing is to give an opinion on management’s statement not to create a management statement. Making statements about operations status, financials, internal controls accomplishments, tone at the top, and strategy, is the sole responsibility of management and are duties that solely management has capacity to fulfill. For the auditors, the best auditing methodologies and techniques cannot compete nor make up for

- Management position in an organization
- Management responsibility over operations and processes
- Management accountability

Sarbanes-Oxley Act - §404. Management’s Assessment of Internal Controls. (b) “Internal control evaluation and reporting – with respect to internal control assessment required by subsection (a) each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagement issues or adopted by the Board (PCAOB). Any such attestation shall not be the subject of a separate engagement.

5. Additional guidance on the assessment of IT general controls would be valuable. This area represents a significant portion of the scope of work and efficiencies can be obtained. The scoping of IT General Controls (ITGC) continues to be a significant issue for both auditors and management. In a recent IIA survey almost 49% of the respondents felt their organizations' costs related to scoping ITGC were too high (see our attached survey results – Attachment C). We strongly suggest additional guidance, potentially incorporating material The IIA has included in its GAIT Methodology, be included in the Standard.
6. There is a great deal of value in the changes, and we encourage measures (including authoritative guidance on key items before the entire Standard is released) that will enable prompt implementation by the audit firms.
7. The clarification is excellent that the only controls to be tested are those required to prevent or detect a material misstatement of the consolidated financial statements.

The IIA would like to offer its assistance to the PCAOB in the development of their guidance. We have an extensive volunteer network of individuals with specific knowledge in this area that could be valuable contributors to the PCAOB.

The IIA welcomes the opportunity to discuss any and all of these recommendations with you.

Best regards,



David A. Richards, CIA, CPA

Attachment – (A) Detailed Comments to PCAOB Rulemaking Docket Matter No. 021
Attachment – (B) IIA's Response to SEC Release Nos. 33-8762; 34-54976; File No. S7-24-06
Attachment – (C) IIA's GAIN Survey Results – Scoping Information Technology General Controls (ITGC)

About The Institute of Internal Auditors

The IIA is the global voice, acknowledged leader, principal educator and recognized authority of the internal audit profession and maintains the *International Standards for the Professional Practice of Internal Auditing (Standards)*. These principles-based standards are recognized globally and are available in 25 languages. The IIA represents more than 130,000 members across the globe, and has 247 affiliates in 92 countries that serve members at the local level.

Attachment A
Institute of Internal Auditors (IIA)
Response to PCAOB Rulemaking Docket Matter No. 021

Questions from the proposals are in ***bold italics***, with IIA responses following.

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

The proposed standard is a clear improvement to the existing guidance in Auditing Standard Number 2 (AS2). It builds on the additional guidance from the Public Company Accounting Oversight Board (PCAOB) staff in their answer to Q38.

We have a number of observations and suggestions for further improvement:

- The order of the steps can be improved by including the activity of defining materiality as the first step in the approach. Since the scope of work for §404 should be limited to “testing only those controls necessary to obtain reasonable assurance about whether material weaknesses exist,” defining the level of error that would be involved is a critical first step. The discussion in paragraph 14 is limited and not included as part of the top-down approach section.
- We also believe that the above excerpted quote from the end of paragraph 16 should be given more prominence. It cannot be over-emphasized.
- The second step, before the assessment of company-level controls (we commend the use of this term, which is more appropriate than “entity-level”) should be the identification of significant accounts and locations. Although some areas of company-level controls (including those in the control environment) are quite separate and unaffected by the selection, a number of areas (including the period-end financial reporting process, shared service center operations, and IT information processing) are directly impacted by the selection of accounts. The review of activities and controls in the period-end financial reporting process should be limited to those relevant to significant accounts.

Further, the identification of significant locations affects a number of areas, including those in the control environment as well as in shared service centers, risks assessment, monitoring, etc. For example, a number of organizations’ control environment risks are heavily influenced by cultural and ethical differences. In addition, the adequacy of monitoring activities should be assessed based on the locations and portions of the business that are more significant to financial reporting.

- Additional guidance should be provided relative to the selection of significant accounts. The proposed standard does not explain why significant accounts should be identified, which may lead to the inappropriate selection of too many accounts. We suggest paragraph 25 should include a reference to the definition of a significant account in paragraph A11. In addition, a definition of a significant location should be included in paragraph 29, consistent with the definition of a significant account.

- The control environment should be assessed prior to other company-level controls. The results should be used in assessing the risk of control failure, especially management override. We recommend establishing control environment as a separate step, prior to company-level controls.
- The period-end financial reporting process includes, in addition to those listed, other important controls that may be key higher level controls: period-to-period, budget to actual, forecast to actual, and other variance and trend analyses and financial metrics. These key controls may be selected for testing rather than activity level controls, especially for accounts that are not expected to fluctuate significantly or are close to the materiality level. In addition, the strength of these controls can influence the assessment of risk related to controls at the activity level.
- Although the auditor must perform his or her own assessment, we believe the auditor should be encouraged to discuss his or her top-down approach and make every reasonable effort to understand the opinions of management on such matters as materiality and significant accounts and locations. Such discussions between the auditor and management should occur early on in the process and on a regular basis during the engagement. Gaining management’s insights on materiality and significant accounts in the beginning is crucial to an ongoing dialogue that facilitates an efficient engagement.
- The term “key control” is now generally accepted and we suggest the PCAOB adopt it in the standard.
- The scoping of IT general controls (ITGC) continues to be a significant issue for both auditors and management. We strongly suggest additional guidance, potentially incorporating material The IIA has included in its GAIT Methodology, be included in the standard.
- We have noted significant variance in the level of work audit firms are performing relating to walkthroughs of automated application controls. While some have joint financial and IT audit specialists performing walkthroughs together by way of interviews and observation of processing, others are tracing transactions through complex IT applications. On occasion, they are performing more detailed work on a walkthrough than is required to test the operation of the automated control. Additional guidance in this area to enable efficiency and consistency would be valuable.

We recommend the top-down approach be amended as follows:

Current Steps	Recommended Steps
	Determine materiality level for planning purposes (what would constitute a material misstatement of the consolidated financial statements)
Identify and assess company-level controls	
Identify significant accounts and locations	Identify significant accounts and locations
Identify relevant assertions	Identify relevant assertions

	Assess the control environment and related risk of management override and other control failures at either company or activity level
	Identify and assess other company-level controls, including the period-end financial reporting process and the risk of management override of controls
Identify major classes of transactions and significant processes	Identify major classes of transactions and significant processes
Identify key controls	Identify key controls

The top-down approach is continued for IT general controls:

- Determine which key controls of those identified in the last step above involve critical IT functionality (e.g., automated controls, key reports, or other functionality such as calculations, updates, and interfaces) relied upon to prevent or detect a material misstatement.
- Identify in-scope financially significant applications: applications containing critical IT functionality, or where an unauthorized change to data is at least reasonably likely not to be detected and result in a material misstatement of the financials.
- Identify risks with IT general controls processes and related control objectives that provide assurance over the consistent operation of the automated controls or which protect the data from unauthorized change.
- Identify key IT general controls.

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

The proposed standard places sufficient emphasis on the importance of controls that prevent or detect fraud that results in a material misstatement of the financials.

We have a concern related to the use in paragraphs 45 of the phrases “company’s *programs* and controls” and in paragraph 78 “*antifraud program*” (emphasis added). The assessment should be limited to the adequacy of controls that prevent or detect fraud that could result in a material misstatement. Inclusion of the word “program” has the effect of influencing audit firms to assess whether the company has a specific, formal anti-fraud program. Even if the company has effective controls to prevent or detect fraud, the audit firms may suggest (based on paragraph 78) that the failure to have a formal anti-fraud program is not only a deficiency but potentially at least a significant deficiency. Since there is currently no requirement that a “program” be in place, we believe it could create an “opportunistic” environment to suggest one is necessary, as opposed to controls aimed at preventing or detecting fraud. Adequate controls and processes will make more impact in fraud prevention and detection than suggesting that a purchased program could prevent fraud.

There is a substantial linkage between the results of the assessment of the Control Environment and the risk of fraud. Studies of fraud risk have shown risks to be higher when there are environmental factors such as poor 'tone at the top' or employee morale. We recommend that the standard discuss these factors as well as others that affect the likelihood of fraud, such as the liquid nature of assets, and explain how the assessment and testing of fraud-related controls are affected.

The proposed standard should also require the consideration of these fraud risk indicators when assessing control deficiencies in areas where the risk is primarily fraud, e.g., IT security, approvals of credit memos, physical inventory adjustments, etc.

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

We agree that the top-down, risk-based approach is critical if the scope of work is to be effective and efficient. We believe the suggestions and comments in our response to question 1 above are *essential* improvements. The definitions of significant account and significant location are very important. The area most in need of additional guidance and tightening of scope is ITGC.

With respect to the discussion of materiality in paragraph 14, one of the major audit firms has informed us that their methodology requires them to allocate tolerable error to each location. They identify significant accounts at each location based on this allocated tolerable error, resulting in the need to test additional controls for the financial statement portion of their audit: controls that are not part of their scope of work for the assessment of internal control over financial reporting.

We recommend that the standard address this issue. The same set of controls should satisfy both elements of the integrated audit, and should be set based on consolidated and not allocated materiality.

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?

The discussions in the proposed standard on company-level controls are important and provide improved guidance compared to the current standard. Please see also our response to question 1.

Improvements can be made in the following ways:

- In both paragraphs 17 and 41, the auditor is guided to "test those controls that are *important* (emphasis added) to the auditor's conclusion." This language is weaker than the language in paragraph 16: "The top-down approach thereby leads to the auditor testing only those controls necessary to obtain reasonable assurance about whether material weaknesses exist." We strongly urge PCAOB staff to define the controls to test consistently as only those necessary to obtain reasonable assurance about whether material weaknesses exist. Using the term "important" allows controls at the company-level to be tested that do not meet this criterion.

- The language in paragraphs 41–44 could be improved to make it clearer that the auditor’s selection of controls to test could be at company-level or activity-level. The controls selected to test to address a specific risk could be singular or a combination of controls. The auditor should be guided to select that combination of controls that is both efficient and provides a reasonable level of assurance.
- Changing the order of the steps in the top-down process to position the identification of significant accounts and locations ahead of the discussion of company-level controls will improve the understanding of relevant company-level controls.
- Separating the discussion of control environment controls from company-level controls will also contribute to a better understanding as well as improved risk assessment practices.
- Paragraph 20 should be amended to include the following area to assess as part of the control environment:
 - Whether there are sufficient quality, experienced, and qualified personnel in all areas significant to internal control over financial reporting.
- The language “on a timely basis” is important when discussing detective controls. Our recommendation is to provide guidance that “on a timely basis” should be interpreted as sufficiently timely to avoid material errors in either the interim or annual financial statements.
- We believe the standard should include language on the auditor’s obligation to perform an efficient as well as an effective audit.
- The relevance of controls within the Committee of Sponsoring Organizations of the Treadway Commission (COSO) control environment, information and communications, risk assessment, and monitoring layers to the risk of material misstatement of the financials remains unclear. The proposed standard includes these areas in company-level controls but does not provide guidance on which controls in those areas, if any, should be selected for test or how an assessment of these controls impacts the overall risk assessment of the company.

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

Paragraphs 8 and 51–60 represent a reasonable introduction to the role of risk assessment and related evidence requirements. However, we believe further guidance is appropriate and necessary.

- While the level of work performed should be directly related to the risk, there is a point at which the level of work should be “none.” For example, if there is less than a reasonable likelihood that an account (or an account at a location) could contain a material misstatement, then no further work on controls related only to that account should be performed. While this is briefly stated in paragraph 8 of the standard, it bears repeating in the paragraphs relating to testing to ensure clarity and consistency.

- The identification of significant locations can affect the assessment of the controls environment and the risk of management override. Please see our response to question 1.
- The assessment of the controls environment and the risk of management override should be discussed further, as it may impact risk assessment of controls in the period-end financial process and at the activity level.
- As mentioned earlier, the scoping of work on ITGC that is risk-based is an important area and needs additional guidance.
- Although there is discussion on major classes of transactions, clear guidance is needed that controls over classes of transactions where there is less than a reasonable possibility that they might be the source of material misstatement do not have to be tested.
- We believe additional guidance is needed for the auditor's decision of whether exceptions found during testing indicate that a control deficiency exists. We have noted that when external auditors find one or two exceptions in a daily or more than daily control, they frequently do not extend the sample size or consider the results from management testing before asserting the existence of a control deficiency.

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

The performance of a walkthrough might be sufficient to provide reasonable assurance about both the design and operating effectiveness of certain controls. For example, a walkthrough might be sufficient when the frequency of control and/or the number of transactions is low. The auditor should be able to use judgment in making this decision.

As noted earlier, guidance on the performance of walkthroughs related to automated application controls would be valuable. In some cases, depending on how the walkthrough is performed, it may be sufficient to confirm that the automated control is adequately designed and operating effectively.

7. *Is the proposed definition of "significant" sufficiently descriptive to be applied in practice? Does it appropriately describe the kinds of potential misstatements that should lead the auditor to conclude that a control deficiency is a significant deficiency?*

The definition, unfortunately, continues to be less than clear and more than reasonably likely to result in inconsistent application. It also does not appear to meet the objectives of the SEC, namely that the audit committee is informed of all internal control deficiencies of significance. In the past, a number of control issues have been given the label "significant deficiency" when they do not necessarily indicate, as described in the definition in paragraph A12, "that there is a reasonable possibility that a significant misstatement of the company's annual or interim financial statements will not be prevented or detected." Examples would include the restatement of prior period financial statements as a result of errors identified in the current period, an ineffective internal audit department, or ineffective controls to prevent fraud (when there are strong controls to detect fraud and prevent misstatement of the financial statements).

We recommend that “significant deficiency” should be redefined as a condition (generally one or more control deficiencies) that the auditor believes represents a risk to the business (which may not be limited to the integrity of the financial statements) of such significance that it should be reported to the audit committee.

This change in the definition would allow the auditors to bring issues of importance to the attention of the audit committee without implying there is an unacceptable risk of error in the financial statements.

8. *Are auditors appropriately identifying material weaknesses in the absence of an actual material misstatement, whether identified by management or the auditor? How could the proposed standard on auditing internal control further encourage auditors to appropriately identify material weaknesses when an actual material misstatement has not occurred?*

The inappropriate identification of a material error in the absence of an actual material misstatement is not common in our experience. However, guidance has not been clear either for the auditor making the assessment, or for management to challenge the auditor’s assessment.

The proposed standard represents a risk that auditors will assess inappropriately the quality of the system of internal control when there has been a restatement due to a material misstatement in a prior period. Instead of considering specific facts and circumstances, auditors may believe that the existence of an error that leads to a restatement necessarily means there is at least a significant deficiency and potentially a material weakness.

The restatement of previously issued financial statements to reflect the correction of a misstatement, contrary to paragraph 79, should not be considered a strong indicator of a material weakness without other factors present indicating the cause of the error has a reasonable possibility of reoccurring.

By definition, the error occurred in a prior period and is not necessarily any indication that the current system of internal control is not adequate. For example, there may have been significant changes in the system of internal control since that period. Frequently, the improved system of internal control enabled management to identify the prior period error.

We suggest the PCAOB consider whether the root cause of a material misstatement in a prior period was the result of an event that was reviewed and agreed with the external auditor. The review and agreement by the external auditor should be prima facie evidence that reasonable steps were taken and there was no material weakness.

Rather than the restatement indicating a significant deficiency in the system of internal control as of the assessment date, many restatements indicate that the system of internal control is highly effective as of the assessment date.

As stated in the current version of Standard Number 2, even an effective system of internal control is not perfect and errors may occur.

“Internal control over financial reporting cannot provide absolute assurance of achieving financial reporting objectives because of its inherent limitations. Internal control over financial reporting is a process that involves human diligence and compliance and is subject to lapses in judgment and breakdowns resulting from human failures.”

A material error in a prior or current period can be the “once in a lifetime” exception that is (due to the presence of humans in the process) inevitable. One situation of which we know was the result of three unrelated controls happening to fail at the same time. The auditors agreed with management that this confluence, a perfect storm of control failures, was highly unlikely ever to occur again. However, guidance suggests that this would require an assessment of significant deficiency or material weakness. Yet, a reasonable official would not assess the design and operation of the system of internal control as of the assessment date as ineffective. In this situation, it is not logical and is even misleading to describe the same system of internal control effective three years, ineffective when there is a single exception, then effective again.

We recommend that an assessment that indicates the quality of the system of internal control as of the assessment date, and the assurance provided relative to the integrity of financial statements be filed with the SEC in the next year. That assessment would be more valuable and less misleading to the investor and other stakeholders.

The standard should require the following tests when a significant or material misstatement is detected in either the current or a prior period:

- Was the root cause of the misstatement a failure of internal control in the current period?
- Was the failure an isolated incident or did it indicate one or more control deficiencies?
- Is the control deficiency (or multiple control deficiencies) present as of the assessment date? If multiple control deficiencies contributed to the misstatement, are they reasonably likely to fail together?
- Would a prudent official conclude that there is a reasonable likelihood of a similar significant or material misstatement?

Our suggested redefinition of a significant deficiency would enable the auditors to bring all important internal controls, in their judgment, to the attention of the audit committee.

We believe the use of *judgment* is insufficiently emphasized in the proposed standard. The definitions are useful, especially when the changes noted above are made and the assessment truly is focused on the quality of the system of internal control as of the assessment date. The auditor should understand the principles and objectives of internal control, the purpose of their assessment, and use their judgment to assess deficiencies.

If judgment is given sufficient emphasis, paragraphs 78 and 79 are not needed and can be deleted in their entirety. Paragraph 77 is excellent and should be the last word on this topic.

If the PCAOB prefers to retain the discussion of areas that are more likely to be significant deficiencies, the descriptions of each area should allow for:

- Consideration of compensating and mitigating controls that reduce the risk of error in the financial statements.
- De minimis failures. Not all controls are equal and failure is not binary. For example, a control may require that a journal entry be approved by both the controller and the chief financial officer. If only one signed for one month without formally delegating to the other, the control technically fails as it is not operating as documented. However, the risk is probably low as at least one senior financial manager approved the entries.
- Application of the prudent official rule in paragraph 77, emphasizing the judgment of the auditor.

9. *Will the proposed changes to the definitions reduce the amount of effort devoted to identifying and analyzing deficiencies that do not present a reasonable possibility of material misstatement to the financial statements?*

In our response to question 8 above, we commented on the fact that the guidance in the existing and the proposed standard incorrectly guides the auditor to assessing as significant and even material weakness issues that do not present a reasonable possibility of material misstatement.

We agree with the need to ensure the audit committee is informed whenever there is an important issue relating to the system of internal control. However, including such issues as significant deficiencies in the current system of internal control results in misleading assessments. Items are being assessed as significant deficiencies and material weaknesses that are inconsistent with their definitions. Reporting the presence of significant and/or material weaknesses when the system of internal controls provides a reasonable level of assurance could mislead readers of the assessment.

Our recommended change to the definition of a significant deficiency will, we believe, allow both appropriate communications to the audit committee and a realistic assessment of the quality of the system of internal control as of the assessment date.

The standard should require the auditor always to exercise professional judgment and ensure a true and fair assessment of the quality of the system of internal control. The auditor should answer the question: “Does the system of internal control as of the assessment date provide reasonable assurance that material errors in the financial statements filed with the SEC would either be prevented or timely detected?” We believe the assessment should be based on the probability of material errors in the financial statements to be filed with the SEC in the next year, assuming no material changes in the design or operation of the system of internal control over financial reporting.

10. *Should the standard allow an auditor to conclude that no deficiency exists when one of the strong indicators is present? Will this change improve practice by allowing the use of greater judgment? Will this change lead to inconsistency in the evaluation of deficiencies?*

As noted above, we disagree with the strong indicators and recommend deletion of the section in its entirety. Please refer to our answers to questions 7–9.

11. Are further clarifications to the scope of the audit of internal control needed to avoid unnecessary testing?

We believe progress can still be made. The most important step would be to take every opportunity to repeat the guidance that the scope of work should be limited to accounts, locations, processes, transactions, and controls where there is at least a reasonable possibility of a material error in the financial statements. Controls should not be tested when it is already known, should they be found to fail, that they would not be material weaknesses.

This is especially true in the case of IT general controls. Failures in IT general controls only have an indirect effect on the risk of material error in the financials, so great care is needed to ensure unnecessary testing is avoided. The proposed standard does not advise the auditor as to how this can be done. Attached to this letter is a copy of our Guide to the Assessment of IT General Controls Scope Based on Risk (GAIT) Methodology, which we commend to the PCAOB as a potential source of ideas for additional guidance.

The sequence of steps in the top-down approach can be enhanced, as noted in our answer to question 1, to improve the efficient testing of company-level controls.

12. Should the reference to interim financial statements be removed from the definitions of significant deficiency and material weakness? If so, what would be the effect on the scope of the audit?

We have recommended that the assessment should be based on the probability of material errors in the financial statements to be filed with the SEC in the next year, assuming no material changes in the design or operation of the system of internal control over financial reporting. Those financial statements will include interim as well as annual financial statements. Therefore, the risk of misstatement of interim financial statements should remain part of the assessment of the quality of the system of internal control as of the assessment date, and part of the evaluation of deficiencies.

However, when planning and defining the scope of testing, materiality should be based on annual and not interim materiality levels. This should be more clearly stated in the standard in paragraph 14.

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

Removal of this requirement will have minimal impact (reduction) of external audit work. However, understanding management's assessment process, especially the identification of significant accounts, locations, and key controls, is an opportunity for the auditor.

We believe the external auditor should be encouraged to perform an efficient audit. The auditor should work with management (and the internal auditing function if they perform independent testing of controls for Section 404) to coordinate his or her work and reduce overall costs.

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

The auditor can certainly perform an effective audit of internal control over financial reporting without also evaluating management's assessment process. However, the auditor should be encouraged to work with management and the internal auditing function to perform an efficient audit.

15. Will an opinion only on the effectiveness of internal control, and not on management's assessment, more clearly communicate the scope and results of the auditor's work?

If the auditor performs an assessment of the effectiveness of the system of internal control but not of management assessment process, the opinion should be limited to the effectiveness of the system of internal control.

16. Does the proposed standard appropriately incorporate the value of cumulative knowledge?

The language in paragraphs 65–67 provides solid guidance in this area.

We disagree with the conditions for benchmarking in the proposed standard. Paragraph B31 requires all of the following:

- Adequate controls over:
 - i. Program changes
 - ii. Access to programs, and
 - iii. Computer operations
- Verification that the automated application control has not changed

The requirements should be modified to reflect the true nature and extent of risk to the continued operation of the automated application controls. The auditor should use his or her judgment to assess whether the conditions are met and benchmarking provides a reasonable level of assurance. Our concerns with B31 include the following:

- If it can be verified that the automated application control has not changed, there is no reliance on controls over program changes or on access to the programs. In fact, if it can be verified that automated application controls have not been changed, controls over program changes should not have been tested. Only those general controls where a failure would represent at least a reasonable likelihood of an undetected failure of automated applications controls (such that they are at least reasonably likely to fail to prevent or detect a material misstatement) or to the undetected change of data (that would lead to a material misstatement) should be included in the auditor's scope of work.

- Not all automated application controls are affected by or reliant on the proper operation of controls over computer operations.
- The auditor should use his or her judgment to assess the risk of IT general controls to the operation of automated application controls. For example, controls over program changes may be effective for some applications and not others. Decisions on the use of benchmarking should be based on an assessment of the quality of IT general controls and the risk to continued proper operation of automated applications controls.
- The risk of deliberate changes to automated application controls may be low, as there frequently is no benefit to the individual. (When assessing the risk of deliberate change to programs or data, similar factors should be considered to those relevant to the assessment of the likelihood of fraud: the ability to use the scheme to divert assets, the convertibility of assets, employee morale, etc.) In addition, unauthorized changes are likely either to result in application failures or other prompt detection by the users. Depending on specific facts and circumstances that should be assessed by the auditor, the risk to the proper operation of automated application controls presented by defects in access to programs may therefore also be low.
- When there are effective IT general controls, especially those over program changes, the auditor should be able to test a representative sample of automated application controls each year.

We would welcome the opportunity to discuss the specifics of benchmarking and applicable revisions to the standards with PCAOB staff.

17. What are the circumstances in which it would be appropriate for the auditor to rely upon the walkthrough procedures as sufficient evidence of operating effectiveness?

Please see our answer to question 6.

18. Will the proposed standard's approach for determining the scope of testing in a multi-location engagement result in more efficient multi-location audits?

We believe the goal will only be achieved by making the language clearer.

- The section that starts with paragraph B12 should directly state that the selection of locations or combination of locations (if and only if multiple simultaneous errors are at least reasonably possible) should be based on the consolidated financial statement materiality level, not on an allocated portion. One CPA firm shared their approach with us in January 2007:

“We analyze financial significance of each individual location (that is done through analysis of contribution of each individual location to consolidated results of operations), and based on this analysis determine the locations in-scope. Further, we identify (for each financially significant location) significant accounts that are material for each individual location. All of these procedures are fully compliant with A16 of AS2.

We do not believe that using consolidated materiality for determining significance of accounts for each individual location is appropriate (due to the aggregation issue, i.e., errors slightly less than consolidated materiality in two or three separate locations would aggregate to consolidated error of amount over consolidated materiality).”

- The conditions required for consideration of aggregation should be discussed. We suggest that the auditor should use his or her judgment to determine whether simultaneous multiple failures are at least reasonably possible. Conditions that might affect that assessment might include:
 - i. Whether the controls over transactions flowing into the same accounts at different locations are performed by the same people (e.g., at a shared service center).
 - ii. Common use of the same IT applications and/or key reports. (Note: it may only be necessary to test the automated controls if that is the only common risk among the different locations).
 - iii. The strength of company-level or other higher level controls (e.g., regional controls or controls at a business unit level).

19. Is the proposed standard's single framework for using the work of others appropriate for both an integrated audit and an audit of only financial statements? If different frameworks are necessary, how should the Board minimize the barriers to integration that might result?

The adoption of a single framework is a solid step in the right direction. Additional benefits can be achieved by guiding the auditor to consider the potential use of the work of others during the planning process. Discussions with appropriate parties should be held early to ensure that the work will be performed to quality standards and agree on the scope of work to be performed.

Including in the standard comments about the auditor’s responsibility to perform an efficient audit would be valuable. Relative to the use of the work of others, the guidance might stress the need for early planning and definition of the scope of work, and the possibility of increased reliance on the work of others.

20. Does the proposed definition of relevant activities adequately capture the correct scope of activities, including activities that are part of the monitoring component of internal control frameworks?

Paragraph 4 of the proposed standard defines relevant activities as:

“tests performed by others that provide evidence about the design and operating effectiveness of a company’s internal control over financial reporting or that provide evidence about potential misstatements of the company’s financial statements. Tests performed by others that provide such evidence typically are similar in nature, timing, and extent to the procedures that the auditor would have performed himself or herself as part of obtaining sufficient, competent evidence to support the auditor’s opinion.

We do not believe this is consistent with the intent of the PCAOB:

- The procedures described in paragraph 7 are not always “tests.” In particular, procedures performed when obtaining an understanding of the company’s internal control over financial reporting, and procedures performed when assessing risk, are not necessarily tests. For example, the auditor should be able to rely on walkthroughs or analytical reviews for risk assessment performed by internal auditors. We recommend the standard use the word *procedures* instead of *tests*, and extend the description to include any work that the auditor can use to reduce or eliminate tasks they otherwise would have to perform themselves.
- Management has a number of ways in which they can obtain assurance of the adequate operation of controls. They include the use of continuous monitoring or auditing techniques. These techniques may not be “similar in nature, timing, and extent to the procedures that the auditor would have performed,” but the auditor should have the ability to rely on them after assessing their adequacy.

21. Will requiring the auditor to understand whether relevant activities performed by others identified control deficiencies, fraud, or financial statement misstatements improve audit quality?

The requirement in paragraph 6 is important. However, we believe that this is already standard practice and therefore will not affect audit quality.

22. Is the principal evidence provision that was in AS No. 2 necessary to adequately address the auditor’s responsibilities to obtain sufficient evidence?

We agree with the change in the standard and the elimination of the principal evidence provision. The latter was not consistently interpreted and the new language enables the use of judgment.

23. Does the proposed standard provide an appropriate framework for evaluating the competence and objectivity of the persons performing the testing? Will this framework be sufficient to protect against inappropriate use of the work of others? Will it be too restrictive?

This is an area of specific interest to The IIA. We believe other factors to be considered when assessing competency and objectivity should include:

- Whether the individual’s activities are governed by a Code of Ethics, such as that of The IIA.
- Whether the individual or the department adheres to recognized standards that address quality and objectivity, such as *The International Standards for the Professional Practice of Internal Audit*.
- Whether the certifications held by the individual are relevant to the work performed.

We suggest that the objectivity of individuals who test matters in areas in which they work, even if they are not in supervisory positions, may be impaired (see paragraph 15a).

24. Has the Board identified the right factors for assessing competence and objectivity? Are there other factors the auditor should consider?

Please see our answer to question 23.

25. What will be the practical effect of including, as a factor of objectivity, a company's policies addressing compensation arrangements for individuals performing the testing?

This is an interesting addition to the factors to be considered. While we would prefer the auditor to assess compensation practices rather than policies (as there may not be formal policies on this topic), we agree that the factor should be included in some form. We recommend the language be revised to state:

“Compensation practices (such as bonuses related to successful testing results or to the absence of deficiencies) that might impair the objectivity either of the tester, the reviewer of the testing, or the individual responsible for the function.”

The practical effect should be positive, deterring the use of inappropriate bonuses.

26. Will requiring a walkthrough only for all significant processes reduce the number and detail of the walkthroughs performed without impairing audit quality?

In our experience, the auditors have only been performing walkthroughs for significant processes, so there should not be a major change. However, as stated earlier, we believe additional guidance is necessary to ensure consistency in walkthroughs of automated application controls.

27. Is it appropriate for the auditor to use others as direct assistance in performing walkthroughs? Should the proposed standard allow the auditor to more broadly use the work of others in performing walkthroughs?

The auditors should be able to use direct assistance for any activity normally performed by the auditor, applying professional judgment to the selection of tasks assigned and the level of supervision and review applied.

We believe the external auditor should be able to exercise professional judgment and rely on walkthroughs performed by others, if performed by competent and objective personnel. A number of internal audit functions already perform walkthroughs prior to testing. If there is an opportunity for the external auditor to rely on internal auditor walkthroughs, then we expect more internal audit functions would perform them.

28. Does the proposed standard on auditing internal control appropriately describe how auditors should scale the audit for the size and complexity of the company?

COSO's *Internal Control over Financial Reporting - Guidance for Smaller Public Companies* identifies a number of key considerations in its Executive Summary. These are captured in the proposed standard and we believe their description is appropriate and clear.

The issue of scalability, including the assessment of complexity, is part of and should be included in the risk assessment process. Many larger companies are relatively non-complex, and some smaller organizations have quite complex systems and processes. As COSO says, the principles in its *Guidance for Smaller Public Companies* should be considered by and are valuable for companies of all sizes. Our recommendation is to fold this discussion into the Risk Assessment process for companies of all sizes. The standard might indicate that some of the issues are more common in smaller companies.

29. Are there other attributes of smaller, less-complex companies that the auditor should consider when planning or performing the audit?

Please see our response to question 28.

30. Are there other differences related to internal control at smaller, less complex companies that the Board should include in the discussion of scaling the audit?

Please see our response to question 28.

31. Does the discussion of complexity within the section on scalability inappropriately limit the application of the scalability provisions in the proposed standard?

Please see our response to question 28.

32. Are the market capitalization and revenue thresholds described in the proposed standard meaningful measures of the size of a company for purposes of planning and performing an audit of internal control?

Please see our response to question 28. We do not believe the capitalization and revenue thresholds have practical application. The principles to be followed in risk assessment should apply to companies of all sizes.

33. Is there other information the auditor should provide the audit committee that would be useful in its pre-approval process for internal control-related services?

We believe one significant item of information should be provided: estimated fees, which are a direct proxy for the level of work to be performed. The regulations currently require only that the service be pre-approved. Some firms are relying on this to obtain agreement for the service from the audit committee and then negotiate fees with management. We recommend strongly that to preserve independence, the fees must be approved and not just the service.

34. How can the Board structure the effective date so as to best minimize disruption to on-going audits, but make the greater flexibility in the proposed standards available as early as possible? What factors should the Board consider in making this decision?

Early implementation of the clarifications and changes included in the proposed standards is both valuable and necessary. Companies and their auditors need to have certainty in their assessment and audit processes. We recommend that the PCAOB continue to move rapidly to obtain and review comments, make the necessary changes, and move towards as early an effective date as possible, and certainly this year.

Audit firms should be encouraged to be 'early adopters' of the proposed standard, as soon as the PCAOB is able to indicate which areas are likely to change and which are unlikely to change.

The PCAOB should consider making their answers to frequently asked questions authoritative, or provide them in a different form. One of the issues is that the guidance provided in past documents as well as the May 2005 policy statement, were not authoritative.

If the PCAOB were able to achieve the above, consideration should be given to using that facility to implement those portions of the revised standard that are generally accepted and can be adopted before the entire standard is effective.

February 26, 2007

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

Response e-mailed to: rule-comments@sec.gov

**Re: SEC Release Nos. 33-8762; 34-54976; File No. S7-24-06
MANAGEMENT'S REPORT ON INTERNAL CONTROL OVER FINANCIAL
REPORTING**

Dear Ms. Morris:

The Institute of Internal Auditors (The IIA) welcomes the opportunity to comment on the referenced release. Our comments are based on in-depth analysis and discussions, harnessing the experience of a core team of prominent chief audit executives from major U.S. corporations who serve on The Institute of Internal Auditors' Professional Issues Committee.

The following are our principal observations. Detailed responses to each of the questions contained in the release can be found in Attachment A.

The draft document prepared by the SEC staff is helpful in establishing clear general principles regarding management's assessment of internal control over financial reporting (ICFR). While we commend the SEC staff for this initiative, we do not believe the document fully addresses the pressing need of management — whether of large or small companies — for more detailed guidance in specific areas (such as the scoping of information technology general controls, see our attached survey results – Attachment C). We identified many of these areas in our comments dated September 18, 2006 on the Concept release.

The IIA recommends that the SEC staff proceed with the following steps:

- Refine the draft document as one documenting general principles, incorporating the items commented on in this response.
- Work with the Public Company Accounting Oversight Board (PCAOB) to upgrade Audit Standard No. 2; we have attached our comments on their revised standard draft – see Attachment B. The most efficient approach for management is to align its approach to that used by the external auditor, as discussed in our answer to question 1 in Attachment A.

- Additional detailed authoritative guidance can then be issued by the SEC where management's approach should vary or where clarification is necessary. For example, the external auditors need to follow existing standards when establishing materiality levels. Plain English guidance should be provided for management, who also need to establish materiality levels but are not required to follow auditing standards. This additional guidance could take the form of an authoritative Q&A.

Further, as stated in our responses to the SEC in May and September 2006, The IIA continues to believe the intent and the benefit of the Sarbanes-Oxley Act¹ are met with only two attestations – namely, management's attestation, and the external auditor's attestation over management's attestation. We believe that the third attestation – the auditors own report on internal control over financial reporting – represents a fundamentally unrealistic and unfair expectation on the part of the auditors, which in turns leads to operating inefficiencies and costs. The essence and sole responsibility of auditing is to give an opinion on management's statement not to create a management statement. Making statements about operations status, financials, internal controls accomplishments, tone at the top, and strategy, is the sole responsibility of management and are duties that solely management has capacity to fulfill. For the auditors, the best auditing methodologies and techniques cannot compete nor make up for

- Management position in an organization
- Management responsibility over operations and processes
- Management accountability

We also continue to believe that the principle of identifying areas as automatic sources of significant deficiencies and strong indicators of material weaknesses is inappropriate. Each situation should be assessed on its specific facts and circumstances, determining whether there is at least a reasonable likelihood of a significant or material misstatement of the financial statements.

An area of concern to our practitioners is that while the assessment date is the registrant's year-end, many, if not most, of the year-end procedures and controls are performed after year-end. The external auditors test those year-end controls and consider as deficiencies any failures in their execution, even though they are performed after the assessment date. We believe the assessment date should be changed to a date proximate to the filing date for the financials on Form 10-K (or equivalent). Guidance should limit tests of transactions to those included in year-end balances and tests of controls to those performed prior to the assessment date. We have included this recommendation in our response to the PCAOB.

One area not covered by our comments below, and where we believe additional guidance would be of value in both a general principles document and in detailed guidance, relates to the linkage between the annual assessment of internal control over financial reporting required by Section 404 of the U.S. Sarbanes-Oxley Act of 2002 and the certifications required under its Sections 302 and 906.

Sarbanes-Oxley Act - §404. Management's Assessment of Internal Controls. (b) "Internal control evaluation and reporting – with respect to internal control assessment required by subsection (a) each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagement issues or adopted by the Board (PCAOB). Any such attestation shall not be the subject of a separate engagement.

Again, The IIA would like to offer its support to the SEC in the development of their guidance. We have an extensive volunteer network of individuals with specific knowledge in this area that could be valuable contributors to the SEC.

The IIA welcomes the opportunity to discuss any and all of these recommendations with you. We would suggest spending two hours in an open dialogue with a few members of our volunteer network to discuss our comments, the basis for them, and suggestions that will support companies in their compliance efforts.

Best regards,



David A. Richards, CIA, CPA

Attachment – (A) Detailed Comments to SEC Release Nos. 33-8762; 34-54976; File No. S7-24-06
(included herein)

Attachment – (B) IIA's Response to PCAOB Rulemaking Docket Matter No. 021

Attachment – (C) IIA's GAIN Survey Results – Scoping Information Technology General
Controls (ITGC)

About The Institute of Internal Auditors

The IIA is the global voice, acknowledged leader, principal educator and recognized authority of the internal audit profession and maintains the *International Standards for the Professional Practice of Internal Auditing (Standards)*. These principles-based standards are recognized globally and are available in 25 languages. The IIA represents more than 130,000 members across the globe, and has 247 affiliates in 92 countries that serve members at the local level.

Attachment A
Institute of Internal Auditors (IIA)
Response to SEC Release Nos. 33-8762; 34-54976; File No. S7-24-06

Questions from the Release are **bolded**, with IIA responses following.

1. Will the proposed interpretive guidance be helpful to management in completing its annual evaluation process? Does the proposed guidance allow for management to conduct an efficient and effective evaluation? If not, why not?

We do not believe that the high-level interpretive guidance alone is sufficient to enable an efficient and effective evaluation. It does not address and provide guidance on the difficult issues for management. We refer the SEC staff to our prior comments (attached) on the Conceptual Release. We identified a number of areas (particularly in our answers to questions 11, 16, and 24) where more specific, practical guidance would be valuable.

To work toward providing more detailed guidance in difficult areas, we suggest that the SEC focus attention on the proposed standard issued by the PCAOB with consideration of how the standard will impact actions by management. While management does not have to follow the same process as the external auditors, there are significant advantages to following a process that is substantially the same. For example:

- Management desires an approach that is efficient when considering the cost of its own assessment and the external auditor's audit. One way to optimize costs is maximize reliance by the auditor on the work of management, which may be performed by the internal audit function. That is best obtained when the external auditor and management identify the same significant accounts and locations, and test the same key controls. The likelihood of reliance is enhanced when management's testing methods are similar to those preferred by the auditor.
- The work of the external auditor is more efficient when the auditor is able to review and benefit from management's risk assessment, identification of significant accounts and locations, and selection of key controls. If management and the auditor identify the same key controls, documentation of the design of those controls will be available for the auditor, and operating management will be better prepared to assist the auditor.
- When a process is used that is substantially the same, it is likely that both management and the auditor will identify the same deficiencies, compensating or mitigating controls, and arrive at the same assessment of their significance.

Our recommendation is for the SEC to work with the PCAOB to enhance its guidance to the external auditors. We have attached our response to the PCAOB with comments on the proposed revised standard. There are a number of areas where we disagree with the proposed standard, some of which also apply to sections of the SEC's draft interpretive guidance (e.g., the assessment of significant deficiencies and material weaknesses).

Once the PCAOB's standard has been updated and released, the SEC should issue guidance — potentially through *authoritative* questions and answers (Q&A) — on areas of difficulty for management. The SEC and the PCAOB should ensure consistent guidance is provided to auditors and management. The Q&A also can be used to explain how management may take different approaches to those required for the auditor. The Q&A should be focused on specific areas, for example the assessment of the control environment, where management may not be truly objective in assessing the tone at the top.

With respect to the control environment, we continue to believe there is too much focus in both the PCAOB and the SEC guidance on control activities. In our response to the Conceptual Release, we said:

“We suggest that SEC Staff perform an assessment of risk related to materially misstated financials, with particular reference to those incidents (many of which companies have become household names) that led to significant investor losses. The root causes should be identified. We believe that such an assessment will identify more issues existed within the COSO Controls Environment layer, with little risk within Control Activities.

“This assessment and the identification of root causes should determine what the Commission should require both of management and their auditors. The current approach under §404 and Auditing Standard 2 is not, in our opinion, addressing the root causes and therefore not providing the assurance to investor that the SEC and Congress desires.

“One alternative for consideration is the development, together with parties such as The IIA, the National Association of Corporate Directors, the AICPA, the FEI, and the Ethics and Compliance Officer Association, of a corporate governance standard. Companies could be asked to assess their practices against such a standard and explain any exceptions.”

We again make these recommendations.

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

Please see our answer to question 1 above.

The discussion of the role of entity-level controls needs to be repositioned and clarified. The first part in the evaluation process included in the draft (identifying financial reporting risks and controls) has five steps:

- Identify financial reporting risks.
- Identify controls that adequately address financial reporting risks.
- Consider entity-level controls.
- Role of general information technology controls.
- Evidential matter to support the assessment.

The order of these steps can be improved as consideration of entity-level controls should come before identifying controls placed in operations to address financial reporting risks. The identification and review of specific controls (i.e., control activities) discussed in the second step should only be performed after careful consideration of the entity-level controls — especially the control environment. With the recommended change in the order of these steps, the guidance would encourage the appropriate practice of assessing control activities only after considering the risk-based impact of the control environment.

- 3. 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?**

Please see our answer to question 1 and our response to the SEC dated September 18, 2006. Additional detailed guidance should be based on an updated PCAOB Auditing Standard No. 2, clarifying issues not sufficiently addressed in that standard or where additional guidance is required specifically for management.

- 4. Do the 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 was extremely valuable and remains relevant. There are no areas that should be retracted at this time.

If the SEC agrees with our recommended approach, the May 2005 FAQ can be used as a starting point for preparing the more detailed guidance we are recommending.

We recommend that the SEC work closely with the PCAOB to ensure that its guidance is authoritative for both management and the external auditor.

- 5. Will the proposed guidance require unnecessary changes to evaluation processes that companies have already established? If yes, please describe.**

The proposed guidance is general and should not affect established evaluation processes.

- 6. 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?**

Please see our response to question 1. The proposed interpretive guidance is high-level and does not conflict with the PCAOB’s draft standard. However, we disagree with a number of elements of the draft standard, some of which also apply to elements of the SEC’s draft guidance.

7. Are there any definitions included in the proposed interpretive guidance that are confusing or inappropriate and how would you change the definitions so identified?

We have proposed to the PCAOB a change in the definition of *significant deficiency* (please refer to our answers to their questions 7 and 8). Our recommendation is that *significant deficiency* be defined as:

“A condition (generally one or more control deficiencies) that the auditor believes represents a risk to the business (which may not be limited to the integrity of the financial statements) of such significance that it should be reported to the audit committee.”

We understand the intent of the SEC is to ensure all important matters related to the system of internal control are discussed with the audit committee. As a result of this intent, guidance in both the auditing standard and the interpretive guidance direct the assessment of control failure as significant deficiencies — even if they do not represent a reasonable risk of material misstatement in future periods — based on the quality of the system of internal control as of the assessment date. Examples discussed in our response to the PCAOB include the assessment as significant deficiencies restatements of previously issued financial statements to correct a material misstatement or the identification of a material misstatement by the auditor in the current period when it is not reasonably likely that an error would reoccur in future periods. In addition, the examples provided in footnote 74 of the proposed guidance define deficiencies as significant deficiencies without regard to their potential impact on the company, their likelihood of occurrence, etc. An assessment of risk elements should always be included in the determination of a significant deficiency.

8. Will the guidance for disclosures about material weaknesses result in sufficient information to investors and if not, how would you change the guidance?

We believe the guidance in paragraph B3 is sufficient. However, as stated above, we disagree with some of the guidance in paragraph B1 relative to the assessment of deficiencies.

9. Should the guidance be issued as an interpretation or should it, or any part, be codified as a Commission rule?

We believe that both the high-level guidance and the needed more detailed guidance should be codified as authoritative guidance, which can be in the form of an interpretation.

10. Are there any considerations unique to the evaluation of ICFR by a foreign private issuer that should be addressed in the guidance? If yes, what are they?

While we believe they should be addressed as recommended in our response to question 1 above, there are a number of issues relevant only for foreign issuers:

- The use of internal control frameworks other than COSO, and how their use may be reconciled to the external auditor's use of a different framework.
- Efficiencies that may be obtained by assessing controls not only over financial statements filed with the SEC, but also those filed with other countries' regulators.

- Reconciliations between financial statements prepared in accordance with the issuer's local GAAP with U.S. GAAP requirements.
- Varying governance standards and practices (e.g., the impact on the control environment of the absence of an audit committee).

**QUESTIONS ON THE PROPOSED REVISIONS TO EXCHANGE ACT RULES 13A-15(C)
AND 15D-15(C) AND RULES 1-02 AND 2-02 OF REGULATION S-X**

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

If the guidance is issued, compliance should be voluntary.

- 2. Is it necessary or useful to amend the rules if the proposed interpretive guidance is issued in final form, or are rule revisions unnecessary?**

We do not believe that the guidance addressing high-level principles is sufficiently detailed to support the assessment that management's evaluation was appropriate.

Assuming more detailed guidance is also prepared, rules revisions are not likely needed.

- 3. Should the rules be amended in a different manner in view of the proposed interpretive guidance?**

We recommend that the need to amend the rules be deferred until the updated PCAOB Auditing Standard No. 2 has been released and the need for additional management guidance is fully addressed.

- 4. Is it appropriate to provide the proposed assurance in Rules 13a-15 and 15d-15 that an evaluation conducted in accordance with the interpretive guidance will satisfy the evaluation requirement in the rules?**

Please see our answer to question 2 in this section.

- 5. Does the proposed revision offer too much or too little assurance to management that it is conducting a satisfactory evaluation if it complies with the interpretive guidance?**

Please see our answer to question 2 in this section.

- 6. Are the proposed revisions to Exchange Act Rules 13a-15(c) and 15d-15(c) sufficiently clear that management can conduct its evaluation using methods that differ from our interpretive guidance?**

Please see our answers to questions 2 and 3 in this section.

- 7. Do the proposed revisions to Rules 1-02(a)(2) and 2-02(f) of Regulation S-X effectively communicate the auditor's responsibility? Would another formulation better convey the auditor's role with respect to management's assessment and/or the auditor's reporting obligation?**

We understand that the requirement for the external auditor to review management's assessment will be removed, with the auditor only required to perform an independent assessment of the system of internal control.

We disagree with this decision. We believe the auditor should only attest to management's process as we recommended in our letter of September 18, 2006.

The revised language requires the auditor to "attest to, and report on, such [i.e., management's] assessment." It also requires the auditor to audit management's assessment. This language is not consistent with the intent of removing the requirement to review management's assessment. In fact, it supports our position that the auditor should only review and attest to management's assessment and not perform an independent audit of the system of internal control.

8. Should we consider changes to other definitions or rules in light of these proposed revisions?

As noted earlier, we believe the definition of a significant deficiency should be revised. It will enable all important internal control issues to be brought to the attention of the audit committee without misleading them or others that there is a risk of significant misstatement in future periods.

We also believe that the assessment of internal control should reflect the quality of the system of internal control as of the assessment date, and the assurance provided that there will not be material misstatement of financial statements to be filed with the SEC in the next year.

Further, we believe guidance should clarify that testing of events subsequent to the assessment date (e.g., the operation of controls involved in the preparation of the Form 10-K) should only be performed when clearly relevant to the assessment as of the assessment date. Tests of routine controls (e.g., approvals of vendor invoices) within a few days after the year-end are likely reflective of the quality of the system of internal control as of the effective date. However, testing the operation of controls in February for a December year-end company may not be reflective of the assessment date quality.

9. The proposed revision to Rule 2-02(f) highlights that disclaimers by the auditor would only be appropriate in the rare circumstance of a scope limitation. Does this adequately convey the narrow circumstances under which an auditor may disclaim an opinion under our proposed rule? Would another formulation provide better guidance to auditors?

We have no comment on this point.

COMMENTS ON THE COST AND BENEFITS OF THE PROPOSED AMENDMENTS

We request comment on the nature of the costs and benefits of the proposed amendments, including the likely responses of public companies and auditors concerning the introduction of new management guidance. We seek evidentiary support for the conclusions on the nature and magnitude of those costs and benefits, including data to quantify the costs and the value of the benefits described above. We seek estimates of these costs and benefits, as well as any costs and benefits not already identified, that may result from the adoption of these proposed amendments and issuance of interpretive guidance. With increased reliance on management judgment, will there be unintended consequences? We also request qualitative feedback and related evidentiary support relating to any benefits and costs we may have overlooked.

We do not believe the proposed guidance and rule amendments, with the exception of the removal of the requirement for the external auditor to provide an opinion on management's assessment, will result in significant change in companies' assessment processes. The proposed guidance of high-level principles is unlikely to have a fundamental impact on the processes most companies follow.

However, we do believe that detailed guidance on some specific issues — like those we identified in our response dated September 18, 2006 to the Concept release — could result in significant changes in a company's assessment process.

The proposed changes to Audit Standard No. 2, especially if our recommendations are adopted, should result in significant improvement in the efficiency of the external auditors' work, and accordingly, reductions in auditor fees.

QUESTIONS ON THE INITIAL REGULATORY FLEXIBILITY ANALYSIS

- 1. The number of small entity issuers that may be affected by the proposed extension;**
- 2. The existence or nature of the potential impact of the proposed amendments on small entity issuers discussed in the analysis; and**
- 3. How to quantify the impact of the proposed amendments.**

We do not believe the proposed interpretive guidance will result in a significant change in approach for small entity issuers.

Attachment C

Scoping Information Technology General Controls (ITGC)

Type: Executive Summary Report

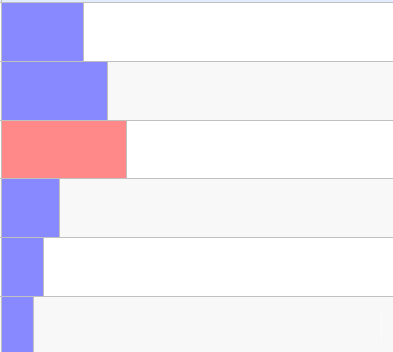
Date: 1/25/2007

Total invitations sent: 11,118

Total number of responses collected: 532 (4.79%)




1: What percentage of your organization's SOX 404 costs relate to ITGC?

(Respondents could only choose a **single** response)

Response	Chart	Frequency	Count
Less than 10%		18.7%	98
11-20%		25.2%	132
21-30%		29.6%	155
31-40%		12.6%	66
41-50%		8.6%	45
More than 50%		5.3%	28
Not Answered			8
		Valid Responses	524
		Total Responses	532

2: How do you feel about your organization's costs related to scoping ITGC for SOX 404?

(Respondents could only choose a **single** response)

Response	Chart	Frequency	Count
The costs are in line with what should be spent		41.5%	219
The costs are too high		48.7%	257
Neither (explained below)		9.8%	52
Not Answered			4
		Valid Responses	528
		Total Responses	532

2a: Additional comments regarding the organization's costs related to scoping ITGC for SOX 404:

Response
We are not a public company and therefore do not fall under Sox
Government Agency not subject to SOX at this point
No sox requirement
No sox requirements for company
Not enough spent on this. however, we are voluntary
SOX 404 does not apply to the school district
Glad to integrate into SOX process - more efficient for company
Costs are marginally too high
We are in Year One but we estimate costs to be 20-30%.
Overall costs are too high, but relative to non-IT costs, ITGC costs are in line
Not sure where the cost figure should be.
The costs were very high, but we did benefit. My issue is with the number of systems that were determined to be "in-scope" based on input from our external auditors.
Educational non-profit institution, but still interested in ITGC information

Attachment C

I don't feel there is good communication between external auditors for ITGC and operational controls, so the expense may be low.
We co-source the ITGC testing, so the cost will be higher than in house.
Not enough value is placed on the role of ITGC
We are a government agency and SOX does not apply
The learning curve is past its apogee and has now helped us to reduce the costs.
Not enough focus on ITGC to date
SOX compliance is not required
We don't have enough resources to adequately scope all ITGC needed.
We have not scheduled it yet as a Private Company.
We do not have SOX costs - we are a private company
Not doing enough around ITGC
Costs were due to remediation efforts
No funding for this
Our effort in this area needs to be more robust
ITGC costs are higher because they require a specific resource skill set
Not required to comply with SOX
Private company not subject to SOX
The costs are as low as we think they can be, given the requirement to evaluate general computer controls. However, given that backup/recovery has little to do with financial reporting, our overall costs could be reduced if this area was excluded.
SOX 404 do not apply to us.
We do not have to comply with SOX.
We simply don't agree with the scope that our external auditors require. If we relate overly broad scope to the excessive audit procedures required to fulfill it, then I suppose you could say that scoping costs are too high.
Probably disproportionately low
I think we need to spend more and rely on the scoping more
We are a not-for-profit and doing "lite-SOX"

External auditors get too focused on the controls as they apply to the financial systems. They ignore or minimize the controls relating to the running the business. Other systems are far more critical than the financial apps.
SOX is not currently applicable to my organization - it's NFP
We do not do enough in the area of ITGC
Do not have to comply with SOX
Not a company which falls under SOX 404 rules.
Hard to determine since the PCAOB SOX recommendations keep changing. They are moving in the right direction though.
Not affected
As a non-profit entity, the organization has not yet developed a full blown plan for the identification and testing of ITGCs.
We do not have to comply with SOX at this time.
As an OCC regulated bank, this is woven into our compliance program
The concern is overall cost on SOX404 and the efficient use of resources.
ITGC are extremely important for us whether or not they deal with SOX

Attachment C

3: Please rate how valuable you think guidance on scoping of ITGC would be:







		(1) Not Valuable At All	(2)	(3)	(4)	(5)	(6) Extremely Valuable	Total	Mean
How valuable do you feel guidance on the efficient scoping of ITGC would be?	Count	6	9	44	62	153	258	532	5.107
	% by Row	1.1%	1.7%	8.3%	11.7%	28.8%	48.5%	100.0%	
Total	Count	6	9	44	62	153	258	532	N/A
	% by Row	1.1%	1.7%	8.3%	11.7%	28.8%	48.5%	100.0%	

4: Please rate how you feel about the following efficiency factors related to scoping ITGC:

		(1) Not Efficient At All	(2)	(3)	(4)	(5)	(6) Extremely Efficient	Total	Mean
How do you feel about your organization's efficiency in scoping ITGC?	Count	28	64	172	151	74	12	501	3.429
	% by Row	5.6%	12.8%	34.3%	30.1%	14.8%	2.4%	100.0%	
How do you feel about your external auditor's efficiency in scoping ITGC?	Count	61	114	195	114	39	6	529	2.951
	% by Row	11.5%	21.6%	36.9%	21.6%	7.4%	1.1%	100.0%	
Total	Count	89	178	367	265	113	18	1030	N/A
	% by Row	8.6%	17.3%	35.6%	25.7%	11.0%	1.7%	100.0%	

5: Please select the title that best fits your current position:

(Respondents could only choose a **single** response)

Response	Chart	Frequency	Count
Chief Audit Executive (CAE)		32.1%	168
Audit Director		20.0%	105
Audit Manager		19.8%	104
IT Audit Director		6.9%	36
IT Audit Manager		10.7%	56
Other (specified below)		10.5%	55
Not Answered			1
		Valid Responses	524
		Total Responses	525

5a: Please select the other title that best fits your current position:

Response
Finance
IT Security Staff
VP Technology Controls and Compliance
IT Audit Supervisor
Audit Senior
Senior Internal Auditor
Director of Compliance
SOX 404 Manager
Compliance Manager
Director Internal Control

Attachment C

SOX 404
Compliance Director
Internal Control Manager
Senior Exec
Internal Auditor
Internal control manager
Internal Controls Senior Manager
Internal Audit
Accounting & SOX Manager
SOX Project Mgr/Assistant Controller
VP Audit
Compliance Manager
Staff
Controller
Consultant
Sr. Auditor
Audit Supervisor
Senior Leader, IT Audit
Director, Financial Controls
IT Supervisor
Asst. VP, IT Audit
Risk Manager
SOX IT Specialist
Sarbanes Oxley Compliance Manager
IT Compliance Manager
Director, Internal Controls

CEO
Sr. Manager Internal Accounting Controls
IT Auditor
IT Risk Analyst
SOX Manager
World-Wide SOX Director
Accounting manager
Financial Compliance
Consultant
SOX Team ITGC Liaison
Controller
SOX Auditor
Sr. IT Audit Mgr (Leading IT Audit function)
SOX Auditor
Staff
Internal Assurance, IMT Specialist
General Partner