The Institute of Internal Auditors

David A. Richards
Certified Internal Auditor
President

September 18, 2006

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: Release No. 34-54122; File No. S711-06
CONCEPT RELEASE CONCERNING MANAGEMENT'S REPORTS ON INTERNAL CONTROL OVER FINANCIAL REPORTING

Dear Ms. Morris:

The Institute of Internal Auditors (The IIA) welcomes the opportunity to comment on the referenced concept 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. We also conducted a focused survey, and obtained inputs from our other IIA technical committees and IIA members.

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

1. As stated in our response to the SEC in May 2006, The IIA continues to recommend a fundamental change be considered to legislation and PCAOB's Auditing Standards Number 2 be modified accordingly. Currently three attestations are being produced to provide assurance on internal controls over financial reporting:
    a. attestation from management
    b. attestation of the auditors on management's attestation
    c. independent report of the auditors on their assessment of internal control over financial reporting

We believe the intent and the benefit of the Sarbanes-Oxley Act[1] are met with only two attestations – namely, management's attestation, and the external auditor's attestation over management's attestation.

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.

Tel: +1-407-937-1200 • Fax: +1 407-937-1101 • E-mail: dave.richards@theiia.org

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 U.S.A.
Tel: +1-407-937-1100
Fax: +1-407-937-1101
www.theiia.org

This approach (two attestations) is prevalent in other securities trading markets and would provide for international consistency, harmonization, and fair treatment for corporations in a global economy. Requiring all three attestations creates a competitive disadvantage for U.S. companies, especially for those doing business abroad.

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

2. We believe additional guidance from the SEC directly to filers would be appropriate. All guidance should be principles-based and applicable to companies of all sizes and ownership. The guidance should emphasize the need for a top-down and risk-based approach and that only a reasonable level of assurance is required. New guidance should assist organizations in determining their appropriate level of risk tolerance and communicating that risk tolerance to their shareholders. We further believe that development and discussion of this guidance will result in the identification of required revisions and clarifications to PCAOB's Auditing Standard Number 2.

3. Further, we suggest that SEC ensure that all future guidance be consistent with *all* significant, acceptable frameworks, including COSO, Turnbull, etc. Not all registrants are US-based and may prefer alternative frameworks to COSO.

   We suggest that a critical first step in determining what changes in current requirements are needed would be for the SEC to perform an assessment of risk related to materially misstated financials, with particular reference to those incidents that led to significant investor losses. The root causes should be identified. We believe that such an assessment will identify that more issues exist within the COSO Controls Environment layer, with little risk within Control Activities. This assessment and identification of root causes should determine what the SEC should require both of management and their auditors. The current approach does not, in our opinion, address the root causes and therefore does not provide the assurance to investors that the SEC and Congress desire.

   One alternative for consideration is the development, together with parties such as The IIA, the National Association of Corporate Directors, the American Institute of Certified Public Accountants, the Financial Executives International, 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.

Another alternative would be for the SEC to consider an approach adopted by the AMF in France. In 2005, AMF commissioned a market-wide working group to establish a joint position on internal controls and an internal control assessment framework. The expectation was that the outcome would be endorsed by companies, regulators and auditors. The working group consisted of representatives from the listing exchanges, professional associations (internal audit and risk management), accountancy profession (chartered accountants), the chairs of the corporate directors and financial executives, and regulators from banking, treasury and insurance. The secretariat of the working group and writing of the guidance was delegated to The Institute of Internal Auditors.

Such a position and common assessment framework was developed and all stakeholders in the process from management to regulators have endorsed and follow the guidelines set forth by it. The IIA would welcome the opportunity to work with the SEC to explore the results of this framework and potentially establish the same within the U.S.

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 an SEC task force.

I welcome the opportunity to discuss any and all of these recommendations with you.

Best regards,

David A. Richards, CIA, CPA

Attachment – (A) Detailed Comments to SEC Concept Release, File No. S7-11-06
Attachment – (B) IIA SEC Response Year 2 Sox Implementation – May 2006
Attachment – (C) S*arbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners*

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 124,000 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 Concept Release, File No. S7-11-06

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

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?**

   All guidance should be principles-based and applicable to companies of all sizes. The guidance should emphasize the need for a top-down and risk-based approach and that only a reasonable level of assurance is required. Further, we suggest that SEC ensure that all future guidance be consistent with all acceptable frameworks, including COSO, Turnbull, etc.

2. **Are there special issues applicable to foreign private issuers that the Commission should consider in developing guidance to management on how to evaluate the effectiveness of a company's internal control over financial reporting? If so, what are these? Are such considerations applicable to all foreign private issuers or only to a sub-group of these filers?**

   Principles-based guidance should be applicable to all companies, including foreign private issuers. However, there may be areas of interest primarily to foreign issuers, such as the choice of an acceptable internal controls framework.

3. **Should additional guidance be limited to articulation of broad principles or should it be more detailed?**

   The guidance should be principles-based, but in sufficient detail (preferably with a variety of examples and definitions of key terms) to enable a clear and consistent understanding and application by issuers. Examples may be needed to ensure clear and consistent understanding. However, the examples should not transform the guidance from principles-based to rules-based, which has been the case to a large degree with PCAOB's Auditing Standard 2.

4. **Are there additional topics, beyond what is addressed in this Concept Release, that the Commission should consider issuing guidance on? If so, what are those topics?**

   All of the critical areas are addressed in the various questions and our answers in this document. In particular, we would like to reference our answer to question 11.

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

The answer depends on the guidance being provided. A Commission rule is critical when companies *and their auditors* are expected to adhere to the guidance and where sufficient detail is provided to ensure understanding. If the issue relates more to guidance that is recommended but not required, then a Commission rule is not necessary. As noted elsewhere, there are a number of areas where principles-based guidance from the Commission rule would have value. Currently, filers are forced, to varying degrees, to back into what is expected through direction from their external auditors who are in turn interpreting (inconsistently and perhaps not always accurately) PCAOB guidance.

6. What types of evaluation approaches have managements of accelerated filers found most effective and efficient in assessing internal control over financial reporting? What approaches have not worked, and why?

A top-down and risk-based approach that focuses on risks of material misstatement that are at least reasonably likely is the best approach, especially when also followed by the external auditor. Keys to the success of the evaluation work include:

a. It is top-down and risk-based.
b. The assessment is based on the principle of reasonable assurance; both management and the external auditor take a principles-based and not a rules-based approach.
c. Executive management provides leadership; all levels of operating management not only recognize the importance of the assessment but also ensure flawless execution of key controls.
d. The audit committee of the board of directors (or equivalent) monitors the status of the assessment on a routine basis.
e. Coordination and cooperation with the external auditor are close and consistent.
f. Scoping and planning for the year's work is completed early by both management and the auditor. Sufficient quality resources are assigned to perform the work.
g. Management and the external auditor have a common understanding of what represents materiality to the entity's financials, what constitutes a reasonable level of assurance, and what are "key controls." The latter includes not only an agreement of which controls are key, but what is meant by the term. A number of organizations have found the definition of a key control in The Institute's publication *Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioner* (The IIA's §404 Guide) very helpful. The guide is Attachment C.
h. Ensure a holistic, corporate-wide view of the program. This would include ensuring the appropriate identification of key controls as the result of a top-down and risk-based approach. It also includes corporate-wide standards for the quality of documentation and testing. Many organizations have achieved this through a corporate-level §404 project management or financial compliance organization; others have requested their corporate controller or the head of internal audit to provide this leadership.

i. Pay careful attention to the area of IT general controls. As discussed in our response to the May SEC Roundtable, this has been a difficult area both for registrants and their auditors. The IIA is sponsoring the development of guidance for the assessment of risk related to IT general controls as part of an organization's §404 risk assessment process (the GAIT project). The developing GAIT guidance is proving very useful for a number of companies in assessing risk in this area and then identifying related key IT general controls.

j. Process and controls documentation is kept current as the business changes, and controlled through a formal change management process.

k. The assessment process includes sufficient work during the year to allow the external auditor to perform walkthroughs and a significant part of their testing early in the third quarter. Management performs walkthroughs (which may also be performed by internal auditors) and tests of all key controls by midyear. Prompt attention is given to any control deficiencies to ensure prompt remediation and retesting. The earlier both management and external auditor testing can be performed (even if only for a partial sample size), the earlier potential deficiencies can be identified and remediated.

l. A large number of companies have found a self-assessment process effective, especially when combined with objective testing by the internal auditors. This can increase operating management's ownership of internal control and related risk management, as well as potentially reduce detailed attribute testing. However, this approach may not work well for all organizations.

m. Duplication of testing and "checking the checkers" is minimized. Criticism regarding the level of work, disruption of operations, and cost comes in part from organizations that have a management self-assessment or self-testing process, Sarbanes-Oxley project management office testing, internal auditor testing, and then external auditor testing. The most efficient processes entail a high level of coordination and cooperation among everybody involved, including not only reliance on others' work but also the sharing and agreement of standards, expectations, resource requirements, and timetables.

Approaches that have not worked include:

a. Following a strict rules-based approach, without regard to the underlying principle of reasonable assurance (whether this is the approach of management or the external auditor).

b. Using a checklist or inventory of risks and/or key controls, whether provided by a CPA firm, professional services provider, software vendor, or others. This may result in assessing key controls that are not related to the risk of material misstatement and/or omitting key controls that are.

c. Including risks and related controls because they have been problems before, whether in prior years' audits at the company or at other clients of the external auditor. This generates work that is not necessarily related to the risk of material misstatement for the current year at the company.

d. Allowing the scope to be set below the reasonably likely risk of material misstatement. Registrants have been *heavily* influenced by decisions made by their

external auditors, especially related to materiality. One firm has been starting with an agreed level of materiality, but then setting "planning materiality" (the quantitative level used in determining significant accounts) by applying a "haircut" that may be in two stages and brings accounts into scope that are as little as 40 percent of materiality – with no qualitative reasons for doing so. Other registrants' auditors have continued to want to keep the scope at the level where errors that are more than inconsequential but less than material will be identified

e. Only updating process and controls documentation prior to management testing, rather than keeping it current throughout the year. This creates risks that work will be delayed, controls may not be performed consistently through the year, process changes might introduce controls design weaknesses, and documentation is not updated to reflect actual year-end conditions.

f. Starting the assessment in the second half of the year, delaying identification of control deficiencies and limiting the time available for remediation. This compresses the timetable and creates pressure on limited resources, for both management and the external auditor.

g. Assessing the adequacy of internal controls over financial reporting based on prior period errors. Errors made in prior periods are not necessarily indicative of the quality of the system of internal control more than a year later.

h. Assessing the system of internal control over financial reporting as ineffective because material errors were detected by the external auditor during the year. The adequacy of a system of internal control should be evaluated based on whether its condition as of that point in time provides reasonable assurance that material errors would be prevented or detected in future financial statements filed with the SEC. As explained in COSO, internal control is a continuing process that is measured at a point in time. It is not perfect and there will be (primarily human) errors. While the fact that errors occur may indicate frailty, the level of continuing assurance needs to be assessed. Reasonable assurance acknowledges that errors will occur. The actualization of that probability does not mean the system of internal control is not effective and providing reasonable assurance.

7. Are there potential drawbacks to or other concerns about providing additional guidance that the Commission should consider? If so, what are they? How might those drawbacks or other concerns best be mitigated? Would more detailed Commission guidance hamper future efforts by others in this area?

We do not expect valuable guidance by others to be deterred by the fact that the Commission is providing guidance. Rather, we recommend that SEC ensure they are able to provide assistance through the review and comment on draft guidance developed by others. Where appropriate, SEC Staff should consider sponsoring or participating with others to develop guidance in difficult areas. For example, The IIA is sponsoring the development of guidance for the assessment of risk related to IT general controls as part of an organization's §404 risk assessment process (the GAIT project). Participation in any form by SEC Staff would be very welcome.

There is a risk that strict rules-based guidance would result in most companies adhering to the rules rather than using their judgment. Principles and risk-based guidance would require management to use their judgment to determine whether reasonable assurance is provided that material errors would be prevented or detected on a timely basis.

8. **Why have the majority of companies who have completed an assessment, domestic and foreign, selected the COSO framework rather than one of the other frameworks available, such as the Turnbull Report? Is it due to a lack of awareness, knowledge, training, pressure from auditors, or some other reason? Would companies benefit from the development of additional frameworks?**

   Most organizations have adopted the COSO Internal Controls Framework because of the level of existing knowledge within their organization (especially by their internal auditors, who provided many organizations with early leadership in this area), their consultants, and the major CPA firms. The latter generally have internal controls-related standards and procedures based on the concepts in COSO.

   Although some have expressed concern that COSO is not an effective framework for assessing internal controls, which is not the experience of most organizations, we believe COSO remains a solid foundation. Interpretive guidance in performing an assessment, typically but not necessarily based on COSO, carries value that is separate and distinct from the framework itself. We recommend priority be given to the interpretive guidance in performing an assessment, rather then developing additional frameworks.

   However, we suggest that SEC provide guidance in the selection of a controls framework in the following areas:

   - How COSO internal controls framework for smaller companies should be used as an application guide with the traditional COSO document.
   - How foreign issuers already using another framework (e.g., U.K. companies using the Turnbull framework) should choose which to use for §404. We would guide that foreign issues should in fact use those frameworks they are most comfortable with and are generally accepted within their countries and recognized globally.
   - The assessment of IT general controls. We understand that the SEC recommends that COBIT be considered a supplement to and not an alternative to COSO. If this is the case, it merits further discussion and explanation.

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 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 16, 2005 guidance was excellent and should be continued and expanded. It should be provided in a form that will encourage understanding and consistent compliance by both management and auditor. In particular, those aspects of the May guidance and related FAQs that are considered requirements (such as the top-down and risk-based approach and the focus on the risk of material misstatement) should be incorporated into new Commission rules.

Consideration should be given to requiring modifications to Auditing Standard Number 2 - in particular:

- Incorporate aspects of the May 2005 guidance that the external auditors are expected to follow.
- Reinforce the use of judgment and the view of the reasonable investor (rather than the reasonable or prudent official, which is not clear nor necessarily relevant to the assessment).
- Provide more guidance on the assessment of *material misstatement* and *remote likelihood* for scoping purposes. Commission staff should understand that existing guidance related to *reasonably possible* or *reasonably likely* is not plain English and therefore prone to misunderstanding and misapplication
- Where it suggests the assessment is based on control weaknesses that do not exist as of the date of assessment.
- Look into the appendices to the standard that are not consistent with the underlying principles of an assessment based on reasonable assurance and the use of judgment (with careful re-examination of those areas where a *rule* has been established that certain situations are always at least a significant deficiency and a strong indication of a material weakness).
- As noted above, the assessment should reflect the quality of the controls as of the date of assessment and whether they provide reasonable assurance that future material misstatements will be prevented or detected on a timely basis.

10. We also seek input on the appropriate role of outside auditors in connection with the management assessment required by Section 404(a) of Sarbanes-Oxley, and on the manner in which outside auditors provide the attestation required by Section 404(b). Should possible alternatives to the current approach be considered and if so, what? Would these alternatives provide investors with similar benefits without the same level of cost? How would these alternatives work?

In The IIA's May 1, 2006 input to the SEC's Roundtable, we indicated that the intent and the benefit of the Sarbanes-Oxley Act could be met with only two attestations: management's attestation of the effectiveness of the system of internal control over financial reporting and the external auditors' attestation over management's attestation. We continue to believe that investors are better served by limiting the role of the external auditors to audits of the financial statements (which provide assurance over those statements that have been filed and generally includes the testing of internal controls at the level required to provide that assurance) and a review of management's attestation process (which provides reasonable assurance related to financial statements that will be filed in future).

As a critical first step, we suggest that SEC perform an assessment of risk related to materially misstated financials, with particular reference to those incidents (companies many of which 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 of both 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 investors 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 American Institute of Certified Public Accountants, the Financial Executives International, 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.

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?

Guidance should be based on the PCAOB's suggested steps in their answer to FAQ 38. Each step should be reviewed and discussed. This is the approach taken in the IIA §404 Guide, which we recommend as a resource for the SEC staff developing the guidance.

Guidance should include:

a. A detailed discussion of materiality, with examples, and how it affects the scope of work to be performed.

b. What is "reasonable assurance" and what constitutes a "reasonable likelihood" of a material misstatement.

c. When the scope is the result of a risk-based assessment, how does *risk tolerance* relate? COSO ERM and the new framework for smaller companies both discuss risk tolerance and how the system of internal control should be sufficient to ensure risk is managed to those levels approved by management and the board. Does risk tolerance relate to reasonable assurance?

d. The assessment of the COSO controls environment layer and how it affects the assessment of risk for §404 (e.g., the selection of significant accounts and the identification of certain key controls in the controls activities layer, such as approvals for journal entries).

e. The assessment of other COSO layer activities that tend to operate at entity levels (monitoring, information and communications, and risk assessment) and their significance to the §404 assessment. COSO provides a high-level and general understanding of these layers, but not one that is focused on the risk of material error in the financial statements.

f. The identification of significant accounts and key locations.

g. The identification of key controls, with special attention given to the identification of key controls within IT business processes.

h. The testing of key controls, including whether both examination of evidence and specific re-performance are required; guidelines for testing automated controls; the use of benchmarking and base-lining for automated controls; and the extent, nature, timing, and documentation of testing.

i. Fraud assessment, focused on the risk of fraud or other deliberate error that could result in the material misstatement of the financials.

j. How registrants can report the results of their assessment, so that interested parties have a clear understanding of the quality of internal control over financial reporting as of the date of the assessment and whether there is a risk of misstatement in future filings. Since the annual assessment is included with financial statements that have been audited, the assessment of internal controls does not provide additional assurance of the quality of those financials, only of those being developed in the near future.

12. Does the existing guidance, which has been used by management of accelerated filers, provide sufficient information regarding the identification of controls that address the risks of material misstatement? Would additional guidance on identifying controls that address these risks be helpful?

The guidance provided by the Commission and the PCAOB is not sufficient and others, including The IIA in their §404 Guide, have developed additional guidance. In particular, we recommend to the Commission the definition of a key control, the discussion of aggregation, and the concept that assurance relates to future financial statements in the §404 Guide. The §404 Guide (which is attached) contains a number of points and clarifications in this area. The SEC's endorsement of such guidance, or development of similar guidance, would be valuable. Guidance from the SEC has the added benefit of helping management and their external auditors come to and apply a common understanding and approach.

We also refer you to our answer to question 10 of this document which focuses on the root cause of many material misstatements: defects within the control environment layer processes. Ensuring that management's and the external auditor's assessments of controls over the integrity of financial reporting are more appropriately focused on areas of real (rather than theoretical) risk would be of value.

13. In light of the forthcoming COSO guidance for smaller public companies, what additional guidance is necessary on risk assessment or the identification of controls that address the risks?

We believe principles-based guidance would be valuable to registrants of all sizes. That guidance should provide further interpretation of the frameworks sufficient to ensure a consistent and clear understanding and application. As noted above, we believe additional

guidance (or endorsement of existing guidance such as The IIA's §404 Guide) will have significant value.

14. In areas where companies identified significant start-up efforts in the first year (e.g., documentation of the design of controls and remediation of deficiencies) will the COSO guidance for smaller public companies adequately assist companies that have not yet complied with Section 404 to efficiently and effectively conduct a risk assessment and identify controls that address the risks? Are there areas that have not yet been addressed or need further emphasis?

As the Commission knows, The IIA is an active participant in COSO and endorses the new guidance for smaller public companies. This supplement to the COSO Internal Controls Framework is principles-based and therefore will provide value to those organizations using it. We encourage the SEC to indicate that the new framework is an acceptable one to use for registrants. As indicated in the Executive Summary, the COSO guidance for smaller public companies is intended to help them apply the principles of the COSO Internal Controls Framework.

With respect to the guidance necessary to determine an effective scope for the §404 assessment, we continue to believe that reinforcement and additional guidance on the top-down and risk-based approach (including guidance on risk tolerance, reasonable assurance, remote likelihood, materiality, etc) as detailed in our answer to question 11 would be valuable.

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 there is a significant lack of clarity and understanding when it comes to the term "entity-level." COSO tells us that controls within each of the layers exist both at entity and activity levels. However, the effectiveness and value of making a distinction and separately discussing controls at the entity and other levels is unclear. In fact, the use of terminology such as *higher-level* or *indirect* controls may be of more value that *entity-level* controls. The choice for many is between controls at a detailed "in the trenches" level, versus controls at a higher level.

There is merit in assessing the controls environment prior to other layers of COSO, as it can help assess risk at the significant account, process, and key control levels. In addition, this layer has been where the root causes were for most of the public failures (e.g., WorldCom, Enron, etc). We encourage guidance that places more focus on this level and less on detailed controls activities layer controls and procedures.

However, all other controls (whether they operate at the entity or activity levels) should be identified as the result of a top-down and risk-based approach. Once risks to the financial

statement are identified, controls may be identified that operate at corporate, region, shared service, or individual office levels.

Internal control practitioners, including our members, have used an approach that SEC might consider. This requires obtaining an understanding of the risks and then selecting the most effective *combination of controls* (including manual and automated controls, higher-level and detailed controls, and controls within various COSO layers) to provide reasonable assurance that the risks are addressed.

The choice of controls to be assessed as part of management's §404 program should be made based on which controls provide the most effective assurance over risks defined as the result of a top-down assessment.

There is value in guidance relative to all layers of the COSO model. The level of understanding is greatest at layers such as control activities, and least at controls environment, information and communications, and risk assessment. Not only is the level of understanding limited, but also how to apply the assessment of processes and controls at those levels. For example, what risk is present if corporate goals are not communicated to employees? What necessary activities should be performed within risk assessment?

Guidance relative to the choice of key controls would be valuable, including the use of higher-level controls. The guidance should stress the value of the top-down and risk-based approach, as this enables selection of the most efficient and effective controls.

Principles-based guidance that includes a top-down and risk-based approach is relevant and valuable to organizations of all sizes.

16. Should guidance be given about the appropriateness of and extent to which quantitative and qualitative factors, such as likelihood of an error, should be used when assessing risks and identifying controls for the entity? If so, what factors should be addressed in the guidance? If so, how should that guidance reflect the special characteristics and needs of smaller public companies?

We believe that guidance in the setting of materiality based on both quantitative and qualitative factors, and its subsequent use in determining scope for the §404 assessment, would be valuable. The guidance should consider:

a. Whether "materiality" is determined based on what would influence the reasonable investor, or some other basis.

b. How materiality is affected when results are volatile or the organization is in a loss situation.

c. What represents "reasonable assurance", or what is a reasonable quality of internal control given the size and nature of the organization. This is a question for companies of all sizes and types, not just smaller companies.

d. Many organizations have implemented enterprise risk management. Those organizations would benefit from a discussion of risk tolerance and how it relates to reasonable assurance. We believe that reasonable assurance is the appropriate level

of risk tolerance. The SEC staff may wish to review recent research by The Conference Board on enterprise risk management and setting of risk tolerance. Furthermore, several rating agencies such as Standard & Poors and Moody's have provided frameworks for evaluating a company's enterprise risk management process including the establishment of risk tolerance.

e. What level of likelihood is "more than remote." As noted above, linking "more than remote" to "reasonably likely" or "reasonably possible" is not clearly defined and is inconsistently applied in the context of internal controls.

Once risks that are at least reasonably likely to result in a material misstatement have been identified, it is possible to identify the key controls that will prevent or detect resulting material errors. Quantitative and qualitative factors affect risk, and do not directly affect the selection of key controls.

17. Should the Commission provide management with guidance about fraud controls? If so, what type of guidance? Is there existing private sector guidance that companies have found useful in this area? For example, have companies found the 2002 guidance issued by the AICPA Fraud Task Force entitled "Management Antifraud Programs and Controls" useful in assessing these risks and controls?

The §404 assessment should focus on the risk of material misstatement as a result of fraud or other deliberate acts. Unfortunately, the need to focus in this way is not well understood. Most of the guidance is general and relates to fraud prevention and detection in general rather than how fraud can result in material misstatement of the financials. This is discussed in the §404 Guide and further guidance in the same vein from the Commission would be of value.

One issue that merits consideration is the relationship between fraud risk and IT general controls security risks. The risk to the financials of IT general controls security weaknesses is not always assessed well in terms of the likelihood of an undetected material misstatement. Fraud likelihood is well-documented as being affected by a number of environmental and other factors (access to assets, rationalization, etc). These same factors affect the risk of deliberate acts using weaknesses in IT security

18. Should guidance be issued to help companies with multiple locations or business units to understand how those affect their risk assessment and control identification activities? How are companies currently determining which locations or units to test?

As noted above, successful organizations are using a top-down and risk-based approach to identify not only which locations or business units to include in their §404 scope, but also which accounts and processes at each location to include. The multi-location process recommended in PCAOB Auditing Standard 2 has been followed by most organizations.

The PCAOB's more detailed guidance in FAQ 16, dated June 23 2004, is clearer and we would support and encourage its use. It is more consistent with the top-down approach than the approach described in section B of Auditing Standard 2.

We suggest that SEC guidance should direct management and auditors to consider whether there are significant accounts with related processes at locations or business units where there is an inherent risk of a material error that is at least reasonably likely. This is a logical extension of the approach to identifying significant accounts; once an account is identified as significant, at which locations is there at least an inherent risk of a material error within that account.

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.

As noted above, we prefer the use of a top-down and risk-based approach to identify risk and the most effective combination of related controls – which may operate at any level within the organization.

We believe all key controls should be tested, and the nature, timing and extent of testing should be based on the level of risk (that the control may not perform consistently as designed, achieving its objective) and the frequency of operation of the control. The essence of an efficient and effective §404 assessment process is the selection of key controls.

When a top-down and risk-based approach is used, all controls that provide assurance that material misstatements are either prevented or detected can be identified – wherever they may occur. For example, it may be possible to identify an effective combination of:

a. Higher-level controls in the consolidation, corporate close, budget to actual, management performance review, standard costing, or other processes.

b. Controls at other locations or business units (for example, receiving controls at a warehouse can help with inventory shipping risks at a factory).

c. Automated controls that can be relied on instead of manual controls.

d. Increased or reduced reliance on key IT general controls, depending on risk and the presence of other controls.

e. Controls design improvements that will reduce the number of key controls (e.g., by implementing a high level review, such as a period-to-period comparison of payroll expense).

When higher-level controls are sufficient to prevent or detect a material error without detailed activity level controls, it may be possible to rely on these alone.

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 on-going 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?

There are a number of ways in which assurance of controls can be achieved, some of which approaches are relatively new. Some examples are continuous monitoring and data mining. As noted in the question, management has daily interaction with controls and may not require specific testing to know that certain controls are operating effectively as designed (e.g. management knows and does not need to test whether there are regular audit committee meetings and whether there is a business conduct guide.) Guidance on the various approaches would be valuable, but it needs to be linked to guidance to the external auditor as to how they can place reliance on management testing when such approaches are used.

21. What considerations are appropriate to ensure that the guidance is responsive to the special characteristics of entity-level controls and management at smaller public companies? What type of guidance would be useful to small public companies with regard to those areas?

We believe that principles-based guidance that emphasizes a top-down and risk-based approach, and focuses on reasonable assurance that material misstatements in future financials will be prevented or detected, is equally applicable to companies of all sizes and types.

SEC staff should consider the guidance for smaller companies recently published by COSO. Further, SEC staff should consider that the principles discussed in the guidance for smaller companies are applicable and of value for companies of all sizes.

22. In situations where management determines that separate evaluation-type testing is necessary, what type of additional guidance to assist management in varying the nature and extent of the evaluation procedures supporting its assessment would be helpful? Would guidance be useful on how risk, materiality, attributes of the controls themselves, and other factors play a role in the judgments about when to use separate evaluations versus relying on ongoing monitoring activities?

As noted above, guidance in how assurance is obtained has value. However, the guidance should certainly include reinforcement that the assessment should focus on the risk of material misstatement of the financials. If the risk of a material misstatement is less than reasonably likely, then it is not in scope.

Guidance on "separate evaluation" and how management should perform its testing, varying according to risk, would be of value.

23. Would guidance be useful on the timing of management testing of controls and the need to update evidence and conclusions from prior testing to the assessment "as of" date?

Such guidance would be of value, especially as interpretation of related PCAOB guidance has not been consistent.

We believe there would be value in explaining why only testing of controls over transactions (including the operation of automated controls) *during* the year is permitted. The assessment is as of the year-end and tests of the operation of a control during the week after the year-end

are more indicative of the quality of the control at year-end than tests of the control eight weeks prior to year-end. The current guidance, that tests be performed during the year, is a hold-over from financial statement auditing theory and not appropriate to an assessment of controls at a specific point in time.

Similarly, an explanation of why external auditors include financial reporting activities performed after the year-end date in their §404 scope tests of would be useful. We recognize that activities related to the annual financial statements continue into the first quarter of the new year. However, the assessment of the system of internal control is as of year-end and financial reporting activities that occur weeks and months after that date are not necessarily indicative of the quality of the system of internal control at year-end.

We recommend that the timing of testing should reflect the need to support an assessment of the system of internal control as of year-end. We would distinguish that from an assessment of the controls related to the 10-K for that year. Testing may include testing controls immediately after the year-end date when they are likely to reflect the quality of controls at year-end. However, testing of activities performed well after the year-end should be included only after a careful and considered assessment as to whether they are relevant to an assessment as of the year-end.

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?

Guidance would be of value in the following areas:

a. Aggregation of deficiencies. We recommend the assessment be based on the likelihood of all the deficiencies occurring simultaneously and resulting in a material misstatement.

b. The relevance of misstatements in prior periods, which can include earlier quarters in the current year.

c. Reasonable assurance, including its relationship to management's and the board's risk tolerance level.

d. What level of likelihood represents "at least reasonably possible."

e. The relevance of control failures other than directly in financial reporting. This occurs most often in compliance controls, where a failure could lead to a legal liability that is not recorded until the non-compliance is identified. We do not believe this represents a defect in control over financial reporting, but there is disagreement on this topic among external auditors, SEC counsel, and registrants.

f. The assessment of risk of material misstatements in future financial statements.

g. The assessment of deficiencies within IT general controls.

h. The assessment of accounting "errors", where the external auditor agreed at the time of the entry that it was appropriate. This should be prima facie evidence that reasonable assurance was present.

i. How the perspective of a "reasonable official" should be considered.

j. The relationship between the assessment for §404 and that required for §302, including whether the assessment for §302 is based only on the design of controls and does not include testing.

25. Would guidance be helpful regarding the definitions of the terms "material weakness" and "significant deficiency"? If so, please explain any issues that should be addressed in the guidance.

As noted above, further guidance on the elements of these definitions would be valuable:

- Reasonable assurance
- Material
- At least reasonably likely
- Inconsequential

26. Would guidance be useful on factors that management should consider in determining whether management could conclude that no material weakness in internal control over financial reporting exists despite the discovery of a need to correct a financial statement error as part of the financial statement close process? If so, please explain.

As noted above, we believe that the assessment should be based on whether the quality of internal control is such that it provides reasonable assurance that future filings with the SEC will not include material misstatements. Controls are not perfect and an effective system of internal control only provides reasonable and not total assurance. Rather than justifying (indicating a bias) a conclusion that no material weakness exists, guidance should assist organizations and their auditors assess whether:

- A control deficiency was the root cause of an undetected financial statement error that was material,
- It was an isolated incident,
- There continues to be a control deficiency (rather than a deficiency only during the prior period), and,
- There is more than a reasonable likelihood of a repetition in the near future.

Unfortunately, our experience is that most external auditors seem to believe that when there is a restatement they need to go to great lengths to justify why there is not a material weakness, rather than using judgment to determine the root cause and assess whether the quality of internal controls provides reasonable assurance as of the end of the year.

We also refer to our answer to question 27.

27. Would guidance be useful in addressing the circumstances under which a restatement of previously reported financial information would not lead to the conclusion that a material weakness exists in the company's internal control over financial reporting?

As in the prior question, this question appears to indicate a (erroneous) bias that a restatement is always the result of a control deficiency and that it should be considered a material weakness. We are also troubled by the assumption by some that a prior period error is indicative of a current period control deficiency.

As indicated publicly by the PCAOB, specific facts and circumstances need to be considered in every case. We do not believe that restatements automatically reflect a control deficiency in either prior or current periods when the prior estimates were reasonable based on credible evidence and judgment.

For example, it is our belief that when restatements are the result of a prior period's incorrect accounting that was reviewed and accepted by the external auditor, there is prima facie evidence that reasonable steps were taken and no material weakness exists. The system of internal control was operating at the level of reasonable, not perfect, assurance.

Other restatements have arisen when legal actions have led to judgments against the company that exceed current provisions; as a rule, we do not believe these restatements automatically reflect a control deficiency in either prior or current periods. A reasonable person would conclude that the prior estimates were reasonable (which assessment would have been reviewed by the external auditors) based on credible legal advice.

We also refer to our answer to question 26.

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)?

Technology has proved useful, to a varying number of companies, by:

a) Providing automated tools to manage the §404 assessment, including repositories for documentation and testing, dashboards for measuring progress, etc. (common practice).

b) Assisting with the testing of certain IT controls, such as restricted access and segregation of duties (common practice).

c) Enabling controls self-assessment (relatively common practice).

d) Enabling continuous monitoring (less common).

e) Testing application code to validate that it has not been changed (less common).

f) Supporting tests of activity (e.g., CAATs) that demonstrate control deficiencies did not lead to inappropriate activity (less common).

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?

The IIA has sponsored development of the GAIT methodology, which addresses the major part of this challenge: how to identify inherent risks (from potential IT business process

failures) to critical functionality in financially-significant applications, as a continuation of the top-down and risk-based approach. Key controls in IT general controls are then identified to address those risks.

We welcome guidance in this difficult area from the SEC and the opportunity for the GAIT team to assist in that endeavor. In the absence of current guidance that enables an identification of specific risks, many organizations are performing full IT general controls testing on all applications involved in financial reporting processes. As we indicated in our response to the recent SEC Roundtable, we believe that has led to excessive testing and resource costs among both registrants and their auditors.

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?

Many but not all organizations have been using the COBIT framework to supplement COSO. COBIT is a valuable product that we believe adds value to the selection of key controls within IT general controls once risks (preferably using GAIT) have been identified as the result of a top-down and risk-based process.

31. Were the levels of documentation performed by management in the initial years of completing the assessment beyond what was needed to identify controls for testing? If so, why (e.g., business reasons, auditor required, or unsure about "key" controls)? Would specific guidance help companies avoid this issue in the future? If so, what factors should be considered?

As indicated in our previous letters, the level of both documentation and testing was in many cases more than necessary in prior years. The documentation always has to be sufficient to support an understanding of the business processes related to significant accounts. That understanding then enables the efficient identification and selection for reliance of key controls. Necessarily, more than key controls will always be documented.

It should be noted that key benefits from Sarbanes-Oxley have been achieved for many organizations that either had documentation and process maps or used the initial year's efforts to create them – all for the purpose of improving their key transaction processes. These basic management tools did not always exist, yet when used, consistently improve the efficiency and effectiveness of the organization. The level of documentation and ease of its maintenance was driven by the experience and skills of the management team with process analysis and process mapping. While some companies paid large amounts to outside consultants to prepare them for the assessment, others were able to achieve their documentation goals without any external expenditure. Therefore, the costs cited by many organizations need to be thoroughly understood so that expenditures of time and effort necessary to overcome a lack of process management knowledge along with basic documentation and process infrastructure are not considered as inherent Sarbanes-Oxley compliance costs.

We have noted variation not only among registrants but also among audit firms in terms of what documentation they consider sufficient. Guidance from the SEC should enable a more consistent and, we trust, a more efficient standard.

32. What guidance is needed about the form, nature, and extent of documentation that management must maintain as evidence for its assessment of risks to financial reporting and control identification? Are there certain factors to consider in making judgments about the nature and extent of documentation (e.g., entity factors, process, or account complexity factors)? If so, what are they?

We have not found this a common area of difficulty and a principled standard should be sufficient (e.g., that the documentation be sufficient to support a broad understanding of processes and controls, the selection of key controls, and an assessment of the adequacy of their design).

33. What guidance is needed about the extent of documentation that management must maintain about its evaluation procedures that support its annual assessment of internal control over financial reporting?

We have not found this a common area of difficulty, but would support a high-level guidance statement.

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?

We do not believe that separate and distinct standards are needed, especially when the guidance is in the form of higher-level principles. Furthermore, as information technology supports the underlying business process, risk and control assessment should be focused first from the specific of that business process. Separate and distinct information technology standards may confuse that key point.

35. How might guidance be helpful in addressing the flexibility and cost containment needs of smaller public companies? What guidance is appropriate for smaller public companies with regard to documentation?

The majority of companies have cost-containment needs, not just smaller companies. All organizations should understand the minimum standards (based on high-level principles) and may choose to complete documentation at that or higher levels.

The question appears to recognize that a reasonable level of internal control assurance should take into account the cost of providing that control, especially when compared to the risk of misstatement. Unfortunately, cost is not a consideration in today's guidance and we welcome a contribution in this area by the SEC.

The Institute of Internal Auditors

May 1, 2006

David A. Richards, CIA
President

Tel: +1 407 937 1200
drichards@theiia.org

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: File Number 4-511 Public Comments on second-year experiences with Implementation of Internal Control Reporting and Auditing Provisions

Dear Ms. Morris:

The Institute of Internal Auditors (The IIA) welcomes the opportunity to comment on our members' second-year experiences with implementation of the Sarbanes-Oxley Act §404, Internal Control Reporting and Auditing Provisions.

Clearly, the first-year implementation of §404 provided many benefits. Most notable were a more engaged system of internal control over financial reporting with active participation by the board, audit committee, and management and a broader understanding of controls by personnel and management throughout the organization. However, it also created many challenges. These included questions regarding cost-benefits; its capacity to significantly impact the confidence of investors; the lack of balanced focus on financial reporting and other business risks; sustainability of the processes; and the redefinition of the relationship between management, internal audit, and external audit.

For this response, The IIA has focused on the evolution of both the benefits and challenges of §404, consolidating comparative experiences of filers that have been through two years of implementation. The following comments have been prepared using the feedback of chief audit executives of 131 organizations who responded to a comprehensive questionnaire (see Attachment A); prominent chief audit executives from Fortune 100 companies who serve on The IIA's Professional Issues Committee; focus groups composed of chief audit executives; and The IIA's Professional Practices staff.

Our overall conclusion is that, although progress has been made, the great majority of the issues identified in year one were still experienced in year two. On the benefits side, our survey results indicate that:

- Management was more successful in ensuring strong corporate governance and quality financial reporting than in year one. More than 75% of respondents believed their organization's §404 efforts have increased the reliability of controls over financial reporting and the vast majority of survey respondents indicated that their organizations have approached §404 with a long-term strategy to achieve sustainability, as opposed to doing the basics just to comply.

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 U.S.A.
Tel: +1-407-937-1100
Fax: +1-407-937-1101
www.theiia.org

- The average number of key controls identified by management decreased from 824 to 650, recognizing a more top-down approach by management. 42% of respondents stated that they used this approach in year one, while it was used 75% of the time in year two.

- The relationship between internal and external auditors has migrated from coexistence and coordination to coordination and integration, which indicates an improved risk assessment and audit-planning process.

- 35% of the respondents believed external auditors used their work and the overall audit plan was more effective in year two, up from just 11% in year one.

But, our survey results indicate there are still challenges to implementation:

- When comparing costs from year one to year two, organizations have gained cost efficiencies in their own processes (e.g., creating process documentation, testing key controls) To some degree, these efficiencies should continue to occur into future years. What is noteworthy, however, is that attestation and certification costs associated with SOX remained at the same level of cost for 41% of the respondents, with an additional 7% indicating that attestation costs had increased. In addition, more than 20% of respondents saw an increase in other audit services (e.g., tax) in year two over year one.

- The variance between guidance issued by PCAOB and actual practical experiences seems to be large. For example, in year two, 46% of our survey respondents believed that their external auditors utilized a risk-based and top-down approach as required by PCAOB Auditing Standard Number 2 (AS 2). During year two, 27% believed their external auditors focused their scope of §404 work on the identification of potential material weaknesses and performed only limited work on areas that were unlikely sources of material error. During year two, only 42% stated that their external auditors conducted an integrated audit. Sixty percent of respondents stated that their external auditors performed separate tests for the purpose of the audit of internal controls and the financial statement audit.

- Of the 75% of respondents using a top-down and risk-based approach, 30% of these respondents indicated that their organization did not see a more effective and efficient external audit process. In addition, 58% of the respondents indicated the external auditors tested controls that did not relate to a risk-based approach and that could not materially impact the financial statements. This practice is tremendously ineffective, does not follow AS 2 guidance and is driving costs up without benefits.

- Although the May and November 2005 guidance from the PCAOB was discussed between management and internal and external audit, this guidance was not followed according to 31% (May) and 25% (November) of our survey participants. The reasons most often provided were that the guidance came too

late in the process and/or it was not given the same weight by the external auditors because it was not a "standard" but only informal guidance. We believe that AS 2 should be amended to include the messages from the May guidance and any appropriate guidance going forward.

- Though external auditors relied on internal auditors' work to a greater extent, the degree remains relatively low. Our results indicated that 48% of our respondents committed over 51% of their total internal audit resources to §404. And while many departments dedicated over 51% of their time to §404 work, 44% responded that the extent (percentage of total cost) that the external auditors reduced their work due to reliance on internal audit's work was less than 10%. This diversion of internal audit resources for seemingly little gain in efficiencies and effectiveness cannot continue. 60% of respondents believe that their internal audit resources were diverted away from areas that were high to moderate in risk, which, if audited, would have provided greater value to the organization.

In addition, new challenges to implementation arose in year two:

- Survey results indicated that 34% of respondents believe that, to significantly reduce external audit costs, a major driver will be the alignment of PCAOB guidance and accounting firm inspections.

- 33% of the respondents whose external auditor received a PCAOB inspection report did not share the results of the report with the company. We believe that senior management, internal auditing, and the audit committee should be apprised of inspection results of the firm they employ for financial statement audits as a matter of transparency and to ensure improved future efficiencies.

In order to address a critical impediment to long-term sustainability and to achieve a cost and benefit acceptance of §404 from both corporations and investors: The IIA recommends a fundamental change be considered and AS 2 be modified accordingly. Currently three attestations are being produced to provide assurance on internal controls over financial reporting: management's attestation; the external auditor's attestation over management's attestation; and, the external auditor's own attestation over internal control.

We believe that the intent and the benefit of the Sarbanes-Oxley Act[1] are met with only two attestations – namely, management's attestation, and the external auditor's attestation over management's attestation. This approach is prevalent in other securities trading markets (e.g., Canada - Ontario Securities Commission regulation – CSA notice

[1] Sarbanes-Oxley Act – §404. Management 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 engagements issues or adopted by the Board (PCAOB). Any such attestation shall not be the subject of a separate engagement.

52 -313; and, France - Loi sur la Sécurite Financière article 117 & 120), and would provide for consistency internationally, harmonization, and fair treatment for corporation in a global economy. Also, in the United Kingdom, The Combined Code on Corporate Governance only requires boards to review the effectiveness of all internal control (not just financial control) and report publicly that they have done so. External auditors will review such reports, essentially for consistency with their knowledge gained in other work, but do not audit the disclosure in any sense equivalent to the §404 requirement. Thus, UK companies do not provide any external reporting on internal control effectiveness and do not have a requirement of attestations, either by management or external auditors. Requiring all three attestations creates a competitive disadvantage for U.S. companies, especially for those doing business abroad. If only two attestations are required, comment relating to the external auditor's attestation below would not be relevant.

The IIA recognizes that the above proposed change would require some time to consider and implement, thus, the following summarizes what we believe to be the key issues that continue to be germane for improvements to the §404 implementation process as it currently exists:

I. Additional guidance is needed for both management and audit firms
II. There remains a need for increased reliance on the work of others
III. Continued improvement in the effectiveness and efficiency of the §404 process

The above key issues should be considered a priority for expected impact on year 3. Additional suggestions that we believe will further improve the 404 process are discussed in Attachment C below. We recommend that you address those as priorities permit.

IIA's Recommendations for Improvement

I. Additional Guidance Needed for Both Management and Audit Firms

A. 75% of our survey respondents believe that additional detailed guidance for management is needed regarding the §404 control assessment process and the quarterly §302 assessment process. We believe the audit process will become more proficient when management's assessment process becomes more efficient. We encourage the U.S. Securities and Exchange Commission to consider finding ways to provide more guidance to management to promote efficiencies in management's assessment of internal controls over financial reporting. Such guidance should provide management with the knowledge and tools to properly identify risks and key controls, build the assessment processes, and provide for consistent transparent disclosures of material weaknesses and their remediation. Without such guidance, management relies on the guidance provided by PCAOB to the external auditors, which was not intended to guide management's implementation of §302 and §404.

As a means of trying to fill the void in management guidance voiced by our members, The IIA has recently issued, *Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners* (Attachment B). Written for management by experienced internal auditors who have worked on internal controls hand-in-hand with their organization's external auditors, audit committees, and management, it incorporates and reflects up-to-date guidance from the SEC and PCAOB.

B. The SEC, PCAOB and/or other appropriate bodies should collaborate to ensure there is an effective resolution process for differences of opinion between registrants and their auditors. Examples include when the issue may not be quantifiable, involves judgment on something such as the sufficiency and extent of documentation that may be needed, or in situations where future events, such as loan losses, bad debts, contingent liabilities, or potential legal actions may require reserves to be established. Even if models are used to forecast potential outcomes based on past history, there is still the need to apply judgment. Professional judgment must be exercised when it comes to assessing the likelihood that exceptions found as a result of audit tests will actually result in misstatements of accounts. Feedback received in our survey indicated that this part of the §404 process was probably the most tenuous and the timely communication between management and the external auditors the most strained.

C. There is a tendency with Information Technology General Controls (ITGC), due to the incorrect and overuse of the term "pervasive," to ascribe too much significance to ITGC risks. While ITGC as a whole may affect multiple applications and multiple key automated controls, in practice, individual key controls within ITGC do not always have a "pervasive" affect but may only impact a limited number of applications or locations. Further clarification would be valuable on the use and meaning of pervasive, as well as on the related topic of aggregation. Also, by their nature, ITGC are somewhat removed from direct linkage to financial statement assertions. ITGC are critical to support computerized applications that are generally an integral part of a company's system of internal control of financial reporting (ICFR). We have observed that this linkage provides difficulties to external auditors when they are trying to define a scope for ITGC that focuses on risks that are at least reasonably likely to be the root cause of an undetected material error in the financial statements.

   This appears to be caused by a sizeable amount of bottoms-up risk identification, especially when determining what ITGC issues should be in scope. The IIA, in association with a number of audit firms and companies of all sizes (including 13 of the Fortune 100) is developing a scoping methodology for ITGC that is based on risk. We anticipate this product will be available in the second half of 2006.

II. Need for Increased Reliance on Work of Others

D. The IIA promotes increased reliance on the use of the work of a competent and independent internal audit function as survey results have shown that this is an

effective way to reduce external audit costs and increase efficiencies. We believe an internal audit function operating in accordance with The IIA's *International Standards for the Professional Practice of Internal Auditing* is well equipped to meet the challenges of good governance. While the PCAOB standard appears to allow the external auditor to rely on the work of internal auditors, year-two implementation (as reflected in the survey) has not shown this to be as extensive as it could be. Where internal auditing has independently done testing or performed walkthroughs that fall within the scope of the financial reporting controls, external auditors should rely on that work.

E. It should be stressed that planning by the external auditor should not only be done early, but should be shared with management to enable more effective use of and reliance on management testing. As noted by many organizations and again reflected in our survey, significant opportunities remain for improved reliance by the external auditors on management testing, including and especially testing performed by the internal auditing function.

III. Continued Improvement in the Effectiveness and Efficiency of the §404 Process

F. The importance of a top-down, risk-based approach cannot be over-emphasized. The SEC and PCAOB were correct when they indicated in May 2005 that this approach is critical to an efficient process that focuses appropriately on risks to the financial statements. However, as shown by the results of our survey, implementation of this approach has been disappointingly slow (only 46% of respondents believed external auditors used a risk-based approach).

G. The IIA encourages increased consideration of company-level controls. Guidance issued by the PCAOB subsequent to AS 2 has addressed the importance of company-level controls in executing a risk-based audit. However, the supplemental guidance has addressed this topic at a very conceptual level, while the detailed guidance of AS 2 provides numerous detailed examples of designing audit testing without reference to company-level controls.

The supplemental guidance issued after publication of AS 2 gives a strong endorsement to the need for external auditors to give early and complete consideration of company-level controls as a method to fully implement a risk-based testing approach. While this supplemental guidance has made these statements, AS 2 continues to have a number of elements that appear inconsistent with this guidance. More specifically in AS 2:

1. Paragraph 40 discusses what an external auditor should do to obtain an understanding of management's process for assessing the effectiveness of internal controls. The first element listed for the external auditor's consideration is a discussion of which controls management has decided should be tested. Company-level controls are the last item listed, transaction level controls are listed first.

2. Paragraph 52 discusses identifying company-level controls. This paragraph states: "Controls that exist at the company-level often have a pervasive impact on controls at the process, transaction, or application level. For that reason, as a practical consideration, it may be appropriate for the auditor to test and evaluate the design effectiveness of company-level controls first…" The only discussion is regarding how company-level controls impact detailed transaction level testing, and then only as a practical matter. Missing is a clear discussion of considering company-level controls as part of a risk-based audit.

3. AS 2 has numerous examples of how to determine which detailed transaction-level controls should be tested. There are no examples of how the external auditor should consider testing company-level controls as a partial substitute for detailed transaction control testing in lower risk areas. For example, none of the examples in Appendix B to AS 2 starting after paragraph B31 have any discussion or consideration of company-level controls.

4. Paragraph B1 directs the auditor to move from identifying business units that are individually important to evaluating documentation and testing controls over significant accounts. There is no discussion of company-level controls other than for individually unimportant business units.

In conclusion, The Institute believes that much has been achieved and that more can be done to enhance sound corporate governance. We think that effective and efficient corporate governance emanates from the synergy and balanced relationships between those in charge of governance -- the board and management -- and their two primary support partners, external and internal audit.

Essential to any corporate governance structure is the need to establish clear roles for all involved. Management's control responsibility covers all operations and risks and they should be provided with further guidance that help them meet the expectations of §302 and rebalance their overall control and monitoring efforts. Internal auditors should support management in carrying out its responsibilities but not take on management's responsibilities for documenting controls or implementing systems of internal controls. The investors and shareholders should be equally concerned with all risks and related controls that may impact the sustainable performance of the businesses in which they invest, and not just those risks and controls that relates to financial reporting. The SEC and PCAOB should support this approach.

Professional internal auditors, performing their duties in compliance with the *International Standards for the Professional Practice of Internal Auditing,* are traditionally the ones who provide an objective assessment of internal control over core risk areas of the organization on an on-going basis. It is essential to recognize that internal auditing has been diverted (to varying degrees) to support management's §404 effort instead of being complemented (i.e., additional resources provided) to continue its essential tasks

as well as support management in the implementation and on-going monitoring of the SOX §404 effort. It would be appropriate for both the SEC and PCAOB to reinforce this key message.

Representatives from The IIA will be attending the SEC and PCAOB roundtable meeting in Washington on May 10 and we welcome the opportunity to discuss any and all of these issues with you.

Best regards,

David A. Richards, CIA

Attachments

A – Year 2 Sox Implementation Survey Results

B – *Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners*

C – Additional Issues of Interest to be Considered

About The Institute of Internal Auditors

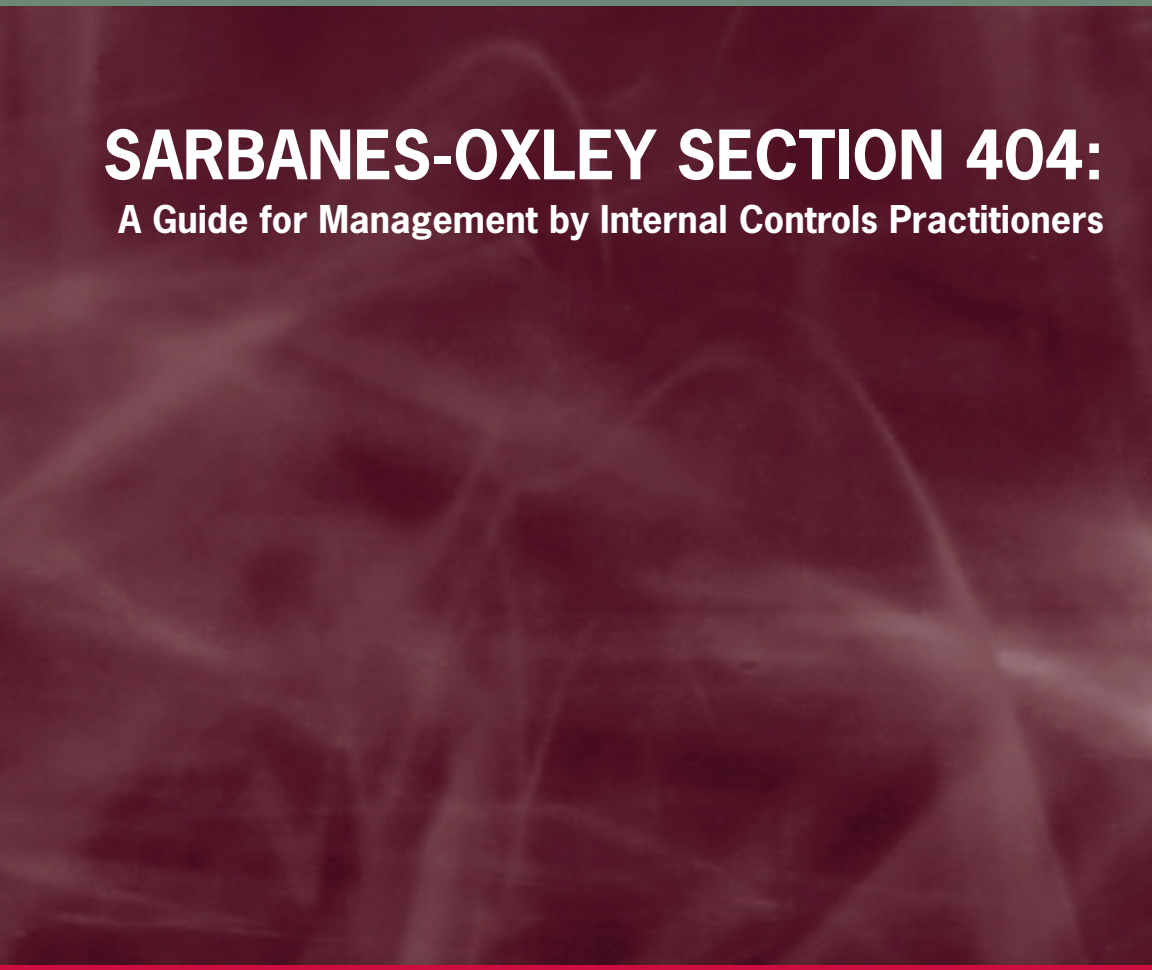
The IIA is the global voice, acknowledged leader, principal educator and recognized authority of the internal audit profession and maintains the *International Standards for the Professional Practice of Internal Auditing (Standards)*. These principles-based standards are recognized throughout the world and are available in 25 languages. The IIA represents more than 120,000 members across the globe, and has 247 affiliates in 92 countries that serve members at the local level.

The IIA also administers the Certified Internal Auditor (CIA) examination, given in 16 languages. The four-part test assesses the knowledge, skills, and abilities needed to be an effective internal auditor. Worldwide there are more than 57,000 CIAs.

The Standards and Code of Ethics are part of The IIA's Professional Practices Framework (PPF) that also includes Practice Advisories (help interpret the *Standards*), and other guidance (e.g., position papers, research studies, books, seminars, conferences, and services related to the practice of internal auditing). The PPF provides practitioners throughout the world with a full range of guidance, products and services for high-quality internal auditing services.

SARBANES-OXLEY SECTION 404:

A Guide for Management by Internal Controls Practitioners



The Institute of Internal Auditors

PROFESSIONAL GUIDANCE

Setting the Standard

PREFACE

This is the first publication in the Professional Guidance series of the Professional Practices Framework.

The series sets out to tackle subjects of global importance to a wide constituency of IIA members and others. The material includes matters of internal audit principle or practice, and issues of a broader social importance on where The Institute should be able to make a valuable contribution.

Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners is the product of The Institute of Internal Auditors (the recognized authority and standard-maker in internal auditing in the United States and around the world) and is written for management by those who have worked on internal controls hand-in-hand with board and management — experienced internal auditors.

This ***Guide*** incorporates and reflects up-to-date guidance from the U.S. Securities and Exchange Commission (SEC), the Public Company Accounting Oversight Board (PCAOB), The Institute of Internal Auditors (IIA), and the real-world experience and insight of practicing internal auditors. As management, regulators, and internal and external auditors increase their understanding of the practical aspects of Section 404, and as related rules, regulations, and guidance change, this guide will be updated electronically to reflect new guidance and best practices. To keep updated, please visit ***www.theiia.org***.

Cost is an issue for all management teams. This guide focuses on how total costs can be minimized without impairing the effectiveness of the program.

The guide also discusses the interplay between the requirements of Section 404 and those of Section 302. The latter requires annual and quarterly certifications by the chief executive officer (CEO) and chief financial officer (CFO)[ii] that include assessments of internal controls.

We encourage you to review your plans for Section 404 with the head of your internal audit function, especially how you will ensure that your ongoing program for the years to come is efficient and minimizes disruption to the business. The internal auditor is uniquely positioned not only to review and test your controls, but also to provide internal consulting on the adequacy of their design and on the whole management assessment and testing process. This guide contains a checklist that will be of value in assessing the efficiency of your program.

About The IIA *- Established in 1941, The IIA has more than 115,000 members worldwide. It serves as the internal audit profession's global voice, recognized authority, acknowledged leader, principal educator, and chief advocate. The Institute monitors legislation, regulations and pronouncements of other professional organizations throughout the world on matters that directly impact the practice of internal auditing. It promulgates the* International Standards for the Professional Practice of Internal Auditing *and offers a variety of leading-edge professional development opportunities, a comprehensive certification program, thorough quality assessment services, benchmarking surveys, and valuable research reports and educational products through The IIA Research Foundation. For more information, please visit www.theiia.org.*

TABLE OF CONTENTS

Organizations that have not completed their first year's Section 404 program (non accelerated filers and foreign registrants) can use this guide to ensure their program is not only effective but cost-effective.

On the other hand, organizations that have completed an assessment can use this guide to:

- Assess the efficiency of their Section 404 program, including how to minimize total cost (including external auditor fees).
- Revisit their assessment process and compare it to best practices identified by experienced internal control practitioners.
- Reconsider their processes for assessing deficiencies and providing an overall opinion. Management should provide an opinion that is based on principles instead of rules — in other words, an opinion that provides the investor with a fair assessment of the system of internal control. It should reflect the true condition of the internal control system, not one that is based on technicalities and could mislead the investor, who needs to have confidence in the financial reports.

Based on their role within the organization and their responsibilities for Section 404, readers may use the guide in its entirety or read selectively based on interest.

The first and last sections — "Summary for the CEO and CFO" and "Closing Thoughts on Efficiency" — merit all readers' review.

INTRODUCTION

Much has been written on the subject of Section 404 of the U.S. Sarbanes-Oxley Act of 2002 and management's annual assessment of its system of internal control over financial reporting. Each of the major accounting firms (as well as other providers of audit services) has given us extensive and valuable guidance,[i] generally consistent with the PCAOB's Auditing Standard No. 2 (AS 2), "An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements" and related Frequently Asked Questions (FAQ).

Management actions are governed by the SEC and not the PCAOB. In practice, the SEC has endorsed the principles in AS 2, which it formally approved for publication in June 2004. However, it is not written as a guide for management, but rather as a standard for the external auditor. The various publications of the accounting firms, while valuable and necessary reading, are influenced by their perspectives.

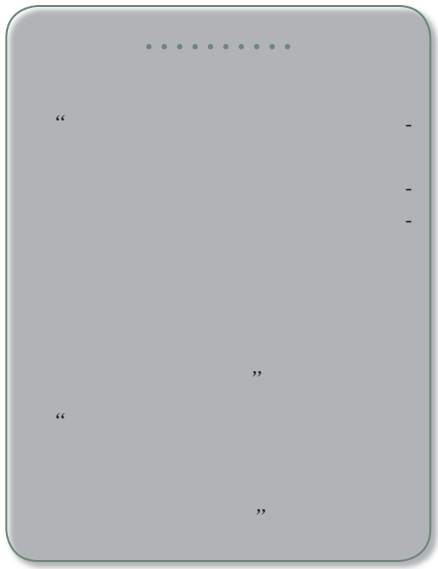
Internal auditors specialize in the assessment of internal controls and have for decades. They do so as a service to the audit committee and management of their organizations and, therefore, have extensive insight into the operation of those controls and the constraints on management in providing those controls. They are experts in the theory and practice of internal controls and related auditing.

SUMMARY FOR THE CEO AND CFO

The costs and benefits of the U.S. Sarbanes-Oxley Act of 2002 have both received a lot of ink as organizations prepared for and issued their first assessments of internal control over financial reporting as required by Section 404. In truth, there have been a lot of complaints by executives over the tremendous additional costs and the discussion of benefits has been muted in comparison.

When U.S. Congress passed the Act, the intent was to drive improvements in companies' internal controls. The benefits were seen as greater assurance to shareholders and other stakeholders in published financial reports; costs were of lesser significance. However, cost is of tremendous importance to corporate executives.

In November 2005, the PCAOB issued a report[iii] that commented on efficiencies, both in management's and the external auditors' work:



> "The Board's monitoring has focused on whether firms' audit methodologies, as well as firms' execution of those methodologies, have resulted in audits of internal control that are effective and efficient. The Board found that both firms and issuers faced enormous challenges in the first year of implementation, arising from the limited time frame that issuers and auditors had to implement Section 404; a shortage of staff with prior training and experience in designing, evaluating, and testing controls; and related strains on available resources. These challenges were compounded in those companies that needed to make significant improvements in their internal control systems to make up for deferred maintenance of those systems.
>
> "The Board's monitoring revealed that audits performed under these difficult circumstances were often not as effective or efficient as Auditing Standard No. 2 intends (and as the Board expects they can be in the future, given the benefits of experience, adequate time, and resources)."

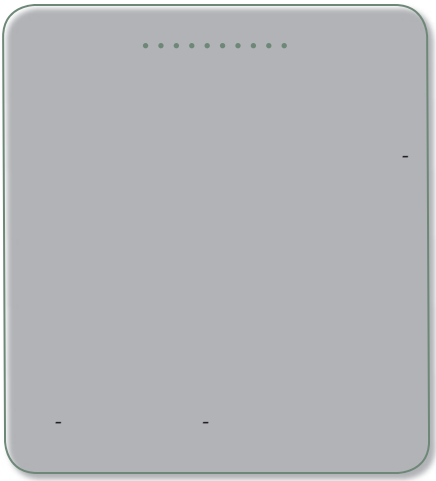
This guide, which is focused on achieving success at the lowest possible total cost, including external auditor fees, can help management tasked with responsibility for the Section 404 program by providing:

- Information on the requirements of Sarbanes-Oxley and the fundamentals of internal controls.
- A discussion of how the annual requirements of Section 404 relate to the quarterly requirements of Section 302 (the quarterly certification by the CEO and CFO).
- An explanation and practical suggestions for each phase of the program, including areas of difficulty: identification of key controls, assessing deficiencies, and the final assessment.

SUMMARY FOR THE CEO AND CFO

- Advice on how to reach a fair assessment that does not mislead investors as to the condition of internal controls and the reliability of financial statements. Even though many companies (and their external auditors) have taken a rules-based approach, management needs to ensure their assessment is principles-based. Management's formal assessment has to reflect their belief as to whether the controls provide reasonable assurance of the reliability of *future*[I] financial statements.[iv] That reliability is based on the likelihood of an error that would be material to a reasonable investor. An assessment that the controls are not effective simply because there has been a restatement may mislead the investor as to the *current* state of internal controls and the reliability of future financial statements.
- A checklist to help management assess the efficiency of their program.

Some companies have adopted a methodology for Section 404 that is rules-based.[v] This can lead to an assessment that is neither effective nor efficient. Instead, management should use judgment to develop and operate a continuing Section 404 program that is principles-based. Executives should understand that:

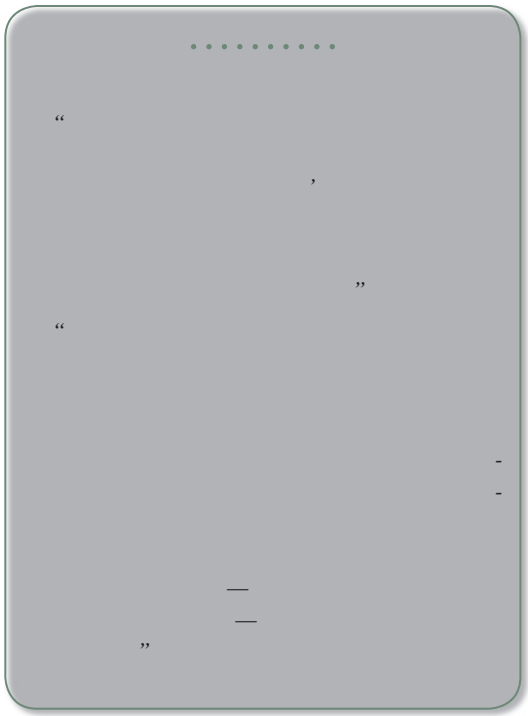


- The SEC, which is the governing authority for corporations, has only provided general guidance and very few specific rules. However, it has approved the standards developed by the PCAOB — the rule-maker for the external audit firms.
- Management has a great deal of flexibility in designing and implementing their Section 404 program, much more than is available to the external auditor.
- Both management and the external auditor have been encouraged by the SEC and the PCAOB to use their judgment and develop an approach that is top-down and risk-based.The Section 404 program should include coverage of all areas where the inherent risk (i.e., the risk before the quality of internal controls is considered) of an error that could lead to a material misstatement[vi] is at least reasonably possible[vii]. There is no need for the program to assess and test every control related to financial reporting, even those that might be considered significant deficiencies if they failed (see the definition of significant deficiency provided later in this guide).

[I]The guidance published by the SEC and PCAOB does not address this issue directly. However, there are indications in comments by officials with these organizations that the value of the Section 404 assessment is that it provides a level of comfort with respect to the reliability of future financial statements (on the assumption that there is no significant change in the quality of the system of internal control). The quality of the system of internal control at the end of the reporting year is an indication of whether it is sufficiently robust to either prevent or detect material misstatements in financial statements that will be prepared under the processes and related controls that management has assessed. In addition, an assessment of the likelihood of any event is difficult, if not impossible, without defining the period during which the event may occur. In this guide, the authors have taken the reasonable position that management's assessment should reflect the likelihood of a material misstatement in one or more of the next 12 months' financial statement filings. Neither the SEC nor the PCAOB have publicly commented on this matter, and our position relative to 12 months (which would include the next annual financials on Form 10-K as well as interim reports on Form 10-Q) is a suggestion based on what we believe is reasonable.

On May 16, 2005, the SEC staff issued a "Statement on Management's Report on Internal Control over Financial Reporting" that said (emphasis added):

> "An overall purpose of internal control over financial reporting is to foster the preparation of reliable financial statements. Reliable financial statements must be materially accurate. Therefore, a central purpose of the assessment of internal control over financial reporting is to identify material weaknesses that have, as indicated by their very definition, more than a remote likelihood of leading to a material misstatement in the financial statements. While identifying control deficiencies and significant deficiencies represents an important component of management's assessment, *the overall focus of internal control reporting should be on those items that could result in material errors in the financial statements.*
>
> "In adopting its rules implementing Section 404, the Commission expressly declined to prescribe the scope of assessment or the amount of testing and documentation required by management. *The scope and process of the assessment should be reasonable, and the assessment (including testing) should be supported by a reasonable level of evidential matter. Each company should also use informed judgment in documenting and testing its controls to fit its own operations, risks and procedures. Management should use its own experience and informed judgment in designing an assessment process that fits the needs of that company. Management should not allow the goal and purpose of the internal control over financial reporting provisions — the production of reliable financial statements — to be overshadowed by the process."*



Similarly, the PCAOB's May 16, 2005, Policy Statement noted (the emphasis is from the Policy Statement):

> "… to properly plan and perform an effective audit under Auditing Standard No. 2, auditors should:

- ***exercise judgment to tailor their audit plans to the risks facing individual audit clients,*** instead of using standardized "checklists" that may not reflect an allocation of audit work weighted toward high-risk areas (and weighted against unnecessary audit focus in low-risk areas);
- ***use a top-down approach*** that begins with company-level controls, to identify for further testing only those accounts and processes that are, in fact, relevant to internal control over financial reporting; and

- ***use the risk assessment required by the standard*** to eliminate from further consideration those accounts that have only a remote likelihood of containing a material misstatement."

Executives should also understand that:

- Management is *not* required to adopt the same methodology as the external auditor, although there may be advantages in using a similar approach. The PCAOB's AS 2 is mandatory for external auditors, not for management.
- The rules-based approach favored by some external auditors may tend toward an assessment of the overall system of controls that is not a fair representation, in the judgment of management, of their condition.
- The regulators believed the greatest benefit from Section 404 was that it would provide greater assurance to investors and others that they could rely on management's published financials. The value of that assurance is not as it relates to the current set of financial statements (to which the Section 404 assessment is attached), as they are subject to a separate assertion by management and opinion by the external auditor on their adequacy. Neither is the value in assessing controls over prior period financials. The value is in providing comfort with respect to the reliability of financial statements that will be published in the *future*. The Section 404 assessment indicates to the investor whether the system of internal control is sufficiently robust such that the risk of material error in *future* financial statements is remote or less[viii].

In practical terms, management's assessment of the system of internal control over financial reporting should reflect whether they believe the risk of material misstatements in financial statements filed with the SEC during the next 12 months[2] is less than reasonably likely. An alternative view is whether management believes its system of internal control over financial reporting contains any material weaknesses, representing a more than remote risk that financial statements filed with the SEC during the next 12 months will contain material errors.

The greatest area of potential cost-savings is through reduction of external costs (i.e., costs other than internal employees' time).[ix] Many companies continue to make significant use of third-party providers of consulting and audit services to perform testing and sometimes manage their Section 404 program. They are working to reduce these costs by hiring project management and testing personnel.

External auditor fees related to their Section 404 work make up a large part of total costs.[x] In addition to the efficiencies they are making from experience and in response to PCAOB guidelines and recommendations, management can effect fee reductions by:

- Limiting the number of key controls — the controls that have to be tested — by adopting a top-down, risk-based approach that focuses on controls that will prevent or detect material errors. Companies and external auditors have, as confirmed in the PCAOB November

[2] *See the earlier footnote(1). The authors recommend using a period of 12 months; however, the SEC and PCAOB have not publicly commented on whether this is an appropriate method.*

2005 report, tested controls that are not key (i.e. - not required to prevent or detect material errors). Controls that are not likely to result in material error should they fail should not be considered "key" and do not need to be within management's scope for Section 404.

- Maximizing reliance by the external auditor on management testing. This requires ensuring management testing is performed by skilled, experienced individuals who are independent of the activity being tested. The latter usually have several years' experience in a combination of external audit firms and internal audit functions. Most companies use their internal audit function to perform the testing; this is the most likely approach to maximize external auditor reliance. Some use other internal staff to perform management testing and rely on internal auditing to review and test their work to ensure it is to appropriate standards.[xi]

- Executing controls flawlessly. The tolerance level for defects in testing is very low. If the external auditors find even one error in their testing of a control, they may assess the control as not operating effectively. This will require remediation and retesting, potentially doubling the work.
- Documenting the processes and controls clearly and in good detail, and then ensuring the documentation is updated promptly as processes change.
- Completing a substantial portion of management's work, including testing (even if only limited in sample size) of all key controls, by mid-year. This enables the external auditors to start their work early, which helps with resource scheduling and reduces the risk of finding deficiencies late.

The above actions will also reduce internal costs, including management and employees' time. The most significant factors are:

- Reduction in the number of key controls.[xii]
- Executing controls flawlessly.

In the past, most CEOs and CFOs have signed their annual and quarterly certifications — which are included in the financial statements filed with the SEC on Form 10-Q, and are required by Section 302 of Sarbanes-Oxley — without a rigorous examination of internal controls. Now that Section 404 is in force (at least for accelerated filers), management should be integrating its quarterly and annual assessment processes. Although management is not required to test all their key controls every quarter, they should perform some degree of testing each quarter to support the quarterly Section 302 certification.[xiii] At minimum, the Section 302 certification process should include a consideration of the status of the Section 404 project, the results of testing, and the severity of any identified control deficiencies.

Companies, external audit firms, and the regulators are all learning how Section 404 should be applied and how both management and the external auditors can be both effective and efficient. The last section of this guide includes a number of questions management may use to assess their programs.

SUMMARY FOR THE CEO AND CFO

The SEC and PCAOB are likely to provide additional guidance. The authors plan to update this guide and provide additional information through other publications to reflect changes in regulations as well as in best practice.

A. SECTION 404: RULES OR PRINCIPLES

Section 404 of Sarbanes-Oxley required the SEC to develop and publish rules for a management assessment of internal control over financial reporting (ICFR). Those rules were completed in June 2003, and the PCAOB followed with its AS 2, which was approved by the SEC in June 2004. Together, they require that:

- Management perform a formal assessment of its controls over financial reporting (see definition below), including testing to confirm both the design and operating effectiveness of the controls.
- Management include in its annual report on Form 10-K[xiv] an assessment of internal control over financial reporting.
- The external auditors provide three opinions as part of a single integrated audit of the company, instead of the one previously provided. This includes:
  - An opinion on management's assessment.
  - An independent opinion on the effectiveness of the system of internal control over financial reporting.
  - The traditional opinion on the financial statements.

The SEC rules are worth reviewing carefully. They "require a company's annual report to include an internal control report of management that contains:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company.
- A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting.
- Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including a statement as to whether or not the company's internal control over financial reporting is effective. The assessment must include disclosure of any "material weaknesses" in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting.
- A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the registrant's internal control over financial reporting."

The "final rules also require a company to file, as part of the company's annual report, the attestation report of the registered public accounting firm that audited the company's financial statements."

Taking each point in turn:

1. Management is responsible for the system of internal control. This is an important clarification, as previously some management teams believed[xv] the system of internal control was the responsibility of internal audit, external audit, or the CFO. By contrast, an effective system of internal control is the responsibility not just of the CFO, but the CEO and the senior executive team as a whole.

2. The assessment has to be made using a recognized internal control framework. Most U.S. companies have used The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, although some have used the Control Objectives for Information and related Technology (CobiT) framework as a supplement to COSO for IT controls. Both COSO and CobiT are discussed in Section B of this guide.

3. The assessment is annual and "as of" year-end. There are restrictions on how management can make its assessment, depending on whether a "material" weakness is identified.

4. The external auditor must perform specified work in relation to management's assessment. The SEC mandated "an attestation report." The PCAOB has interpreted that in AS 2, with SEC consent, to include not only an assessment and related formal opinion on management's assessment, but also an independent assessment and formal opinion on the adequacy of the system of internal control over financial reporting.

Although the PCAOB has provided quite detailed (and generally principles-based) guidance for external auditors in AS 2, AS 2 is not binding on management. In fact, management has a great deal of flexibility in implementing its Section 404 program. The guidance from the SEC is principles-based, only requiring an assessment that is based on one of the recognized internal control frameworks.

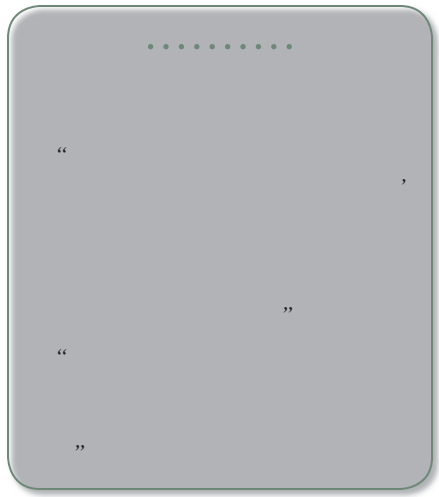
Management needs to understand AS 2, because it explains how the external auditor will review and assess management's assessment process. It is also important if, to contain cost, management is planning to minimize audit fees by maximizing reliance on management testing.

However, management also needs to ensure its process is faithful to the principles behind Section 404: that it provides a fair assessment of the organization's internal controls as of year-end, reflecting whether the system provides reasonable assurance that material misstatements will be prevented or detected.

The following sections provide a road map for understanding the principles and requirements for Section 404 and implementing an efficient and effective Section 404 program. Section D (page 20) explains the requirements of Section 302 (the quarterly certification by the CEO and CFO of the interim financials) and its relationship with Section 404.

B. REVISITING THE PRINCIPLES OF INTERNAL CONTROL

There are a variety of definitions of *internal control*. For the purposes of Section 404, the great majority of companies and all the Certified Public Accounting (CPA) firms[xvi] use the definition in COSO's *Internal Control – Integrated Framework*. COSO's definition relates to all aspects of internal control, not just that over financial reporting. The following is from the Executive Summary of the COSO report.



"Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

"The first category addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources. The second relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. The third deals with complying with those laws and regulations to which the entity is subject. These distinct but overlapping categories address different needs and allow a directed focus to meet the separate needs."

COSO goes on to say:

"Internal control systems operate at different levels of effectiveness. Internal control can be judged effective in each of the three categories, respectively, if the board of directors and management have reasonable assurance that:

- They understand the extent to which the entity's operations objectives are being achieved.
- Published financial statements are being prepared reliably.
- Applicable laws and regulations are being complied with.

"While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time."

The PCAOB, together with the SEC, is responsible for the rules governing the roles and actions of the CPA firms. In AS 2, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements," the PCAOB has a definition that is consistent with that of COSO, although limited to financial reporting. It is also consistent in all material respects with the definition used by the SEC.[xvii] They define ICFR as:

"A process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial

statements for external purposes in accordance with generally accepted accounting principles (GAAP) and includes those policies and procedures that:

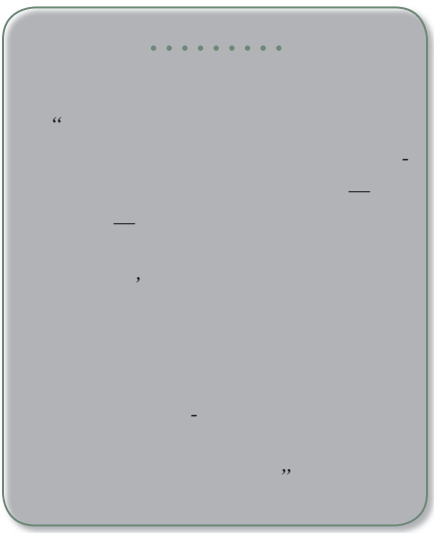
- Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements."

There are a number of key points in these definitions:

1. Internal control is a *process*. It is a continuing process rather than a point-in-time situation. However, any assessment of its effectiveness is made at a point in time. Management must assess the adequacy of its ICFR as of year-end, even though the system operates continuously - not only all year but for multiple years. Management needs to be aware, though, that an assessment as of a point in time is likely to be interpreted by investors and others as indicative of its continuing effectiveness. Stakeholders are concerned with whether or not the internal controls are sufficient to provide comfort, not only with respect to the reliability of the current set of financial statements, but also of future financial statements.

2. Internal control only provides *reasonable assurance*. The COSO Executive Summary expands on this point:

   "An internal control system, no matter how well conceived and operated, can provide only reasonable — not absolute — assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake.



   Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs."

The PCAOB's AS 2 also discusses reasonable assurance, taking it further to establish that *reasonable* is a "high level of assurance":

> "Management's assessment of the effectiveness of internal control over financial reporting is expressed at the level of reasonable assurance. The concept of reasonable assurance is built into the definition of internal control over financial reporting and also is integral to the auditor's opinion. Reasonable assurance includes the understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance."

An effective system of internal control can only provide this reasonable assurance. When assessing its adequacy, management needs to determine whether errors — even if they resulted in a material error in the financial statements — are the result of a "simple error or mistake" that is a momentary or one-time failure, rather than an indication that the system no longer provides reasonable assurance that a material error in the financials will not be prevented or detected. COSO, PCAOB, and the SEC refer to the concept of a reasonable person's view, which should be considered when assessing whether the system of internal control provides reasonable assurance.

The PCAOB states that *reasonable* is a "high level of assurance." They refer to the "understanding that there is a *remote likelihood* that material misstatements will not be prevented or detected on a timely basis." This is fully consistent with the way in which management and the external auditor should assess the overall system of internal control. As noted later, the external auditors typically use a range of 5 percent to 10 percent for remote likelihood.

The SEC has not provided a specific standard with which the effectiveness of internal control should be measured. Instead, in the words of their commentary on the final rules, they have set a "threshold for concluding that a company's internal control over financial reporting is effective." That threshold is the presence of one or more material weaknesses. Therefore, management can assess ICFR as effective if there are no control deficiencies such that a material error is reasonably possible.

Stating the issue perhaps more simply, a system of internal control provides a reasonable level of assurance with respect to filed financial statements (i.e., for Section 404) when:

- The cumulative risk of a material misstatement due to known control weakness is not reasonably possible, i.e. 10 percent or less.[3]
- Any control weaknesses identified by management and external or internal auditors are corrected promptly.
- The management team believes the level of controls is appropriate to the business, enabling reliable financial reporting for external use (i.e., SEC filings).

---

[3] The 10 percent reference is based on the external auditors' general use of a range of 5 percent to 10 percent when determining whether the likelihood of a material error is 'more than remote.' Although it is not generally possible to calculate the probability of an error with any degree of precision, and there is no authoritative guidance in this area, this range is helpful in providing management with a feel for the level of probability being discussed.

B. REVISITING THE PRINCIPLES OF INTERNAL CONTROL

3. Internal control over the integrity of a company's financial statements is part of the overall system of internal control. In practice, there can be significant overlap between controls designed to provide assurance over the financials and those that provide assurance relative to operational effectiveness or compliance. For example, monitoring the cost of units sold is an important control for both financial reporting and for ensuring the efficiency and effectiveness of operations. When assessing control deficiencies to determine the need and value of enhancing controls, management should consider the risk not only to the financial statements, but also to the efficiency of operations or compliance with applicable rules and regulations.

4. Another point of significance is that for Section 404 purposes, ICFR only addresses the controls providing assurance over financial statements filed with the SEC. It does not necessarily address controls over:
   - Other financial statements, including those provided as part of statutory reporting to foreign governments or to financial institutions, as may be required by debt instruments.
   - Financial reporting used in internal management decision-making; for example, monthly management metrics.
   - Other sections of the 10-K such as Management's Discussion and Analysis (MD&A).
   - Earnings releases and proxy statements.

Clearly, management needs to have effective controls over all forms of financial reporting and may consider either extending its own assessment to cover these areas, or asking its internal audit function to perform procedures relative to these areas.

THE COSO FRAMEWORK

Management is required to assess its system of ICFR using a recognized framework. Most have selected the COSO framework, which is recognized as appropriate by both the SEC and the PCAOB.

COSO's internal control framework describes internal controls as consisting of five inter-related components. These are generally called "layers," and the controls within each must be included in management's assessment. The five layers are described by COSO as:

1. **Control Environment**
   "The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors."

2. **Risk Assessment**
   "Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for

determining how the risks should be managed. Because economic, industry, regulatory, and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change."

3. **Control Activities**

"Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties."

4. **Information and Communication**

"Pertinent information must be identified, captured, and communicated in a form and time frame that enable people to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across, and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders."

5. **Monitoring**

"Internal control systems need to be monitored — a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board."

In practice, the assessment of ICFR is conducted at only two levels instead of five. Most of the controls that are assessed are those found in the Control Activities layer. Controls within the other four are typically grouped together; a common term for this group is *entity-level controls*. While the majority of controls are in Control Activities, particular attention to entity-level controls is required because:

- These controls are presumed to have a pervasive effect on the activities of the entire company.

B. REVISITING THE PRINCIPLES OF INTERNAL CONTROL

- Many of the control deficiencies underlying the public accounting issues of the last several years — including Enron and WorldCom — were in these areas.

A number of companies use a separate framework to supplement COSO when assessing information technology (IT) controls. COBIT[xviii] was developed by the Information Systems Audit and Control Association's IT Governance Institute in 1994 and Edition 4.0, released in December 2005, includes important updates for Section 404 and strengthens links to frameworks such as COSO. COBIT is widely used by IT audit professionals in the United States and overseas.

Additional information on internal controls may be obtained from the head of the internal audit function, The IIA, or the external auditor.

C. WHAT CONSTITUTES AN EFFECTIVE SYSTEM OF INTERNAL CONTROL AS IT RELATES TO THE REQUIREMENTS OF SECTION 404?

Management needs to determine whether the system of internal control in effect as of the date of assessment provides reasonable assurance that material errors, in either interim or annual financial statements, will be prevented or detected.

Management is able to make this assessment by:

- Identifying, assessing, and testing the design and operating effectiveness of the key controls over transactions that constitute the balances in significant accounts in the financial statements.
- Assessing whether any control deficiencies identified in the above process represent, either individually or in aggregate, a more than remote likelihood of a material error (a "material weakness").

If the scope and quality of management's identification, assessment, and testing of key controls is sufficient to address all major risks to the integrity of the financial statements and no material weaknesses are identified, then management usually will be able to assess the system of ICFR as effective. However, the presence of a single material weakness precludes management from making such an assessment. This is appropriate, as a material weakness, by definition, indicates that the system of internal control does not provide reasonable assurance regarding the reliability of the financial statements.

Each of the above is discussed in more detail in the following sections.

D. WHO IS RESPONSIBLE FOR INTERNAL CONTROLS?

Sarbanes-Oxley, both Section 302 and Section 404, makes it very clear that management — specifically the CEO and CFO — is responsible for the adequacy of internal controls. The certification by these officers required by Section 302 states:

"(4) The signing officers —
(B) Are responsible for establishing and maintaining internal controls.
(C) Have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared.
(D) Have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report.
(E) Have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date."

Although the CEO and the executive team as a whole may look to the CFO for overall leadership and accountability for financial reporting, other parts of the organization have a significant part to play. For example, the system of ICFR typically includes processes in the procurement, inventory management, manufacturing, sales, and information technology functions, not all of which report to the CFO.

Responsibility for the system of internal control within a typical organization is a shared responsibility among all the executives, with leadership normally provided by the CFO.

The audit committee of the board of directors has a very significant role in a company's system of internal control, which it performs on behalf of the full board and ultimately the shareholders. Specifically, the members:

- Provide oversight of management. Both management and the external auditor are required to consider the effectiveness of the audit committee as part of their assessments of ICFR. COSO describes their role:
  "Management is accountable to the board of directors, which provides governance, guidance, and oversight. Effective board members are objective, capable, and inquisitive. They also have a knowledge of the entity's activities and environment, and commit the time necessary to fulfill their board responsibilities. Management may be in a position to override controls and ignore or stifle communications from subordinates, enabling a dishonest management which intentionally misrepresents results to cover its tracks. A strong, active board, particularly when coupled with effective upward communications channels and capable financial, legal, and internal audit functions, is often best able to identify and correct such a problem."
- Provide direction and oversight of the work of the external auditor, who is appointed by, and reports directly to, the audit committee.
- Direct and oversee the performance of the internal audit function, which typically reports to the audit committee.

D. WHO IS RESPONSIBLE FOR INTERNAL CONTROLS?

The external auditor is engaged by, and is directly accountable to, the audit committee, a requirement of Sarbanes-Oxley. Through their audit of the annual financial statements, review of the interim financial statements, and audit of the system of internal control over financial reporting, they provide the audit committee, board of directors, investors, and management with assurance of the reliability of the financial statements. Although the external auditor provides assurance to the audit committee relative to the financial statements filed with the SEC, management is not permitted to place reliance on their work for purposes of Section 404. Management, instead, must have a system of internal control that is sufficient without relying on the external auditor.

By contrast, the internal audit function is considered part of an entity's internal control system, even though it also is directly accountable to the audit committee in most public companies. Although the chief audit executive (CAE) may report to a senior executive for administrative matters, he/she should report functionally to the audit committee. The internal audit function provides assurance to both management and the audit committee regarding the effectiveness of all aspects (i.e., not only financial, but also operational effectiveness and compliance) of an organization's system of internal control, risk management, and governance practices.[xix] Its activities are considered part of the Monitoring layer of the system of internal control and therefore are included in both management's and the external auditor's assessment. COSO describes their work:

> "Internal auditors play an important role in evaluating the effectiveness of control systems, and contribute to ongoing effectiveness. Because of organizational position and authority in an entity, an internal audit function often plays a significant monitoring role."

The audit committee can and should rely on the assurances of management, internal auditors, and the external auditor in forming its own assessments and in approving financial statements for filing with the SEC.

Additional information on the roles and responsibilities of each participant can be obtained from the company's CAE or The IIA.

E. WHAT IS THE SCOPE OF MANAGEMENT'S ASSESSMENT OF THE SYSTEM OF INTERNAL CONTROL OVER FINANCIAL REPORTING?

Management is actually required to provide more than one assessment of internal controls in its filings with the SEC. One is required by Section 302 and is included in quarterly as well as annual financial reports. The other is required by Section 404 and is only included in annual reports.

When the SEC developed the detailed rules for implementing Section 302[xx], it required the CEO and CFO to make a number of statements relative to internal controls (the Section 302 certification) and the company to include in its annual and quarterly financial statements an assessment of its "disclosure controls" and procedures, a new term not actually mentioned in the Sarbanes-Oxley Act. The SEC defined *disclosure controls* as:

> "…controls and other procedures that are designed to ensure that information required to be disclosed by the company in its Exchange Act reports is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by the company in its Exchange Act reports is accumulated and communicated to the company's management (including its principal executive and financial officers) for timely assessment and disclosure pursuant to the SEC's rules and regulations."

A simple and practical definition of the scope of Section 404 is that it addresses everything in the GAAP-based interim and annual financial statements and related notes that are filed with the SEC.[xxi] Disclosure controls include this and more.

The scope of disclosure controls is broad, including all "information required to be disclosed by the company in its Exchange Act reports." These reports include not only the financial statements and related footnotes, but nonfinancial information as well. It is important to note that disclosure controls cover not just the quarterly and annual financial statements filed on Forms 10-Q and 10-K, but also notifications of material events filed on Form 8-K or other current reports.[xxii] By contrast, Section 404 only relates to the financial information required to be included in filings with the SEC.

Disclosure controls include, in their entirety, all the Section 404 internal controls over financial reporting. Although the SEC in its early publications indicated that there would be significant overlap, in practice there are no key internal controls over financial reporting for Section 404 that are not part of disclosure controls.[xxiii] On the other hand, there are significant areas covered under disclosure controls that are not part of ICFR. Examples of the latter include Management's Discussion and Analysis (MD&A) and the timely notification to investors using Form 8-K of material events.

Companies need not only (1) internal controls to ensure the completeness and accuracy of the financial information included in their filings with the SEC, but also (2) internal controls to ensure the completeness, accuracy, and timeliness of nonfinancial information filed with the SEC. The combination of the two represents disclosure controls.

As a result:

- The assessment of disclosure controls can be that they are not effective, even though internal controls are effective; for example, due to issues surrounding timely notification of material events to investors.
- If internal control over financial reporting is assessed as ineffective, disclosure controls cannot be considered effective[4]. This is because the financial information included in the filings with the SEC is the most critical part of those reports.

Section 302's requirements include, as mentioned above, a certification by the CEO and CFO and an assessment of its disclosure controls. The certification includes the following statements that relate to internal controls:

"4. The registrant's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and ICFR (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

(a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

(b) Designed such internal control over financial reporting, or caused such ICFR to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

(c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

(d) Disclosed in this report any change in the registrant's ICFR that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

"5. The registrant's other certifying officer and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

(a) All significant deficiencies and material weaknesses in the design or operation of ICFR which are reasonably likely to adversely affect the registrant's ability to record, process, summarize, and report financial information; and

---

[4] Management may want to consult with SEC counsel on this matter. As discussed in note xiii in the back of this guide, the SEC and certain SEC counsel believe (and the authors concur) there are aspects of ICFR that are not included in disclosure controls. However, we believe all key controls for Section 404 will be included. An analysis of filings with the SEC in year one of Section 404 identified that 94 percent of the companies that assessed their ICFR as ineffective also assessed their disclosure controls as ineffective.

(b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting."

Clearly, there is a need to assess the adequacy of ICFR at interim periods to support the Section 302 certification, as well as the annual assessment required by Section 404.

There are some major differences between the annual Section 404 assessment and that required for the interim Section 302 assessments:

- The interim assessment[xxiv] for Section 302 is not audited by the external auditor.
- There is no requirement (at present) that the rigor and formality required in practice for Section 404 is repeated each quarter for the Section 302 assessment. For example, there is no requirement that management test all, or even a significant portion of its key controls each quarter. In addition, management's Section 302 process is not required to follow a recognized internal controls framework.

However, prudence suggests that management:

- Has a reasonably formal, documented process for making the quarterly assessment that is included in the 10-Q and supports the Section 302 certifications.
  - The authors suggest that this can be included in the activities of the company's disclosure committee, which most of the larger companies have established.
  - The process should include the assessment of all internal control deficiencies known to management, including those identified not only during management's assessment process, but also any identified by either the external auditors in their Section 404 work or by internal auditing in its various audit activities.
  - As discussed below, the system of ICFR has to provide reasonable assurance with respect to the quarterly financial statements as well as the annual statements. The quarterly assessment is against a lower — typically one quarter the size — determination of what constitutes material.
  - The process and results should be reviewed and discussed with the CEO and CFO to support their Section 302 certifications.
- Confirms that the external auditor does not disagree with management's quarterly assessment.
  - Understands (which requires an appropriate process to gather the necessary information) whether there have been any major changes in the system of internal control during the quarter. A major change can include both improvements and degradations in the system of internal control. Although Section 302 only requires the disclosure in the 10-Q of a *material weakness* and the communication to the audit committee of a material or significant deficiency, the *correction* of a *significant* deficiency is likely to be considered a major change and, if so, should be disclosed.

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

Management's assessment for Section 404 is as of year-end, so there may be a temptation to wait until late in the year before starting the Section 404 program. However, there are important reasons for considering the program a continuing, year-round process and starting early each year:

- Significant resources are required for testing that may be in short supply later in the year. Testing can be performed throughout the year, spreading the resource burden. Note: if controls are tested early in the year, management needs to perform an update procedure to "roll forward" the results to year-end.
- If there are issues relative either to the design or the consistent operation of the controls (in other words, exceptions will be identified during the testing), management will have time to make changes and retest successfully before year-end.
- The external auditors often have a policy requiring they start their testing only *after* management has tested and assessed the individual controls as effective. The earlier the external auditors perform their testing, the more time there is for management to remediate any issues and retest.

As explained above, spreading the testing provides management with improved assurance supporting the quarterly Section 302 certification and assessment of disclosure controls.

1) RISK ASSESSMENT

As discussed above, Section 404 only relates to the GAAP-based, interim and annual financial statements and related notes included in filings with the SEC.

In defining the detailed scope for management's assessment, a risk-based and top-down approach is recommended. This involves identifying:

- The general ledger accounts that make up each line in the filed financial statements. For example, accounts payable is normally a single line in the financial statements, although it represents a group of related general ledger accounts.
- For each of the above, which accounts are considered significant.
- The financial statement assertions relevant to those accounts and material to the investor.
- Locations to include in scope.
- The business processes that process transactions into the significant accounts at in-scope locations.
- The key transactions representing balances in the above accounts.
- The key controls over those transactions that ensure the financial statement assertions are achieved.

Because so much will depend on whether the system of internal control provides reasonable assurance that a material error will be either prevented or detected, the place to start is a definition of *material error.*

There is guidance in the accounting and auditing literature on this topic that is lengthy (and not repeated here), but comes down to a fairly simple test: what would be material to the reasonable investor in making an investment decision in the company's securities. It is preferable if the external auditor agrees with management's determination of what constitutes a material error, so early

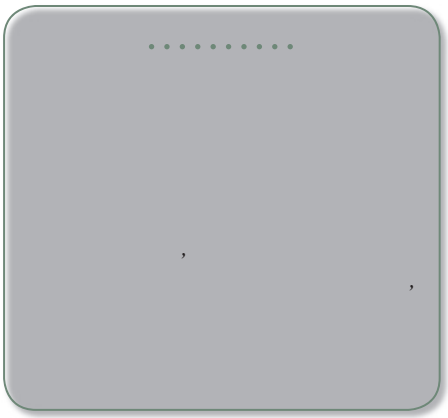
F. DEFINING THE DETAILED SCOPE FOR SECTION 404

discussions should be held. The external auditor may indicate that only a preliminary determination may be made, as facts may change before the end of the year.

The determination of a material a error for Section 404 should consider:

- The level of error that would be material to the full year's results if it affects the income statement.[xxv]
- Not all errors affect the profit and loss (P&L), only the balance sheet. In a few cases, the errors are in the disclosures (e.g., footnotes or earnings per share (EPS) calculations). The specific facts and circumstances of these errors will have to be assessed.
- In all cases, a bright-line definition must be tempered with an assessment of what a reasonable investor might conclude. It is easy to rush to judgment and label an error material that would have no effect on any investor's assessment of the company.

This determination of what would be material for the annual and also for the interim financials should be made by technical accounting personnel, after discussion with the external and internal auditors. The determination will consider not only quantitative but qualitative factors.



Having decided on a materiality level for the full year's P&L, management needs to determine how and where an error could occur. The financial statements are examined to determine in which accounts and disclosures there is the possibility of a material error. These are considered "significant accounts."

Accounts that are small and highly unlikely to contain an error of a material amount can be excluded from the scope for Section 404. Most companies set a threshold for identifying these "small" accounts, called *planning materiality*. This is a convenient, but not required, step in the process.

Management should work closely with the external auditor at every stage of the Section 404 process, and planning materiality is an important agreement to make. Although the external auditors may set a planning materiality for their own purposes that is higher than management's, they will consider management's level when they form their opinion on whether management's Section 404 process is adequate. In addition, management's level will influence the external auditors' own level, which can have implications on the extent of testing and related costs (both for management testing and external auditor fees).

Once planning materiality has been set and agreed upon, management should identify the general ledger accounts that they believe can be excluded, as they fall — or are expected by year-end to fall — below that level[xxvi]. The decision should be reviewed carefully to ensure there are no qualitative reasons (e.g., because of known risks) that indicate one of these smaller lines should be retained in Section 404 scope[5]. Care needs to be taken with accounts that can fluctuate significantly or are anticipated to change before year-end.

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

The scope of Section 404 extends to the footnotes that are part of the financial statements. Management needs to perform a risk assessment on all of the notes to determine which are significant and the nature and magnitude of an error that would be considered material to the investor. That determination may affect the selection of which accounts to include in scope, perhaps including some accounts that are below the agreed planning materiality.

Management can then review each remaining account to determine whether additional accounts can be excluded — because although they exceed planning materiality, by their nature it is unlikely that a material error will be made. An example could be an asset or liability whose value has not changed and is not expected to change, such as a long-term investment or loan.

Materiality, planning materiality, and the accounts in scope should be assessed at least quarterly, or when there are material changes in the business, to ensure there is no need to add or remove areas from scope.

The external audit profession has identified a number of financial statement assertions that may be applicable to the selected general ledger accounts. Management needs to define which assertions are applicable to which accounts, as later in the process, they will have to verify there are key controls to ensure these assertions are achieved. The assertions described in AS 2, which are recommended but not mandatory (if they are not used, management needs to document how they have ensured all potential risks of material error in each significant account are addressed by appropriate key controls) are as follows:

- **Existence or Occurrence** addresses whether assets or liabilities exist at a given date and whether recorded transactions have occurred during a given period.
- **Completeness** addresses whether all transactions and accounts that should be presented in the financial statements are so included.
- **Valuation or Allocation** addresses whether asset, liability, equity, revenue, and expense components are included in the financial statements at appropriate amounts.
- **Rights and Obligations** relates to whether the rights and liabilities are the obligations of the entity at a given date.
- **Presentation and Disclosure** addresses whether particular components of the financial statements are properly classified, described, and disclosed.

The majority of companies have operations in multiple locations, and it may be possible to exclude some of those locations from scope on the basis of materiality. Alternatively, some of the processes at those locations may be excluded. The PCAOB included in AS 2 (as Appendix B) a process for making that determination that has been widely accepted — although each company should

---

[5] *The SEC emphasized this in its May 2005 report: "When identifying significant accounts and related significant processes in order to determine the scope of its assessment, management generally will consider both qualitative and quantitative factors. Qualitative factors include the risk associated with the various accounts and their related processes …*
In addition to considering qualitative factors, the staff understands that management generally establishes quantitative thresholds to be used in identifying significant accounts subject to the scope of internal control testing. The use of a percentage as a minimum threshold may provide a reasonable starting point for evaluating the significance of an account or process; however, judgment, including a review of qualitative factors, must be exercised to determine if amounts above or below that threshold must be evaluated."

confirm that it is suitable for the company's own unique situation. The process is summarized below.

- Are there any locations that are individually significant because of their size, specific risks, or other reasons?
- Are there any locations that, when aggregated with similar locations, should be included because they share common processes or otherwise are similarly affected by a controls deficiency?
- Review the general ledger accounts determined to be in scope and identify from which locations the balances are derived.
- For all the in-scope general ledger accounts, select a combination of the locations that were identified under Steps 1 or 2 above such that the greater part of the balance in each account will be covered (a useful, but informal, rule of thumb is that management should cover sources representing at least 70 percent of balances of in-scope accounts) or at least provide sufficient coverage that the risk of a material misstatement is addressed.
- Review the selected general ledger/location combinations to ensure they are reasonable based on risk. They should represent the areas where a material error is at least reasonably possible, and exclude any areas where such an event is not likely.

The balances in the significant accounts are the result of transactions that flow through a number of business processes. For each account and location combination, the key business processes now need to be identified.

The authors recommend that a further level of detail be considered, identifying which transactions make up the preponderance of the account balances. That will enable a focus on those material transactions together with the related processes and controls, and the exclusion of immaterial transactions that flow into significant accounts. For example, the significant account for depreciation may include not only the depreciation of plant and equipment, but also the depreciation of company vehicles. For most companies, depreciation of the small number of company vehicles is not material either to the P&L or the balance sheet and should be excluded from scope for Section 404.

At this point, management has identified:

- The significant general ledger accounts and notes to be included in scope, and the related financial statement assertions.
- At which locations the controls and processes related to those accounts will be assessed and tested.
- The business processes and material transactions that make up the balances in those accounts.

2) PROCESS AND CONTROL DOCUMENTATION

The key business processes and, especially, the material transactions and related controls now need to be documented. There are various techniques and documentation styles for completing the documentation. However, management needs to complete documentation that:

- Enables a reasonably knowledgeable individual (this person does not have to be an expert with experience in the area but should have some knowledge of the company or its business) to understand the process.

- Provides context for the key controls such that a reasonable person would understand their function.
- Details the operation of key controls, such as identifying who is performing the control, when the control is operating and at what frequency, how the control is performed, what evidence exists that the control has been performed, and what reports are used in the operation of the control. It is important to agree with the external auditor on the quality standards to be established for control documentation.
- Overall, enables a reasonable person to have a basis upon which to assess the design of the controls: Are the controls identified and documented sufficiently to either prevent or detect a material misstatement? This is discussed further under "Key Controls."

Management should remember that the external auditor will be assessing whether management's process for making its assessment for Section 404 is adequate. A significant piece of that is whether there is adequate documentation of the processes and controls on which to base an assessment.

It is critical to establish a change management process to ensure that documentation is kept up-to-date as processes and controls change. The business does not stop just because of Section 404 requirements. A sound change management process for Section 404 will likely have the following attributes:

- The process is well known to all business process owners.
- Changes to business processes, including computer systems, are identified, and the documentation is updated promptly.
- Changes to key controls are identified and assessed promptly to ensure the potential impact on Section 404 assessment and testing is understood.
- Planned changes, especially those planned for late in the fiscal year, are discussed to ensure the impact on the Section 404 assessment is understood. Consideration is given to delaying the change until after year-end.

3) KEY CONTROLS

Although referenced in PCAOB documents (including the Nov. 30, 2005 report), there is no commonly accepted definition for a key control. The authors support the following, which we believe is consistent with PCAOB published guidance:

> *A key control is a control that, if it fails[6], means there is at least a reasonable likelihood that a material error in the financial statements would not be prevented or detected on a timely basis[xxvii]. In other words, a key control is one that provides reasonable assurance that material errors will be prevented or detected timely .*

[6] *The failure could be individual or combined with other controls that are likely to fail at the same time. Although the failure of one control may not be likely to result in a material misstatement, several may fail at the same time, increasing the risk of a material misstatement to more than remote. This scenario is called* aggregation *in the literature. The key is that the controls have to be* likely *to fail at the same time, for example, because they are performed at the same time, by the same people, or using the same computer system.*

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

Careful identification of key controls is important to an efficient and effective Section 404 program. An overly conservative approach, where too many controls are defined as "key," will result in excessive time and resources testing controls that are not critical to the assessment. On the other hand, if too few controls are identified, this may result in a significant problem when the external auditor identifies, and management then agrees with, the need for additional key controls.

Technically speaking, management may be considered not to have an adequate basis for its assessment unless adequate evidence is obtained that all key controls are operating effectively. These newly-identified key controls may not have been addressed. Management may be able to recover by documenting and testing the controls, but that is likely to be later in the year. There is a risk of insufficient time to demonstrate, through testing, the effectiveness of key controls identified late in the process.

It is important to note that there is no generic "laundry list" of what will always be considered "key controls" and, due to differences in systems, procedures, business environments, and models, sound professional judgment is required during the identification process. Management should also give due consideration to the views of the external auditors and ensure they are comfortable with the process management uses for identifying key controls.

Controls may be preventive or detective — either prevent errors or detect their occurrence. Some experts include the determination of whether controls are preventive or detective in their process to identify key controls, because preventive controls are seen as stronger. However, management should recognize that an efficient and effective system of controls will use a combination of both, and the authors do not consider it critical to focus on whether controls are one or the other. Rather, management should instead focus on whether the controls in place are sufficient to ensure there are no misstatements of the financials and are appropriate in terms of management of business risk.

There are two schools of thought when it comes to identifying key controls:

- In the first, risks that may prevent the financial assertions from being satisfied are listed. Then, the controls that address those risks are identified. The benefit of this approach is that it is relatively straight-forward and familiar to most experienced auditors. It is also the approach recommended in PCAOB's AS 2. However, the risk is that the list of risks may not be complete.
- The second approach looks at the transactions that flow into the significant accounts and identifies the controls that assure the transactions are completely and accurately processed and recorded, and that only valid transactions are processed. The second approach, which has been adopted less frequently, includes controls that assure the safeguarding and existence of the assets and the presentation of account balances in the financial statements. The benefit of the second approach is that it provides more assurance that all the controls are addressed. However, it is more complex.

Both approaches have merit. Management should make a choice based on which is more consistent with the experience and training of the individuals managing the project, after consultation with the external auditor.

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

The majority of companies use a process that starts with the significant general ledger accounts by location, defines the relevant financial assertions for each, and then lists all the risks to achievement of the assertions. Finally, the key controls — those required to address each risk such that a material error is not likely — are identified. For example, the process may start with "Cash" at the headquarters location and identify "Existence" as one of the assertions to be achieved. The bank reconciliation is identified as the key control that addresses that assertion.

It is important to ensure the list of risks is complete. The external auditor may have a list of standard or common risks for different types of accounts and the internal auditor can assist with a review of the list of risks. An additional source, if the company uses specialized Section 404 software, is the vendor of the software, who typically has templates that management may use.

For companies with complex reserve calculations (e.g., inventory or product warranty reserves), attention should be given to ensuring there are key controls around all the information used in the reserve calculation (e.g., estimates of future sales prices, customer demand, etc.).

The alternative method also starts with the significant accounts by location, but differs by identifying the material transactions flowing into those accounts. For each material transaction, key controls are identified to ensure the transactions are completely and accurately recorded (including calculations) and that only valid transactions are recorded. In addition, key controls are identified to ensure the appropriate presentation of the significant accounts in the financial statements, and that all assets in significant accounts are safeguarded. For example, cash at the headquarters location is identified as a significant account and location. The bank reconciliation is identified as a key control because it helps ensure both the completeness and accuracy of cash recordings.

Both of these methods can result in the identification of too many controls, including duplication of controls, unless reviewed carefully. A number of reasonable tests can be performed to validate the list of key controls, including:

Highly Persuasive Test

Does the control have one or more characteristics that are highly persuasive to determine that it is a key control?

- Operating management considers it key, even if they are unable to link it to a risk or assertion.
- Common sense indicates it is a key control.
- The control addresses an assertion or risk that is not addressed by other controls.
- It directly addresses a section in the Sarbanes-Oxley legislation, for example, the code of ethics or whistle-blowing procedures.
- It describes a key role in monitoring the effectiveness of controls across the entity (e.g., internal auditing or the audit committee).
- The external auditor considers the control as key.

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

Acid Test

This test needs to be applied to each key control, but with caution to ensure management does not end up with an overly conservative list of key controls.

- If the key control fails, such that it is not consistently performed as documented, is there more than a remote likelihood of a material error in the financial statements?
- If the answer to the question above is "No," is that because there are additional controls (e.g., duplicative or later controls in the process)? Are those controls identified as key controls, and are they effective?

If controls that appear to be key to address a risk or assertion for a significant account fail the acid test, management should consult with the external auditor to reach agreement that they are not key. (Although it is management's responsibility to determine which are its key controls, the external auditor is responsible for assessing management's Section 404 process[xxviii]. In addition, it is more efficient if management and the external auditor can agree on, and then test (the same controls — as it becomes more likely that the auditor can place maximum reliance on management's testing.)

When discussing the results of the acid test with the external auditor, management may refer to the PCAOB's May 16, 2005 guidance — specifically, its Staff Questions and Answers (Number 38) relative to risk assessment and a top-down approach to their audit: "A top-down approach prevents the auditor from spending unnecessary time and effort understanding a process or control that does not affect the likelihood that the company's financial statements could be materially misstated … This approach also helps the auditor to identify and eliminate from further consideration accounts, disclosures, and assertions that have only a remote likelihood of containing misstatements that could cause the financial statements to be materially misstated."

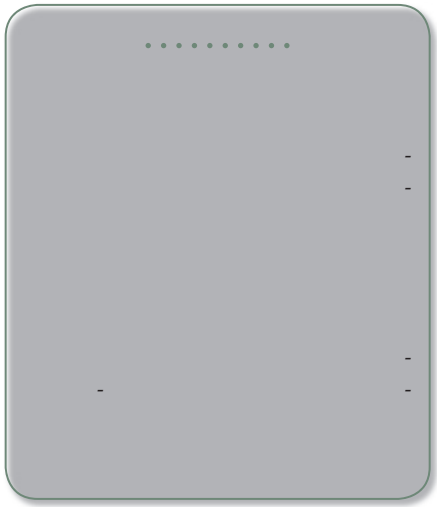
Once management has completed this process, it is prudent to consider the risk of a failure of one or more of the key controls. Points to consider include:

- Are there any higher level controls (e.g., analytical or other monitoring reviews, including executive dashboards and the use of key metrics) that would detect the failure of a key control and/or a material error resulting from a controls failure? For example, if the company measures inventory turns on a regular basis and investigates trends and significant fluctuations, that control is likely to detect a material error in inventory valuation or in the calculation of cost of sales. In such cases, it may be prudent to consider these as key controls.
- Are there additional controls, especially in higher risk areas, that should be added as key controls because they would compensate or mitigate the effects of a failure of a key control? An example might be where the key control — perhaps a review of major fixed asset additions against approved capital expenditure forms — is performed at a regional level. A backup key control may be added: the local review and approval of capital expenditures.

- If the number of key controls is low, it becomes more critical to:
  - Ensure operating management is aware of which controls are key and how important it is to ensure they are operating effectively throughout the year. Operating management may want to monitor performance through supervision and spot testing more carefully.
  - Perform testing early, to provide time for remediation and retesting.
  - Ensure any deficiencies are corrected promptly.

4) IDENTIFYING IT CONTROLS

This is an important area, and the management team should ensure sufficient attention is given to the identification of key IT controls by individuals with a broad understanding of the business and the overall Section 404 project. Experience has shown that, unless managed carefully, significant problems can arise.



- Failures to effectively link work performed on IT controls to the overall, top-down Section 404 risk assessment process and identification of key controls are common. Some external and internal auditors believe specific generic controls should exist in every organization, but that belief is often based on an assessment of technical risk that may not consider the existence of manual controls or the risk of error in the financial statements. It is critical to have a good understanding of why computer systems are important and the impact a failure in general controls may have.

  In other words, IT controls should be the result of a top-down approach. The PCAOB made the following comment in the November report:

  > "Most of the audit engagements reviewed by the Board's inspectors did not use a top-down approach … Auditors who used a bottom-up approach often spent more time and effort than was necessary to complete the audit."

- The scope of work may be more than required, impacting the cost of the project.

It is important to recognize that these comments apply equally to management (perhaps more so, as the auditors typically follow management's identification of key controls).

The authors recommend a process for identifying IT controls to document, assess, and test as follows:

1. Ensure that a single team manages the entire process, including IT-related controls, to ensure a single risk assessment is made. All the work should be driven with a common understanding of the need to focus on risk of material error in the financial statements.

2. Agree on the general approach and on the results of each key stage with the external auditor. It may be possible to realize savings in audit fees through effective joint planning.

3. When defining the key business processes, identify the applications used in those processes to handle the flow of material transactions.

4. When identifying key IT controls, recognize that:
   - Some key business controls are fully automated, for example the calculation of interest for banks or updating the correct general ledger account. These are clearly automated controls.
   - Some controls are partly automated. For most companies, a large number of controls are of this type, where the individual performing the control relies on a computer report or information on a computer screen.
   - Other controls are fully manual, for example the inspection of incoming materials for quality.

5. Key controls that are fully automated need to be documented to the same standard as manual controls. To facilitate testing, attention should be given to documenting the control operation in some detail on page 37.

6. Key controls that are only partly automated need to be examined carefully. If the manual portion of the control is sufficient to detect an error in the automated part (e.g., the computer report) then the control can be considered entirely manual, because no reliance is being placed on the computer system. An example of this is the bank reconciliation, where the control uses reports from the general ledger system listing the cash balance and the various transactions in the month. The reconciliation to the bank statement provides assurance that the reports are correct.

   However, if the automated part of the control is not assured by the manual part, then it will have to be tested as an automated control, as described on page 37.
   - An example of a report that requires further testing is a report of all transactions greater than a defined dollar limit. The individual reviewing and taking action on this report cannot know that the report is complete, and lists all items over the threshold. Therefore, the report should be tested as an automated control.

   Key controls using some form of end-user computing, including spreadsheets or Business Objects reports, may require special attention, as described further in Section G of the is guide[7].

7. Part of the strategy for testing automated controls, whether testing those identified in No. 5 or No. 6 above, will be reliance on general computer controls.

---

[7] *Some of the external audit firms emphasize a concept called "key reports," commonly described as reports used in key controls. However, the authors believe the only key reports that need to be examined as automated controls are those where an error would not be detected in the normal course of the manual part of the control.*

When automated controls are identified, management should identify, document, assess, and test the controls over the related applications. In addition, consideration should be given to any other applications involved in processing material transactions. If the identified key controls would not prevent or detect inappropriate processing or the unauthorized change of data related to those applications, and therefore could result in a material error in the financials, they should be included in the ITGC scope. In other words, the ITGC scope should address applications where a failure in the related ITGC is reasonably possible and could (again, there's a reasonable possibility) result in a material misstatement of the financials.

If an application processes material transactions but a failure in ITGC, which includes security, is not at least reasonably likely to result in a material error, then that application can be excluded from the ITGC scope for Section 404 purposes. (Note: there may be good reason to assess and test ITGC for operational and risk management purposes, even if there is no need to do so for Section 404).

Broadly speaking, information technology general controls (ITGC) provide assurance that applications are developed and subsequently maintained, such that they provide the functionality required to process transactions and provide automated controls. They also assure the proper operation of the applications and the protection of both data and programs from unauthorized change.

8. The balance of the strategy for testing automated or partly automated controls is the specific testing of the automated controls. However, before developing the plan for specific automated controls testing, management should consider *benchmarking.*

   Where there are good change management controls within ITGC over an application, management may decide to test only a sample of automated controls each year. The principle, called "benchmarking," is described in the PCAOB document issued May 16, 2005[xxix]. The principle needs to be applied to each automated control in turn, examining whether: (a) the software has been changed since the last time it was tested, (b) whether there are sound change management processes and controls relative to the software, and (c) whether the control is of such significance that risk demands it be tested every year.

   In principle, when a company has invested in effective and consistent change management controls, it should have increased assurance that the software (including automated controls) will provide the required functionality on a consistent basis. Management should consider this when planning which automated controls to test. Even if no changes have been made, it is advisable to test at least a sample.

   Testing of automated controls is discussed further on page 37.

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

5) IT GENERAL CONTROLS

ITGCs can be extensive and can include a significant number of controls relative to the development, maintenance, and operation of applications and infrastructure (e.g., operating systems and databases), as well as the security of the computer network, applications, and data. Due to ITGC's technical nature, the changing threats to network security, and cost constraints, it is difficult for IT management to design and operate controls that are fully effective, and IT auditors will usually find some deficiency. As a result, IT management at many organizations has incurred additional costs, including personnel, to ensure key ITGC controls are designed and operated adequately.

Failure to define the scope of ITGC carefully can result not only in too much work, but the need to address security and control issues that may have only a very indirect relationship to the possibility of errors in the financial statements. On the other hand, deficiencies in ITGC can result in material error if not mitigated or compensated for by controls in other areas.

- Deficiencies in application change management can imply the functionality in key automated controls is at risk. Even if the automated control is tested, there is reduced assurance that the control continues to operate as tested.
- Security weaknesses can increase the risk of unauthorized changes to data, bypassing normal transaction controls, or to applications, putting automated control functionality at risk.
- Computer operations control issues can imply that backups are in question and, if an application fails, errors could be introduced during the recovery. There could also be a risk that applications are not run properly, putting the functionality of automated key controls or the integrity of data (if interfaces are affected) at risk.

We recommend that management identify a set of control objectives for ITGC that can be applied to each in-scope application. The latter should include all applications that contain key automated controls, as well as all applications that process material transactions where an error in the processing could result in an undetected material error in the financials.

The control objectives should address each sub-area of ITGC:

- Development or major enhancement of new applications.
- Maintenance of existing applications.
- Application user management, such as approval of new user IDs and removal of user IDs for terminated or transferred employees and contractors.
- Management of change to the IT infrastructure (e.g., operating systems and database management systems).
- Computer operations (e.g., execution of applications; monitoring of and responding to application errors; backups of applications and data; and computer room security).
- Network security.

- General management and organization of IT (e.g., segregation of duties and the role of IT security within the organization).

Management then will identify which of these control objectives for each of the in-scope applications represent a risk that (a) is at least reasonably likely to occur, and (b) if it occurred is at least reasonably likely to result in a material error in the financials. For example, in some organizations, failures to achieve objectives related to anti-virus protection or intrusion detection may not present a risk to the proper operation of an SAP application, and thus may not represent a risk to the financial statements. Such failures may be deemed to represent only a risk of business disruption, not a risk of undetected change to SAP data or application functionality.

As with business processes, ITGC processes need to be documented and controls identified that will satisfy the control objectives identified above. Management should identify and test only those key controls necessary to achieve the control objectives for in-scope applications.

Detailed guidance for the efficient scoping of ITGC risks and related controls will be available in 2006 from The IIA (*A Guide to the Assessment of IT General Controls Scope Based on Risk*).

Before making the final selection of key ITGC controls, management should confirm that all meet the definition of a key control: that there is at least a reasonable risk of material error in the financial statements if any of the key ITGC controls fail. Although the effect is not direct, the ITGC key control failure might lead to a failure in one or more key business controls, or the undetected failure of application functionality.

6) TESTING AUTOMATED CONTROLS

In most cases, individuals with IT audit expertise will perform automated control testing; however, management may request IT staff to perform the tests. This is acceptable, but may not allow the external auditors to rely on management testing to reduce the scope of their work.

Each of the automated controls, including key reports, need to be tested unless benchmarking applies; an individual with IT audit experience will usually be able to identify the most appropriate test. Testing will normally consist of one or more of the following:

- Use of test data to confirm the proper operation of the control. The auditor, or IT staff with auditor review and approval, will enter transactions in the test environment and confirm the control operates as documented.
- Examination of related application code (a common technique when SAP is the application, where SAP configuration tables can be reviewed). The auditor must possess a solid understanding of the software configurations or code to perform this test.
- Use of audit software to reperform the functionality. For example, the auditor may use ACL or a Business Objects report to select and age open accounts receivable transactions and compare the results to the reports used by management.
- Manual reperformance of the control. In a few cases, where the control is not complex and the data not voluminous, the auditor may be able to recalculate totals or otherwise reperform the specific functionality of the key control.

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

Unless there are concerns in ITGC that indicate otherwise, automated controls need only be tested once each year (subject to benchmarking, as discussed previous). If ITGC issues indicate there is a significant risk that unauthorized, unapproved, or untested changes may be made to the automated controls, the frequency of testing should be increased with special attention given to year-end closing processes.

7) SEGREGATION OF DUTIES AND RESTRICTED ACCESS

Segregation of duties (SOD) and restricted access (RA) controls need to be identified, assessed, and tested where considered key. Key SOD and RA controls include those that:

- Are required for an authorization control to be effective. For example, if the business control requires that all purchase orders be approved in the system by the purchasing manager, it is critical to ensure that only the purchasing manager has that capability.
- Reduce the risk of a material fraud that could be reported incorrectly in the financial statements.

With restricted access, there is a risk of doing more work than is required for Section 404. Although there are excellent business reasons for restricting access to only those functions individuals need to perform their assigned tasks, it is important to remember that only fraud risk that is both material and also misstated in the financials is within scope for Section 404. *See the Fraud Risk Assessment section on page 42.*

Once the key controls have been identified, they should be tested. A suggested testing strategy includes:

- Test RA and SOD before mid-year to identify any issues and allow time for resolution or an explanation of how the risk is managed.
- Once management has completed all remediation, retest RA and SOD late in the third quarter or early in the fourth quarter. By then, the more significant issues will have been corrected, and the results should be positive.
- This is now an appropriate time for the external auditors to perform their tests, as management has completed their testing and obtained assurance that the appropriate controls are in place and operating effectively.

8) SPREADSHEETS AND OTHER END-USER COMPUTING ISSUES

Much has been made about the risks to financial reporting through errors in spreadsheets and end-user computing in general (including the use of Access databases and Business Objects reporting). Because spreadsheet errors have been found at a number of companies and have resulted in material errors in their financial statements, this risk needs to be acknowledged and addressed.

Risks related to spreadsheets (from hereon, that term also refers to other end-user software) include:

- Errors in the download from the company's systems, including:
  - An incomplete download (e.g., missing a general ledger (G/L) or a region).

  - An out-of-date download.
  - A partial download, where transmission or other errors prevented completion of the entire download.
  - Use of an intermediate database (e.g., a data warehouse) that is not complete, accurate, or current.
  - The incorrect population of the download data into the various cells in the spreadsheet.
- Errors in calculations, sorts, or other programmable elements of the spreadsheet.
- Use of an out-of-date spreadsheet (including use of a current spreadsheet where the calculations are not refreshed").
- Changes to the data by the user.
- Errors in the understanding or use of the spreadsheet (e.g., where the user is not the developer and picks up the wrong total).
- Changes to the spreadsheet by another, due to poor security.

Some consultants have advised the use of specialized software in this area, and there are many products of value. However, before acquiring and implementing additional products, the authors recommend management consider the following approach:

- When a key business control includes the use of a spreadsheet, determine whether an undetected error in the spreadsheet could cause the control to fail and result in a material error in the financial statements. Determine if the spreadsheet is essential to the key control (e.g., enabling a review of an estimate) or incidental (e.g., used to list the documents being reviewed).
- Will the normal operation of the control detect an error in the spreadsheet? There are two ways this can happen:
  - The spreadsheet is used in a reconciliation process. For example, if original documents are summarized in a spreadsheet and then compared to the updated general ledger balance, an error in the spreadsheet will result in an out-of-balance condition with the general ledger.
  - The control includes user procedures to confirm the completeness and accuracy of the spreadsheet. For example, if a spreadsheet is used to analyze sales invoices by region, then confirmation of the totals to the general ledger will ensure that the download of data into the spreadsheet is complete and the formulae are properly calculating the totals.

- If an error in the spreadsheet would not be detected in the normal operation of the control, understand where the risk is and take action accordingly:
  - If the risk is in the download from the general ledger (or other computer system) directly into the spreadsheet, consider changing the design of the control to include a user control (e.g., a user verification of the spreadsheet totals to the general ledger).
  - If the risk is around the download of information into a data warehouse or similar (e.g., Essbase or Hyperion), consider adding controls over the download and then ensuring that the spreadsheet is balanced back to the data warehouse.

- If the issue is that the user is entering data into the spreadsheet manually, consider adding a control to validate the completeness and accuracy of the data in the spreadsheet.
- If the risk of error is in the calculations, consider whether the user can review the results in such a way that it will confirm the calculations are correct. If the calculations are too complex for such a review, consider replacing the spreadsheet with a report or other program developed and maintained by IT. A risk of using complex calculations in a spreadsheet is that the user may inadvertently introduce a mistake into the spreadsheet. Converting the spreadsheet into a report developed and maintained by IT will provide greater assurance that the calculations will continue to function properly, with all changes to the calculations tested and approved, assuming that IT has adequate ITGC.
- If there is no alternative to relying on the spreadsheet and its calculations, then ensure there are controls similar to those discussed in ITGC over:

• The validity of changes to the spreadsheet, including testing and approval.
• Input (whether automated or manual) of data into the spreadsheet.
• The security of the spreadsheet, such that only valid, tested, and approved changes are made and that data is not inappropriately changed.
• The way in which the spreadsheet is used and the results interpreted. For example, there should be controls to ensure that all data is input and validated before the results of the spreadsheet are used in the key controls. In addition, there should be assurance (e.g., through documentation or user instructions) that the use of the spreadsheet is correct (e.g., the correct totals are used). An example of the latter is where a spreadsheet has multiple analyses of the data; the user should understand which analysis and which totals should be used.

When reviewing and assessing the adequacy of the design of key controls using one or more spreadsheets, the above should be considered. If a walkthrough or other formal assessment of the control design is performed, it should include a discussion of how the completeness and accuracy of the spreadsheet results are assured.

To assist the external auditor's review, and to provide a solid double-check in this area, management should consider developing an inventory of all spreadsheets that are a significant part of a key control or a critical part of the financial reporting process. The inventory should describe how assurance of the completeness and accuracy of each spreadsheet is obtained.

Testing of key controls should encompass the controls over the completeness and accuracy of the spreadsheet.

Where the spreadsheet is not assured by the normal operation of the control, management should consider performing periodic independent tests of the spreadsheet. For example, it may be included in the population of automated controls tested by IT auditors.

9) CONTROLS PERFORMED BY THIRD-PARTY ORGANIZATIONS (SAS 70 TYPE II REPORTS)

Many companies have achieved cost savings or other benefits by outsourcing selected functions, such as payroll processing, processing of stock options, or data center management. Management needs to consider these outsourced operations when developing the scope of the Section 404

assessment.[xxx] If key controls are operated by third-party organizations, they need to be assessed and tested before management can be assured that the controls are designed adequately and operating effectively.

One approach is to treat processes and related controls in the same way as management addresses processes and controls within the organization. Management needs to ensure the processes are documented adequately, identify and assess the adequacy of key control designs, then perform tests to confirm the controls are operating effectively and are consistent with the documentation. Management may find that the service provider has good documentation, in which case they need not duplicate that effort, even if the provider's documentation is not in the same format or style as the company's. Management may also be able to place some degree of reliance on any testing of its internal controls by the provider. However, management needs to consider not only the competence of the personnel performing such testing, but also the independence of the personnel from the provider's management.

Most service providers in the United States recognize their customers' need to obtain assurance over the providers' controls. Rather than have every customer send a team of auditors to document and test their controls, these providers engage a third-party auditor to perform an attest engagement under the American Institute of Certified Public Accountants (AICPA's) Statement of Auditing Standards Number 70 (SAS 70). This standard defines how independent auditors identify the controls to test, perform testing of the controls, and report the results. Reports from audits performed by independent audit firms in accordance with the provisions of SAS 70, as long as the report is what the standard calls a "type II" report (some U.S. providers only get a "type I" report, which is not sufficient for Section 404), can be relied upon by management as assurance that the providers' controls are adequate under certain conditions:

- Management needs to identify which key controls it relies on the provider to perform, review the report (which contains a description of the key controls tested), and confirm that the design of the control is sufficient to meet management's control objectives.
- The company typically will need controls that work with those at the service provider. For example, the company should have controls to ensure all transactions are transmitted to the provider for processing. Management should ensure these controls work effectively in combination with the provider's. Most SAS 70 reports include a description of the controls the provider expects its customers to have. This is a section management should review carefully.
- Management should review the report carefully to verify the testing is sufficient to ensure the adequacy of the controls on which they will rely, and then assess the results reported.

If the SAS 70 report identifies deficiencies, management needs to determine what impact the deficiencies have on the controls at the provider on which it relies. For example, the report may identify deficiencies in Windows NT servers at an outsourced data center, while the company's software runs only on Unix servers. Management may also find that controls within the company, compensate, or at least mitigate, the deficiencies.

Service providers do not always provide assurance that any deficiencies will be corrected and retested before their customers' year-ends. Although the authors believe management should work with the provider to include a commitment to address deficiencies in the contract, the provider

may not be responsive. Therefore, management should ensure excellent communications are in place to provide as much notice as possible of potential audit issues.

Outside the United States, providers often do not offer a SAS 70 type II report. Management needs to identify this early and plan accordingly. One option is to pay the provider to obtain such an audit, and another is to develop controls within the company that will address any risks to the financial statements. Finally, management may decide to switch providers to one that provides a SAS 70 type II report.

Additional information on a SAS 70 type II report can be obtained from the external auditor.

10) FRAUD RISK ASSESSMENT

The concept of a fraud risk assessment is one that is frequently misunderstood, even though PCAOB AS No. 2[xxxi] clearly states:

"The auditor should evaluate all controls specifically intended to address the risks of fraud that have at least a reasonably possible likelihood of having a material effect on the company's financial statements." [xxxii]

The key to an efficient consideration of fraud is to focus on fraud schemes that could result in a material misstatement of the financials[8]. Many thefts and frauds, Although significant and important to prevent — or at least detect — promptly, are unlikely to result in a material error in the financial statements.

For example:

- The theft of inventory at a company that conducts a full physical inventory at year-end would not result in an error at year-end because a write-off will have been taken.
- The approval and payment of duplicate or excessive payments for services are recorded correctly in the financial statements: the financials correctly reflect the amounts paid, on the appropriate line of the P&L.

There are a number of detailed guides (including guides from each of the major accounting firms) on how to address fraud risk. The high-level approach is to:

- Identify the fraud schemes applicable to the company that might result in a material error in the financials if undetected. Particular attention should be given to schemes involving the management override of controls, including the approval and processing of manual journal entries.
- Identify the key controls that would either prevent or timely detect any such fraudulent activity, and confirm the adequacy of their design.
- Ensure that the identified key controls are tested.

[8] *In this discussion, fraud includes the misappropriation of assets.*

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

One area of focus RA and SOD. It is possible to spend a significant amount of time assessing and testing these areas, because many frauds are the result of inappropriate access and especially a combination of access capabilities (e.g., the ability to both set up a vendor and approve invoices). In addition, there are significant business reasons (including the loss of assets) for ensuring appropriate RA and SOD are in place. The key to efficient Section 404 testing for RA and SOD is carefully focusing on access abilities where a resulting fraud could mean the financials are materially misstated. If management desires, additional RA and SOD testing for purely business risk management purposes may be added to the Section 404 testing — because the cost of additional testing may be minimal. However, these non-404 tests should be identified clearly as such to the external auditor.

G. TESTING KEY CONTROLS

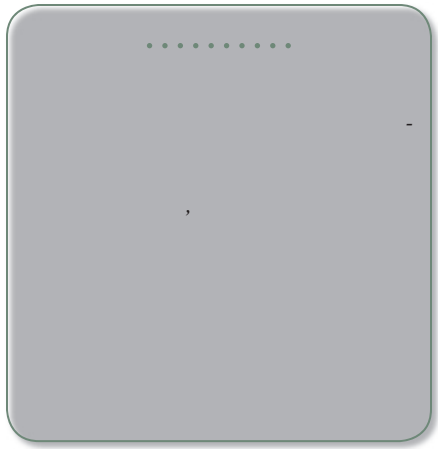
In theory, management has great flexibility in selecting techniques for testing key controls. They do not have to employ the same techniques (or even the same sampling criteria) as the external auditor[xxxiii]. However:

- The testing techniques should clearly provide a reasonable individual sufficient assurance that the controls are operating effectively as documented.
- If self-assessment techniques are used (these are not described here, but information can be obtained on this valuable approach from the internal or external auditor), there has to be a reasonable level of independent confirmation of the self-assessment.
- The testing needs to provide assurance that the controls are operating effectively at year-end, as that is the point in time at which the formal assessment is made. For tests performed earlier in the year, steps should be taken to update and roll-forward the results of the tests. Techniques that can be used include a limited reperformance of the earlier tests using fourth quarter transactions, or obtaining re-certifications by process owners of their key controls.
- The testing needs to be performed by competent and trained individuals. A number of organizations are requiring operating management and staff to perform regular testing of their controls. Although that may appear to be cost-effective (for example, it may free internal audit specialists to focus on valuable operational, compliance, and other control audits), management may need to provide objective reviews and retesting to ensure the tests are performed on a timely basis in accordance with quality standards and the results are reflective of actual operations. This additional review and testing might be performed by internal audit staff or a separate control testing group. Management should consider the total costs of testing and the most efficient use of resources when staffing the testing program.

This document will not explore in depth the testing techniques that are available. Management should select the approach most suitable for the organization after consultation with experts, including the internal auditor. Some of the techniques available include:

- Traditional testing of controls, which includes:
  - Performance of walkthroughs, which confirm the adequacy of the documentation as well as the design of the controls to meet the control objectives.
  - Inquiry, examination, and inspection of related documents to confirm that the control appears to be performed consistently as documented.
  - Reperformance of a sample of transactions to confirm that the control is being performed effectively.
- Continuous auditing, which includes the testing of transactions throughout the period. This is generally done with software that selects the transactions to be reviewed.
- Continuous monitoring. This technique relies on software to monitor transactions and not only identify transactions for testing, but especially to test 100 percent of the processed transactions for compliance with selected parameters. An example would be a test that identifies purchase orders issued in excess of approved requisitions. The software would report such exceptions for assessment as they occur. This technique merits attention and consideration, as several of the CPA firms are partnering with software companies to develop automated tools for continuous monitoring.
- Management self-assessment. There are several varieties of this technique, and management needs to consult with testing experts to ensure that the results of any self-assessment provide reasonable, objective evidence that the controls are operating as assessed. The risk

is that the individuals performing the assessment may not have direct knowledge of the operation of the control or may not perform a rigorous assessment, verifying the consistency of execution of the control.



Performing an annual walkthrough of key processes and controls is highly recommended. The external auditor is required to do walkthroughs, which help confirm the accuracy of the documentation as well as the adequacy of the controls. Walkthroughs by management will not reduce the requirement for the external auditors to perform their own walkthroughs[xxxiv], but they will detect errors early and ensure management:

- Has a clear and current understanding of the processes and their operation.
- Can identify and correct potential issues early.
- Will perform more efficient testing, as documentation issues have been removed.
- Makes more efficient use of the external auditor's time by ensuring the currency, completeness, and accuracy of the documentation.

Earlier, the statement was made that management "has great flexibility in selecting techniques to use for testing its key controls." The "in theory" reservation was included because management should always consider the total cost of the Section 404 program. That total cost includes the external auditor's fees. Management can minimize the total costs by maximizing the degree to which the external auditors can reduce their hours through reliance on management testing.

It is still unclear to what extent the external auditors are able to reduce their hours through reliance on management testing when that testing is other than traditional. This is a developing area and merits continued monitoring. However, for the areas where the external auditor is required to perform independent testing and cannot rely on management testing (e.g., control areas assessed as high risk), management may be able to employ less traditional, more cost-effective methods without impacting external auditor fees.

H. ASSESSING THE ADEQUACY OF CONTROLS, INCLUDING ASSESSING DEFICIENCIES

If all the key controls are properly identified, assessed to be adequately designed, and the results of testing indicates they are all operating effectively, management is able to assess the overall system of internal control over financial reporting as effective. But, in real life, exceptions are identified in testing. A number of key controls will be deemed either to be missing, deficient in design, or not operating effectively.

Management needs to decide whether these deficiencies mean that the system of internal control does not provide a reasonable level of assurance that there will not be material errors in future financial statements.

This is achieved by assessing each control deficiency to determine whether it represents a risk of an error, including the likelihood of the error and its potential magnitude. Each deficiency is assessed to determine whether it is *material, significant,* or neither. Then, management needs to determine whether a combination of deficiencies[9] is likely to represent a risk (an *aggregated* risk) that is material or significant.

The following definitions use the terms *material error* and *inconsequential* (as discussed on page 26 and 49, respectively), and *more than remote* likelihood. The latter is related to the term *reasonable assurance*, means that there is at least a reasonable likelihood, and is generally understood to be in the 5 percent to 10 percent probability range.

- A *material weakness* is one where the likelihood is *more than remote* that an error that is *material* to the financial statements will neither be prevented nor detected within a reasonable period of time. This is more than a test that the likelihood of an error is more than remote; it is a test of the likelihood of a material error.
- A *significant* deficiency is less severe. It means that the likelihood is *more than remote* that an error that is *more than inconsequential* to the financial statements will occur.

The external audit firms have adopted a framework for assessing deficiencies[xxxiv]. This approach is important for management to consider, as it is likely to be followed by the external auditor. However, there is no requirement for management to follow precisely the same process.

Management should adopt a principles-based approach, relying on their judgment, rather than a strict rules-based approach. The PCAOB also has advised the external auditors also to rely on their professional judgment in assessing deficiencies:

> "This evaluation requires an exercise of judgment, based on an assessment of what constitutes reasonable assurance under the circumstances, not on the mechanical application of a predetermined probability formula. Inspectors observed, however, that the quest for quantitative rules of thumb in the application of the definitions described above may have resulted in some auditors exercising less judgment than the standard requires in this area. Many engagement teams used a framework developed through the collective effort of nine firms for evaluating deficiencies. That framework uses terms such as 'gross exposure,' 'adjusted exposure,' and 'upper limit deviation rate.' The statistical precision suggested by these terms may have driven auditors' decision-making process unduly toward simplistic

[9] *As noted earlier, the key to an aggregated risk is that the controls are likely to fail at the same time, for example because they are performed at the same time by the same people or using the same computer system.*

quantitative thresholds and away from the qualitative evaluation that may have been necessary in the circumstances.

"This evaluation framework can result in decisions that are consistent with the provisions of Auditing Standard No. 2. Further, the use of the framework promoted consistency among different audit teams within and across firms. Nevertheless, the framework is not a substitute for the professional judgment that Auditing Standard No. 2 requires. Moreover, using this framework could, in some cases, lead auditors to spend more time evaluating the severity of a deficiency than otherwise would be necessary." (Report dated Nov. 30, 2005).

Management's process must ensure the following are considered:

1. **Could there be an error in the financial statements as a result of the control deficiency?** Note that some controls may present a greater risk of business disruption or fraud that does not result in a financial statement error. If the answer is "No," the process can stop and the deficiency can be assessed as neither significant nor material. Management should further reassess whether this should remain a key control.

   With respect to deficiencies in IT general controls, management should follow the risk assessment back up the chain. They should identify what control objective is impacted and to what extent; what applications the control objective and key control addresses; what automated controls are involved; and, what risk there is of an error in the financials.

   Entity-level controls also require special handling to determine what controls and processes may be impacted. It is not sufficient to simply say these controls are pervasive; instead, management needs to address specifics relative to risk to the financial statements. For example, if there are problems hiring trained accounting staff, what processes and controls are involved, and are there sufficient management-level reviews and controls that would detect or prevent errors?

2. **Are there compensating or mitigating controls (they must be key controls that have tested effective)?** To what extent do they reduce the risk? If the answer is that the risk is fully addressed, the process can stop and the deficiency can be assessed as neither significant nor material. Management should further reassess whether this should remain a key control, as it may be redundant.

   IT general controls and entity-level controls again require special attention. Compensating and mitigating controls for ITGC issues may be found not only within ITGC, but within the business controls. For example, if developers are found to have access to production data, there is a risk that they could change the data (deliberately or inadvertently) and introduce errors into the financials. However, reconciliations and other business controls may be effective in promptly identifying such errors. Similarly, once the true risk presented by entity-level controls is identified, compensating controls may be found within the business processes.

3. **Is the potential error in the financials more than inconsequential?** If the assessment is that the error cannot be more than inconsequential (this may be 20 percent of the materiality level), then the process can be stopped. Management should confirm that this remains a key control.

   The assessment of whether the error could be more than inconsequential must consider where the error would occur in the financial statements. It is relatively straightforward when the error is in the P&L. However, if the effect is only on balance sheet accounts, the error should be considered using a materiality gauge related to that account, rather than the traditional P&L measure. For example, if there is a risk that fixed asset additions are not promptly recorded, the impact may be on understated depreciation, fixed assets, and accounts payable. Assume the following set of facts: materiality is set (based on P&L) at $10 million, the potential understatement of gross fixed assets and accounts payable is $6 million, and depreciation could be $150,000 understated. Total fixed assets are $500 million and accounts payable is $300 million. Management would assess the error separately in light of its effect on P&L, fixed assets, and accounts payable. It would conclude that the potential error is inconsequential, even though the total risk, at $6 million, appears at first glance to be high. This is because the error is small relative to the size of the balance sheet accounts.

   If the error would affect a disclosure, management needs to consider whether the error is material relative to the disclosed amounts and the significance to the investors (and potentially the regulators) of the specific disclosure. One measure that might be considered is whether the identification of an error of such an amount in a prior period's financial statements would result in needing to restate those financials.

4. **Is the risk of an error that is more than inconsequential more than remote?** Once it has been established that there is a risk of an error that is more than inconsequential, management must determine whether it meets the criteria for either a significant deficiency or a material weakness:

   a. Question 3 (above) identified that there is a possibility of an error that is more than inconsequential. The next step is to determine whether the likelihood of that happening is more than remote. As previously stated, "more than remote" means at least reasonably likely and is generally considered to be in the 5 percent to 10 percent range. If not, the process can stop. If there is such a risk, then the issue probably represents at least a significant deficiency.

   b. Is the risk of a material error more than remote? If not, then subject to question 5 (below), the issue is a significant, but not a material, weakness. However, if the risk of a material error is more than remote, then there is probably a material weakness.

5. **Would a reasonable individual assess the deficiency as material?** This is the key "acid" test. Given that management may not assess its system of internal control over financial reporting as effective once they identify a material weakness, they should ask some additional questions to validate the assessment of a deficiency as material.

a. Does management truly believe, and would a reasonable person concur, that the probability of a material error in future financial statements, which would not be detected by other controls, is in the 5 percent to 10 percent range or more? The PCAOB, in their Nov. 30, 2005 report, stated:

> "The definitions in the standard [AS 2] … are designed to lead to a determination as to whether the deficiency would prevent a prudent official from concluding that he or she has reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles.
>
> "Further, the terms 'probable,' 'reasonably possible,' and 'remote,' should not be understood to provide for specific quantitative thresholds. Proper application of these terms involves a qualitative assessment of probability. Therefore, the evaluation of whether a control deficiency presents a 'more than remote' likelihood of misstatement can be made without quantifying the probability of occurrence as a specific percentage."

b. If the assessment of a deficiency is based on prior period errors, perhaps resulting in the restatement of prior period financials, is it reasonable to assess the current condition of internal controls (and therefore identify a material weakness) as ineffective?

This issue (assessing controls following a restatement) has become topical. While some external auditors have taken the position that there must be a material weakness if the financials are being restated, that is neither the position of the SEC nor the PCAOB. Both have indicated that while there is at least a significant deficiency, the underlying facts and circumstances must be considered. For example, if controls are improved in the current period by the hiring of additional technical accountants who then identify prior period accounting errors, then the current condition of internal controls is sound. The material weakness was in the prior and not the current period. On the other hand, if the error was detected by the external auditor and should have been, but was not, detected internally, that may indicate a material weakness in the technical competence of the internal staff.

H. ASSESSING THE ADEQUACY OF CONTROLS, INCLUDING ASSESSING DEFICIENCIES

To quote from the November 2005 PCAOB report: "Auditing Standard No. 2 describes certain circumstances that should be regarded as at least significant deficiencies and as strong indicators of a material weakness in internal control. The identification of one of these strong indicators is the beginning of the auditor's evaluation process of whether a material weakness, in fact, exists. Such indicators require heightened scrutiny, but they are not automatically material weaknesses. The Board's inspectors found that, in general, with respect to evaluating strong indicators — such as restatements of previously issued financial statements — auditors understood that the indicator required heightened scrutiny but was not irrefutable evidence of a material weakness."

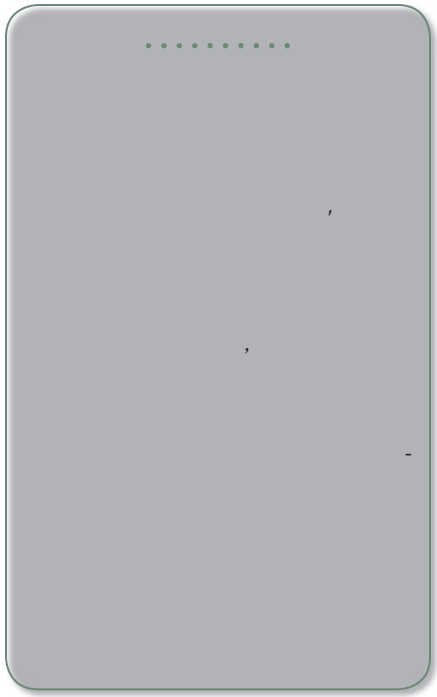
Significant deficiencies need to be reported to the audit committee, and management is not required to disclose them in either the quarterly or annual reports filed with the SEC. Management should give strong consideration to sharing with the audit committee any issues that are borderline significant deficiencies, even though finally not assessed as such, as this is prudent communications. The remediation of a significant deficiency is probably[xxxv] a material change in the system of internal control and should be reported in the interim period within which it occurs.

Material deficiencies need to be considered and will affect both the quarterly Section 302 certification and the annual Section 404 assessment, if they are not corrected prior to year-end. Because the Section 404 assessment is as of year-end, management has the opportunity to achieve a "clean" opinion if they can identify the deficiency early, implement corrective actions, and then test the corrected operations prior to year-end. The external auditor will also need to test the operation of the remediated controls.

I. MANAGEMENT'S REPORT ON INTERNAL CONTROLS: THE END PRODUCT

Whether in the annual assessment for Section 404 or the quarterly certification for Section 302, the language of management's report will be based substantially on the advice of counsel. However, there are certain drivers that management should consider:

- Management has a great deal of latitude in describing the condition of its internal controls. The only formal requirement is that they don't assess the controls as effective when there is a material weakness. Other requirements are being defined over time as the SEC responds to filings and sets expectations for content (counsel can advise on these matters).
- The assessment should clearly describe management's opinion. What is the true condition of the system of internal control at the end of the year? Is it sufficiently robust to provide reasonable assurance that material errors will either be prevented or detected? The investor should be able to read the assessment and understand whether the company has adequate controls to run the business and report the results. (This is especially true when there is pressure to report a material weakness as a result of accounting errors in a prior period. Management should determine whether the current system of internal control is adequate, providing reasonable comfort related to the reliability of future financial statements, and not report deficiencies they do not believe relate to the current condition or future filings. In these circumstances, management may feel pressure to follow the rules at the expense of the principles. The assessment should reflect management's assessment of the controls and not mislead the investor as to their effectiveness.)



- The root cause of deficiencies should be understood. Control failures may be symptoms of a larger problem related to resources or management. The overall system will not be corrected until the larger problem is resolved, and, when known, the root cause should be reported. That is the true deficiency.
- When deficiencies are reported, sufficient related information should be provided to enable the investor to understand their significance, the risk they represent, and how management will ensure the integrity of future financial statements.

J. CLOSING THOUGHTS ON EFFICIENCY

All agree that the Section 404 requirement has improved the quality of internal control systems through increased attention by both management and the external auditor. However, there is less than universal agreement that the improvement has been justified relative to the enormous cost.

The following checklist may help management teams ensure their Section 404 program is efficient.

1. Has operating management taken ownership of their processes and documentation, rather than leaving it to the Section 404 team or the internal audit function?

2. Does operating management update all process and control documentation promptly throughout the year and not just when testing starts? Is there an effective change management process in place, including the timely assessment of process changes for their potential impact on key controls?

3. Is operating management committed to prompt assessment and remediation of all control deficiencies? Where not justified based on management's assessment of risk and cost, is management committed to providing such assessment promptly so the effect on management's overall assessment of controls can be identified and discussed with senior management?

4. Has a top-down, risk-based approach been used to identify the key controls? Is management confident that all identified key controls are truly key? Has the design of the related processes been reviewed to determine if changes can result in fewer and more effective controls, relying more on automated controls or on higher-level controls (e.g., detailed reconciliations and flux analyses)? The fewer the controls to test, the lower the cost.

5. Is management of the Section 404 program at a sufficiently high level within the organization to:
   - Influence operating management relative to completion of their responsibilities?
   - Communicate effectively with executive management relative to progress and potential issues?
   - Negotiate as needed with the external auditor (e.g., to increase reliance on management testing, agree on key controls early, or address concerns as they arise)?

6. Is the use of internal resources optimized, including the use of internal auditors to perform testing or to validate testing performed by management staff?

7. Has overall staffing been optimized, reducing reliance on more expensive external consultants and testers?

8. Has reliance by the external auditor on management testing been optimized?

J. CLOSING THOUGHTS ON EFFICIENCY

9. Does the external auditor follow a top-down, risk-based approach as discussed in the May 16 and Nov. 30, 2005, PCAOB documents?

10. Is there a detailed project plan:
    - That includes a walkthrough of all significant processes early in the year (preferably in the first quarter)?
    - With testing scheduled in such a way that all key controls are tested by mid-year, with additional testing to update the results scheduled closer to year-end? This enables the external auditors to start their walkthroughs and testing early, providing time for management to address and remediate any deficiencies identified in either management or external auditor testing.
    - That includes all key activities required to complete the program, including fraud risk assessment, end-user computing issues, assessment of SAS 70 reports from service providers, etc.?
    - That details all required resources, including specialists (e.g., for IT and/or tax processes and controls), so they can be scheduled early?
    - With regular reporting to senior management that focuses on key metrics and issues, such as:
        - Progress against an established timetable, highlighting steps that are or may be behind schedule?
        - The percentage of key controls tested compared to scheduled completion level?
        - The number and percentage of key controls failing?
        - The number of failed controls that are potentially significant to the Section 404 assessment?
        - The number of failed controls where remediation will not be completed within 30 days (so senior management can focus on timely completion)?
        - The number of key controls where remediation and retesting may not be completed with sufficient time for the external auditor to retest (these are likely to be open deficiencies at year-end)?
        - Costs to date and projected through the end of the year?
        - Potential resource issues?
        - Other issues, such as coordination and concerns raised by the external auditor?

11. Has there been communication and coordination with all service providers to ensure that a SAS 70 type II report will be available at the appropriate time, and that early warning of potential deficiencies identified during the SAS 70 audit is provided?

12. Finally, is the Section 404 program itself assessed for effectiveness on a continuing basis, to ensure it is improved as the organization learns from experience and benefits from changes in regulations or their interpretation?

ADDITIONAL REFERENCE MATERIALS

SEC:

- "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports" at http://www.sec.gov/rules/final/33-8238.htm

- "Commission Statement on Implementation of Internal Control Reporting Requirements" (May 16, 2005) at http://www.sec.gov/news/press/2005-74.htm

- "Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports - Frequently Asked Questions" (revised Oct. 6, 2004) at http://www.sec.gov/info/accountants/controlfaq1004.htm

PCAOB:

- "Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements" at http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_2.pdf

- "Policy Statement Regarding Implementation of Auditing Standard No. 2" (May 16, 2005 guidance) at http://www.pcaobus.org/Rules/Docket_014/2004-09-15_Release_2004-008.pdf

- "Staff Questions and Answers on Auditing Standard No. 2" at http://www.pcaobus.org/Standards/Staff_Questions_and_Answers

- "Report On The Initial Implementation Of Auditing Standard No. 2, An Audit Of Internal Control Over Financial Reporting Performed In Conjunction With An Audit Of Financial Statements" at http://www.pcaobus.org/Rules/Docket_014/2005-11-30_Release_2005-023.pdf

COSO:

- "Internal Control — Integrated Framework, Executive Summary" at http://www.coso.org/publications/executive_summary_integrated_framework.htm

THE IIA:

- "Internal Auditing's Role in Sections 302 and 404 of the Sarbanes-Oxley Act" at http://www.theiia.org/download.cfm?file=1655

- "Sarbanes-Oxley Section 404 Work: Looking at the Benefits" at http://www.theiia.org/?doc_id=5161

DELOITTE:

- "Taking Control: A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002" at http://www.deloitte.com/dtt/whitepaper/0,1017,sid%253D36513%2526cid%253D54135,00.html

- "Sarbanes-Oxley Section 404: 10 Threats to Compliance" at http://www.deloitte.com/dtt/article/0,1002,sid%253D36513%2526cid%253D58359,00.html

ADDITIONAL REFERENCE MATERIALS

ERNST & YOUNG:

- "Emerging Trends in Internal Controls — Third Survey" at http://www.ey.com/global/content.nsf/US/AABS_-_Assurance_-_Library_-_Registration

- E&Y Summary – PCAOB Standard No. 2: Audits of Internal Control Over Financial Reporting at http://www.ey.com/global/content.nsf/US/AABS_-_Assurance_-_Library_-_Registration

KPMG:

- "Making Sarbanes-Oxley Section 404 Compliance Sustainable" at http://www.us.kpmg.com/RutUS_prod/Documents/9/Sustaining_Web.pdf

PRICEWATERHOUSECOOPERS:

- "Management's Responsibility for Assessing Internal Control Effectiveness of Financial Reporting Under Section 404 of the Sarbanes-Oxley Act" at http://www.pwc.com/extweb/pwcpublications.nsf/4bd5f76b48e282738525662b00739e22/75d798ef7d9fc9c385256e3e005cec14

- "How to move your company to sustainable Sarbanes-Oxley compliance — from project to process" at http://www.pwc.com/Extweb/pwcpublications.nsf/docid/31F021B50359960385256FF60056C4B6/

PROTIVITI:

- "Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements - Third Edition" at http://www.protiviti.com/?pgTitle=Sarbanes-Oxley%20Section%20404%20FAQs

FINANCIAL EXECUTIVES INTERNATIONAL:

- "Sarbanes-Oxley Section 404 Implementation Survey" at http://www.fei.org/404_survey_3_21_05.cfm

- "Sarbanes-Oxley Section 404 Compliance: From Project to Sustainability"

NOTES

i See the Additional Reference Materials section for links to the major sites.

ii Included in the quarterly financial statements filed on Form 10-Q with the SEC.

iii "Report On The Initial Implementation Of Auditing Standard No. 2, An Audit Of Internal Control Over Financial Reporting Performed In Conjunction With An Audit Of Financial Statements," PCAOB Release No. 2005-023, Nov. 30, 2005.

iv Of note is this excerpt from Institutional Shareholder Services' "ISS U.S. Corporate Governance Policy - 2006 Updates":

> "Companies with significant material weaknesses identified in the Section 404 disclosures potentially have ineffective internal financial reporting controls, which may lead to inaccurate financial statements, hampering shareholders' ability to make informed investment decisions, and may lead to the destruction of public confidence and shareholder value."

v Executives at some companies have informed the authors that their external auditors told them if they have more than a specified number of control deficiencies, they could not assess their controls as effective. Others have been told that specific deficiencies (for example, failing to monitor the activities of the database administrator, or failing to have a comprehensive fraud assessment program) are always at least significant and probably material deficiencies. These specific cases are not consistent with the language (and we believe the intent) of AS 2, nor of the guidance from the SEC. Although some may disagree, AS 2 is fundamentally a principles-based standard that emphasizes the use of judgment by both management and the external auditor.

vi In this guide, the terms *material error* and *material misstatement* have been used inter changeably to represent the risk of a material error in the financial statements filed with the SEC, regardless of whether the error is the result of fraud or an inadvertent control failure.

vii In AS 2, the PCAOB used the term "reasonably possible." In developing the rules for the Section 404 report, the SEC used the term "reasonably likely." In this guide, we have used the terms synonymously, meaning more than remote, but less than probable.

viii The user of the Section 404 assessment should understand that the quality of the system of internal control as of the reporting date is only an indication of future results and depends, among other matters, on there being no significant change to the internal control financial report (ICFR). It should be noted that the PCAOB requires (in AS 2) that the report of the external auditors include the following statement: "projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate."

ix The Financial Executives International (FEI) study released in May 2005 reports external costs represented approximately 57 percent of total costs.

x Surveys on external audit costs related to Section 404 have varied significantly. Although some have indicated an average increase of 40 percent (the FEI study released in May 2005 reports the portion of the auditors' fees related to Section 404 averaged 57 percent of the annual statement fee), many companies have experienced far greater increases. A December 2005 survey by CRA International reported that external auditor costs represented only 26 percent of total Section 404 costs at larger companies, with market capitalization more than $700 million, and 25 percent at smaller companies. By contrast, the FEI study shows external auditor fees averaged about 43 percent of total costs.

xi The role of the internal audit function in Section 404 testing has been discussed in detail in The IIA's report "Internal Auditing's Role in Sections 302 and 404 of the Sarbanes-Oxley Act," released on May 26, 2004. Key points addressed in the document related to assistance with testing include:

"It is management's responsibility to ensure the organization is in compliance with the requirements of Sections 302 and 404 and other requirements of the Act, and this responsibility cannot be delegated or abdicated. Support for management in the discharge of these responsibilities is a legitimate role for internal auditors. The internal auditors' role in their organization's Sarbanes-Oxley project can be significant, but also must be compatible with the overall mission and charter of the internal audit function. Regardless of the level and type of involvement selected, it should not impair the objectivity and capabilities of the internal audit function for covering the major risk areas of their organization. Internal auditors are frequently pressured to be extensively involved in the full compendium of Sarbanes-Oxley project efforts as the work is within the natural domain of expertise of internal auditing." (Executive Summary)

"Activities that are included in the internal auditor's recommended role in supporting the organization in meeting the requirements of Sections 302 and 404 include:

- Project Oversight.
- Consulting and Project Support.
- Ongoing Monitoring and Testing.
- Project Audit."

(Recommended Role of Internal Audit)

"Ongoing Monitoring and Testing

- Advise management regarding the design, scope, and frequency of tests to be performed.
- Independent assessor of management testing and assessment processes.
- Perform tests of management's basis for assertions.
- Perform effectiveness testing (for highest reliance by external auditors).
- Aid in identifying control gaps and review management plans for correcting control gaps.
- Perform follow-up reviews to ascertain whether control gaps have been adequately addressed.

- Act as coordinator between management and the external auditor as to discussions of scope and testing plans.
- Participate in disclosure committee to ensure that results of ongoing internal audit activities and other examination activities, such as external regulatory examinations, are brought to the committee for disclosure consideration."

(Recommended Role of Internal Audit)

xii In some cases, efficiencies can also be achieved through a redesign of the controls. Some believe that reliance on more automated controls may allow a reduction of cost, as automated controls need to be tested only once, while manual control testing generally requires a larger sample of transactions. However, increasing the number of automated controls may also require additional testing of IT general controls, which is relatively expensive. Any redesign to achieve cost-savings in testing should consider the total cost of testing, including testing of IT general controls.

xiii The SEC provided guidance, in its January 2002 Frequently Asked Questions (FAQ) No. 22, that a formal evaluation of internal controls (similar to that required for Section 404) is not required by current regulations to complete the Section 302 certification. Their answer to FAQ 22 is excerpted in note xxxv below.

xiv Small businesses and foreign filers will use the equivalent forms: 10KSB and 20-F.

xv It is notable that the Foreign Corrupt Practices Act of 1977 directed that internal controls are the responsibility of management.

xvi PCAOB AS 2 is based on the COSO definition of internal control, as is Codification of Statements on Auditing Standards Section 319 ('Auditing Standards Section 319).

xvii Securities Exchange Act Rules 13a-15(f) and 15d-15(f).

xviii COBIT 4.0 is available at www.isaca.org/cobit.

xix This is described further in "A Framework for Internal Auditing's Entity-Wide Opinion on Internal Control" (IIA Research Foundation, 2004) and "Internal Audit Reporting Relationships: Serving Two Masters" (IIA Research Foundation, 2003).

xx The rules were first mentioned in an SEC release in August 2002 and incorporated into the Securities Exchange Act of 1934 (as amended) Rules 13a-15(e) and 15d-15(e).

xxi In question 23 of its October 2004 FAQ report, the SEC addressed whether the assessment of internal controls over financial reporting included required supplementary schedules. As indicated below, their conclusion was that the assessment does not currently need to be included within the scope of that assessment.

"Q: The Commission's rules implementing Section 404, announced in Release No. 34-47986, require management to perform an assessment of internal control over financial reporting which includes the 'preparation of financial statements for

external purposes in accordance with generally accepted accounting principles.' Does management's assessment under the Commission's rule specifically require management to assess internal control over financial reporting of required supplementary information? Supplementary information includes the financial statement schedules required by Regulation S-X as well as any supplementary disclosures required by the Financial Accounting Standards Board (FASB). One of the most common examples of such supplementary information is certain disclosures required by the FASB Standard No. 69, Disclosures about Oil and Gas Producing Activities.

"A: Adequate internal controls over the preparation of supplementary information are required and therefore should be in place and assessed regularly by management. The Commission's rules in Release No. 34-47986 did not specifically address whether the supplementary information should be included in management's assessment of internal control over financial reporting under Section 404. A question has been raised as to whether the supplementary information included in the financial statements should be encompassed in the scope of management's report on their assessment of internal control over financial reporting.

"The Commission staff is considering this question for possible rulemaking. Additionally, the Commission staff is evaluating broader issues relating to oil and gas disclosures and will include in its evaluation whether rulemaking in this area may be appropriate. Should there be any proposed changes to the current requirements in this area, they will be subject to the Commission's standard rulemaking procedures, including a public notice and comment period in advance of rulemaking. As a result, internal control over the preparation of this supplementary information need not be encompassed in management's assessment of internal control over financial reporting until such time that the Commission has completed its evaluation of this area and issues new rules addressing such requirements."

xxii Current reports include Form 6-K, definitive proxy materials, and definitive information statements.

xxiii In its final rules implementing Section 404, the SEC made the following comments related to the difference between internal controls over financial reporting and disclosure controls. Please note the italicized sections:

"We agree that some components of internal control over financial reporting will be included in disclosure controls and procedures for all companies. *In particular, disclosure controls and procedures will include those components of internal control over financial reporting that provide reasonable assurances that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles.* However, in designing their disclosure controls and procedures, companies can be expected to make judgments regarding the processes on which they will rely to meet applicable requirements. In doing so, *some companies might design their disclosure controls and procedures so that certain components of internal control over financial reporting, pertaining to the accurate recording of transactions*

and disposition of assets, or to the safeguarding of assets, are not included. For example, a company might have developed internal control over financial reporting that includes as a component of safeguarding of assets dual signature requirements or limitations on signature authority on checks. That company could nonetheless determine that this component is not part of disclosure controls and procedures. *We therefore believe that while there is substantial overlap between internal control over financial reporting and disclosure controls and procedures, many companies will design their disclosure controls and procedures so that they do not include all components of internal control over financial reporting."*

We concur with the SEC's observation that the referenced controls could be part of a company's system of internal control and yet not be included in disclosure controls. However:

- As noted by the SEC, disclosure controls will include all the components of internal control over financial reporting required to provide reasonable assurance over the reliability of the financial statements. By definition, those are key controls.
- The controls that the SEC has referenced as examples of controls that are included in ICFR but excluded from disclosure controls would not be considered key controls for Section 404 purposes.

Therefore, although the SEC's position is that there is only "substantial overlap" between ICFR and disclosure controls, in practice, the authors believe there will be few situations where key controls for Section 404 are not included in disclosure controls.

Some experts, including certain specialized attorneys, have taken a different approach. Arguments include:

- Disclosure controls only relate to the design of controls and not their operation. If a material weakness relates only to the operation of a control (i.e., it is adequately designed but not consistently followed), these experts believe management can report an ineffective system of internal control for Section 404, but an effective system of disclosure controls for Section 302. However, the authors believe such a determination is likely to confuse, rather than inform investors.
- Safeguarding of assets is included in the scope of internal controls for Section 404 but not in disclosure controls for Section 302. However, ICFR for Section 404 relates to controls that prevent or detect a misstatement of the financials. A misstatement of the financials filed with the SEC is, by definition, within the scope of disclosure controls.

xxiv In this guide, the term *interim assessment* of internal controls or disclosure controls is used to refer to what the SEC describes as the *periodic evaluation* of those controls.

xxv Some companies and external auditors have considered materiality relative to interim financial statements when defining significant accounts. In their May 2005 Staff Report, the SEC made it very clear that:

> "Companies generally should determine the accounts included within their Section 404 assessment by focusing on annual and company measures rather than interim or segment measures. If management identifies a deficiency when it tests a control, however, at that point it must measure the significance of the deficiency by using both quarterly and annual measures, also considering segment measures where applicable."

xxvi The SEC and PCAOB guidance references "significant accounts," meaning individual lines in the financial statements, rather than "significant *general ledger* accounts." We recommend defining significant accounts at the general ledger level, as this provides an improved opportunity to refine the scope of the Section 404 assessment. For example, an individual line in the financial statements may be below the planning materiality level — but contain a number of general ledger accounts that exceed planning materiality and that may not always offset each other.

Management may, for a number of reasons, find that some individual lines in the financial statements do not appear to have any significant general ledger accounts. For example, the numbers may be small. In this case, at least one key control must be identified — as each line is presumed to be significant. Management should consider whether there is one or more higher level controls that provide the necessary assurance that any material error in the line would either be prevented or detected.

xxvii The timely detection of an error is critical, otherwise detection may occur after the financial statements have been filed with the SEC, leading to the potential need for restatement.

xxviii It is possible for the external auditor and management to take top-down and risk-based approaches and reach different conclusions on which controls are key. As long as management has followed a reasonable process and defined key controls that address the likely risks to significant accounts, the external auditor should be able to draw a satisfactory opinion with regard to management's assessment.

xxix The PCAOB discussed benchmarking (Staff Questions and Answers, May 16, 2005, Number 45) as follows :

> "In general, to render an opinion as of the date of management's assessment, the auditor needs to test controls every year. This type of evidence is needed regardless of whether controls were found to be effective at the time of the prior annual assessments or whether those controls have changed since that time, because even if nothing significant changed about the company — the business model, employees, organizational structure, etc. — controls that were effective last year may not be effective this year due to error, complacency, distraction, and other human conditions that result in the inherent limitations in internal control over financial reporting. Automated application controls, however, will continue to perform

a given control (for example, aging of accounts receivable, extending prices on invoices, performing edit checks) in exactly the same manner until the program is changed. Entirely automated application controls, therefore, are generally not subject to breakdowns due to human failure, and this feature allows the auditor to 'benchmark,' or 'baseline,' these controls.

"If general controls over program changes, access to programs, and computer operations are effective and continue to be tested, and if the auditor verifies that the automated application control has not changed since the auditor last tested the application control, the auditor may conclude that the automated application control continues to be effective without repeating the prior year's specific tests of the operation of the automated application control. The nature and extent of the evidence that the auditor should obtain to verify that the control has not changed may vary depending on the circumstances, including depending on the strength of the company's program change controls.

"When using a benchmarking strategy for a particular control, the auditor also should consider the importance of the effect of related files, tables, data, and parameters on the consistent and effective functioning of the automated application control. For example, an automated application for calculating interest income might be dependent on the continued integrity of a rate table used by the automated calculation.

"To determine whether to use a benchmarking strategy, the auditor should evaluate the following factors. As these factors increase in significance, the control being evaluated should be viewed as well suited for benchmarking. As these factors decrease in significance, the control being evaluated should be viewed as less suited for benchmarking. These factors are:

- The extent to which the application control can be matched to a defined program within an application.
- The extent to which the application is stable (i.e., there are few changes from period to period); and whether a report of the compilation dates of all programs placed in production is available and is reliable. (This information may be used as evidence that controls within the program have not changed.)

"Benchmarking automated application controls can be especially effective for companies using purchased software when the possibility of program changes is remote — for example, when the vendor does not allow access or modification to the source code.

"At some point, the benchmark of an automated application control should be reestablished. To determine whether to reestablish a benchmark, the auditor should evaluate the following factors:

- The effectiveness of the IT control environment, including controls over application and system software acquisition and maintenance, access controls, and computer operations.

- The auditor's understanding of the effects of changes, if any, on the specific programs that contain the controls.
- The nature and timing of other related tests.
- The consequences of errors."

xxx Management can reference the PCAOB's answer to Question 24 on Service Organizations in its "Staff Questions and Answers" issued June 23, 2004.

xxxi Paragraph 24 of Auditing Standard No. 2

xxxii SAS 99 makes a similar statement: "For purposes of the Statement, fraud is an intentional act that results in a material misstatement in financial statements that are the subject of an audit."

xxxiii This was affirmed in the PCAOB guidance to the CPA firms on May 16, 2005, in Staff Questions and Answers, Number 47 and Number 49. The relevant passages are in italics.

47: *Management's daily interaction with the system of internal control provides it with a broader array of procedures to achieve reasonable assurance for its assessment of internal control over financial reporting than the auditor has available.* The auditor should recognize this difference when evaluating the adequacy of management's assessment.

"Paragraph 40 of Auditing Standard No. 2, which addresses the auditor's evaluation of management's assessment process, recognizes the important difference between management's assessment and the auditor's testing. The fifth bullet of that paragraph cites as *examples of procedures that management could use to obtain sufficient evidence of the operating effectiveness of controls 'inspection of evidence of the application of controls, or testing by means of a self-assessment process, some of which might occur as part of management's ongoing monitoring activities.' For example, management might be able to determine that controls operate effectively through its direct and ongoing monitoring of the operation of controls.* This determination might be accomplished through performing regular management and supervisory activities, monitoring adherence to policies and procedures, and performing other routine actions. For instance, a supervisor's review of a monthly account reconciliation prepared by one of his or her subordinates could be a monitoring control that also provides management with evidence supporting its assessment of internal control over financial reporting, if the results of the supervisor's review were evaluated and documented as part of management's assessment. To appropriately evaluate the adequacy of management's assessment as directed by the standard, the auditor needs to recognize these other types of procedures that are available to management as part of the basis for its assessment.

"**49:** *The auditor should not evaluate the adequacy of management's assessment by simply comparing, on a control-by-control level, whether management's testing was at least as extensive as the auditor's. The nature and extent of the procedures*

that management uses to support its assessment should be determined by management, independent of the auditor's decisions about the nature, timing, and extent of the auditor's procedures. The procedures that management performs to support its assessment might be different from the auditor's procedures, yet still provide management with an adequate basis for its assessment, for several reasons.

"First, as discussed in Staff Question No. 47, *management has a broader array of procedures available to support its assessment than the auditor. As discussed further in Staff Question No. 48, management also may use self-assessment in particular areas to support its overall assessment of internal control over financial reporting. In this circumstance, the auditor should evaluate whether management's overall assessment process includes periodic, objective validation of the effectiveness of self- assessments in individual areas, such as testing by internal auditors, to verify the effectiveness of self-assessments. This type of validation of self-assessments need not occur every period for every area in which a self-assessment is performed. Management's overall assessment process, however, should include a rational approach for determining how frequently and extensively to verify the effectiveness of self-assessments.*

"The work that management performs in connection with its assessment can have a significant effect on the nature, timing, and extent of the work of the auditor. The more extensive and reliable management's assessment is, the less extensive and costly the auditor's work will need to be."

xxxiv Some companies have gained efficiencies by conducting joint walkthroughs with the external auditors (this is more likely when the management testing is performed by the internal audit function).

xxxv The framework was developed by nine CPA firms in association with a respected academic. It can be found at the Financial Executives International's (FEI's) Web site: http://www.fei.org/download/Framework_10_29.pdf#search='Process%2FTransactionLevel%20Exceptions%20and%20Deficiencies

xxxvi We recommend consulting with SEC counsel, although it appears reasonable to assume that if a material weakness is material to the investor, then its resolution is highly likely to be a material change in the system of internal controls — and similarly likely to be material to the investor.

In January 2002, SEC staff issued answers to a number of FAQ. The answer to question 22 is relevant, and key portions are highlighted in the extract below:

"Although proposed amendments to Exchange Act Rules 13a-15 and 15d-15 would impose a requirement on an issuer's management to conduct an evaluation, with the participation of the issuer's CEO and CFO, of the effectiveness of the issuer's internal controls and procedures for financial reporting … the Commission's rules currently do not specifically require an issuer's CEO or CFO, or the issuer itself, to conduct periodic evaluations of the issuer's internal controls or the issuer's internal controls and

procedures for financial reporting. Some elements of internal controls are included in the definition of *disclosure controls and procedures*. There is a current evaluation requirement involving the CEO and the CFO of that portion of internal controls that is included within disclosure controls and procedures as part of the required evaluation of disclosure controls and procedures. We expect that issuers generally also would engage in an evaluation of internal controls. We believe that issuers generally currently evaluate internal controls, for example, in connection with reviewing compliance with Section 13(b) of the Exchange Act or in connection with the preparation or audit of financial statements.

"[T]o the extent that an issuer has conducted an evaluation of its internal controls as of the end of the period covered by the report, including under the circumstances described
in the preceding paragraph, *the issuer should disclose any significant changes to the internal controls* or in other factors that could significantly affect these controls subsequent to the date of their evaluation, *including any corrective actions with regard to significant deficiencies and material weaknesses.* If the issuer has made any significant changes to internal controls or in other factors that could significantly affect these controls, such changes would presumably follow some evaluation, in which case the required disclosure must be made."

ACKNOWLEDGEMENTS

The Institute of Internal Auditors would like to thank several individuals who assisted in developing this guide. The principal author was Norman Marks. Contributions were made by Philip Moulton and Pierre Pradal. We would also like to thank the following for taking the time to review drafts and provide constructive suggestions for improvement:

Bruce Adamec

Dick Anderson

Doug Anderson

Hubertus Buderath

Jackie Cain

Lee Ann Campbell

Roger Herd

Steve Jameson

Tim Leech

Sandford Liebesman, Ph.D.

Warren Malmquist

Patricia Miller

Heriot Prentice

Larry Rittenberg, Ph.D.

Peter Schlesiona

Kyoko Shimizu

Gil Simonetti

Dan Swanson

James M. Sylph

Jay Taylor

Jeffrey Thomson

Louis Vaurs

Curt Verschoor, Ph. D.

Jody Whitley

The Institute of Internal Auditors

PROFESSIONAL GUIDANCE
Setting the Standard

Order No. 1014
Member US $25
Nonmember US $30
Event pricing US $ 22.50

ISBN 0-89413-593-7