SECURITIES AND EXCHANGE COMMISSION

17 CFR PART 240

[Release No. 34-54122; File No. S7-11 -06]

RIN 3235-AJ58

CONCEPT RELEASE CONCERNING MANAGEMENT'S REPORTS ON INTERNAL CONTROL OVER FINANCIAL REPORTING

AGENCY: Securities and Exchange Commission.

ACTION: Concept Release; request for comment.

SUMMARY: The Commission is publishing this Concept Release to understand better the extent and nature of public interest in the development of additional guidance for management regarding its evaluation and assessment of internal control over financial reporting so that any guidance the Commission develops addresses the needs and concerns of public companies, consistent with the protection of investors.

DATES: Comments should be submitted on or before [insert date 60 days after the date of publication in the Federal Register].

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic comments:

- Use the Commission's Internet comment form (http://www.sec.gov/rules/concept.shtml); or
- Send an e-mail to rule-comments@sec.gov. Please include File Number S7-11-06 on the subject line; or
- Use the Federal eRulemaking Portal (http://www.regulations.gov). Follow the instructions for submitting comments.

Paper comments:

- Send paper submissions in triplicate to Nancy M. Morris, Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-1090.

All submissions should refer to File Number S7-11-06. This file number should be included on the subject line if e-mail is used. To help us process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's Internet Web site (http://www.sec.gov/rules/concept.shtml). Comments also are available for public inspection and copying in the Commission's Public Reference Room, 100 F Street, NE, Washington, DC 20549. All comments received will be posted without change; we do not edit personal identifying information from submissions. You should submit only information that you wish to make available publicly.

FOR FURTHER INFORMATION CONTACT: Lillian Brown, Division of Corporation Finance or Michael Gaynor, Office of Chief Accountant, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549.

SUPPLEMENTAL INFORMATION:

Table of Contents

I. BACKGROUND

Section 404(a) of the Sarbanes-Oxley Act of 2002[1] directed the Commission to prescribe rules that require each annual report that a company, other than a registered investment company, files pursuant to Section 13(a) or 15(d)[2] of the Securities Exchange Act of 1934[3] to contain an internal control report: (1) stating management's responsibilities for establishing and maintaining adequate internal control structure and procedures for financial reporting; and (2) containing an assessment, as of the end of the company's most recent fiscal year, of the effectiveness of the company's internal controls and procedures for financial reporting. On June 5, 2003, the Commission adopted rules implementing Section 404 with regard to management's obligations to report on internal control over financial reporting.

Domestic reporting companies that meet the definition of "accelerated filer" under the Commission's rules were required to comply with the internal control reporting provisions for the first time in connection with their fiscal years ending on or after November 15, 2004. Foreign private issuers that meet the definition of accelerated filer must comply with those provisions for their first fiscal year ending on or after July 15, 2006. On September 22, 2005, the Commission postponed the compliance date for domestic and foreign non-accelerated filers until their first fiscal years ending on or after July 15, 2007.

On May 17, 2006, the Commission announced its intent to issue an additional postponement for compliance for non-accelerated filers. As announced in that press

[1] 75 U.S.C. 7262.

[2] 15 U.S.C. 78m(a) or 78o(d).

[3] 15 U.S.C. 78a et. seq.

release, the Commission expects to propose an additional extension of the dates for complying with our internal control over financial reporting requirements for companies that are non-accelerated filers, including foreign private issuers that are non-accelerated filers.

Section 404(b) of Sarbanes-Oxley, as well as the Commission's rules adopted to implement the requirements of that section of the Act, require every registered public accounting firm that prepares or issues a financial statement audit report for a company also to attest to and report on management's assessment of internal control over financial reporting, in accordance with standards to be established by the Public Company Accounting Oversight Board (PCAOB). On June 17, 2004, the Commission issued an order approving PCAOB Auditing Standard No. 2, "An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of the Financial Statements" (AS No. 2), which established the requirements that apply when an independent auditor is engaged to provide an attestation and report on management's assessment of the effectiveness of a company's internal control over financial reporting.

In the release adopting the Commission's rules implementing Section 404, we expressed our belief that the methods of conducting assessments of internal control over financial reporting will, and should, vary from company to company.[4] We continue to believe that it is impractical to prescribe a single methodology that meets the needs of every company. However, we have received feedback that the limited nature and extent of detailed management guidance available has resulted in management's implementation and assessment efforts being driven largely by AS No. 2. Therefore, we are planning to

[4] See SEC Final Rule: Management's Reports on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Release No. 34-47986 (June 5, 2003) [68 FR 36636] (hereinafter "Adopting Release") at Section II.B.3.d.

issue additional guidance to assist management in its performance of its assessment of internal control over financial reporting. On May 17, 2006, we announced, among other things, our intent to issue this Concept Release seeking comment on a variety of issues that might be the subject of Commission guidance for management. As we noted in that announcement, in writing any guidance we will be sensitive to the fact that many companies already have invested substantial resources to establish and document programs and procedures to perform their assessments over the last few years.

II. INTRODUCTION

Based on the cumulative feedback received since the adoption of the rules implementing Section 404, the Commission deems it necessary to issue additional guidance for management on its assessment of the effectiveness of internal control over financial reporting. We currently anticipate that the guidance issued would be in the form of a rule, which would address the topics that we have outlined in this Concept Release: risk and control identification, management's evaluation, and documentation requirements (each of these topics is addressed separately throughout the remainder of this document). Additionally, we anticipate that the rule would be written in such a manner that if companies followed the rule, they would be deemed to have complied with Rules 13a-15(c) and 15d-15(c) of the Exchange Act. Further, we anticipate any modifications to AS No. 2 would be consistent with the rule.

The Commission is publishing this Concept Release to solicit public comment on the provision of additional guidance to management of public companies that are subject to the SEC's rules related to management's assessment of internal control over financial reporting and, to assist the Commission so that any guidance it ultimately develops

addresses the needs and concerns of all public companies. We raise a series of questions throughout this release on assessing risks, identifying controls, evaluating effectiveness of internal control, and documenting the basis for the assessment. Through the questions in this Concept Release, we seek to elicit specific public comment on such matters including, but not limited to, the extent and nature of public interest in the development of additional management guidance, whether additional guidance would be useful for all reporting companies or just a subset of those companies, the particular subject areas that any additional guidance should address, and the extent of additional guidance that would be useful.

Since the Commission adopted rules in June 2003 to implement Section 404 of the Sarbanes-Oxley Act, companies and third parties have devoted considerable attention to the methods that management may use to assess the effectiveness of internal control over financial reporting. To date, many public companies have developed their own assessment procedures internally. Many also have retained consultants or purchased commercial software and other products to establish or improve their assessment procedures. When the Commission first adopted the internal control over financial reporting requirements, we emphasized two broad principles: (1) that the scope and process of the assessment must be based on procedures sufficient both to evaluate its design and to test its operating effectiveness;[5] and (2) that the assessment, including testing, must be supported by reasonable evidential matter.[6] We stated that it was important for each company to use its informed judgment about its own operations, risks, and processes in documenting and evaluating its controls. We continue to believe that

[5] See Adopting Release at Section II.B.3.d.

[6] See Adopting Release at Section II.B.3.d.

management must bring its own experience and informed judgment to bear in designing an assessment process that meets the needs of its company and that provides reasonable assurance as to whether the company's internal control over financial reporting is effective.

While we emphasized the concept of management flexibility in adopting our rules implementing Section 404, our rules do require management to base its assessment of a company's internal control on a suitable evaluation framework, in order to facilitate comparability between the assessment reports. It is important to note that our rules do not mandate the use of a particular framework, because multiple frameworks exist and others may be developed in the future. However, in the release adopting the Section 404 requirements, the Commission identified the Internal Control—Integrated Framework created and published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as an example of a suitable framework.[7, 8]

---

[7] See COSO, Internal Control-Integrated Framework (1992). In 1994, COSO published an addendum to the Reporting to External Parties volume of the COSO Report. The addendum discusses the issue of, and provides a vehicle for, expanding the scope of a public management report on internal control to address additional controls pertaining to safeguarding of assets. In 1996, COSO issued a supplement to its original framework to address the application of internal control over financial derivative activities.

The COSO framework is the result of an extensive study of internal control to establish a common definition of internal control that would serve the needs of companies, independent public accountants, legislators, and regulatory agencies, and to provide a broad framework of criteria against which companies could evaluate and improve their control systems. The COSO framework divides internal control into three broad objectives: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. Our rules relate only to reliability of financial reporting. Each of the objectives in the COSO framework is further broken down into five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring. Under the COSO framework, management is able to monitor, evaluate, and improve their control systems through the use of the five components.

[8] In that release, we also cited the Guidance on Assessing Control published by the Canadian Institute of Chartered Accountants and the Turnbull Report published by the Institute of Chartered Accountants in England & Wales as examples of other suitable frameworks that issuers could choose in evaluating the effectiveness of their internal control over financial reporting. We encourage companies to examine and select a framework that may be useful in their own circumstances and the further development of alternative frameworks.

While the COSO framework provides an integrated framework that identifies the components and objectives of internal control, it does not set forth detailed guidance as to the steps that management must follow in assessing the effectiveness of a company's internal control over financial reporting. We, therefore, distinguish between the COSO framework as an internal control framework and other forms of guidance that illustrate how to conduct an assessment of the effectiveness of internal control over financial reporting. Any additional management guidance that we may issue is not intended to replace or modify the COSO framework or any other suitable framework.

In determining the need for additional guidance to management on how to conduct its assessment, it is important to consider the steps that already have been taken by the Commission and others to provide guidance to companies and audit firms. The Commission held its first roundtable discussion about implementation of the internal control reporting provisions on April 13, 2005. The Commission held the 2005 roundtable to seek input to consider the impact of the Section 404 reporting requirements in view of the fact that the implementation of the requirements resulted in a major change for management and auditors. A broad range of interested parties, including representatives of managements and boards of domestic and foreign public companies, auditors, investors, legal counsel, and board members of the PCAOB, participated in the discussion. We also invited and received written submissions from the public regarding Section 404 in advance of the roundtable.

Feedback obtained from the 2005 roundtable indicated that the internal control reporting requirements had led to increased focus by management on internal control over financial reporting. However, the feedback also identified particular implementation

areas in need of further clarification to reduce unnecessary costs and burdens without jeopardizing the benefits of the new requirements.

In response to this feedback, the Commission and its staff issued guidance on May 16, 2005.[9] An overarching message of that guidance was that it is the responsibility of management, not the auditor, to determine the appropriate nature and form of internal controls for the company and to scope their evaluation procedures accordingly. Additionally, based on feedback received, a number of the implementation issues arose from an overly conservative application of the Commission rules and AS No 2, and the requirements of AS No. 2 itself, as well as questions regarding the appropriate role of the auditor. Accordingly, much of the guidance in the staff statement emphasized and clarified existing provisions of the rules and other Commission guidance relating to the exercise of professional judgment, the concept of reasonable assurance, and the permitted communications between management and auditors.

The staff's guidance addressed implementation issues in the following seven areas:

- The purpose of internal control over financial reporting;
- The concept of reasonable assurance, the importance of a top-down, risk-based approach, and scope of testing and assessment;
- Evaluating internal control deficiencies;

[9] Commission Statement on Implementation of Internal Control Reporting Requirements, Press Release No. 2005-74 (May 16, 2005) (hereinafter "May 2005 Commission Guidance"); Division of Corporation Finance and Office of Chief Accountant: Staff Statement on Management's Report on Internal Control Over Financial Reporting (May 16, 2005) (hereinafter "May 2005 Staff Guidance) available at SEC.gov/spotlight/soxcom/.htm.

Also on May 16, 2005, the PCAOB and its staff issued guidance to auditors on their audits under Auditing Standard No. 2. The PCAOB's guidance focused on areas in which the efficiency of the audit could be substantially improved. Topics included the importance of the integrated audit, the role of risk assessment throughout the process, the importance of taking a top-down approach, and auditors' use of the work of others.

- Disclosures about material weaknesses;
- Information technology issues;
- Communications with auditors; and
- Issues related to small businesses and foreign private issuers.

Overall, the May 16, 2005 guidance was well-received, and some commenters have indicated there has been some improvement in the effectiveness and efficiency of Section 404 compliance efforts. However, some constituents, especially smaller public companies, continue to request the provision of additional guidance. For example, in its Final Report to the Commission, issued on April 23, 2006, the Commission's Advisory Committee on Smaller Public Companies raised a number of concerns it perceived regarding the ability of smaller companies to comply cost-effectively with the requirements of Section 404. The Advisory Committee identified as an overarching concern the difference in how smaller and larger public companies operate. The Advisory Committee focused in particular on three characteristics: 1) the limited number of personnel in smaller companies constrains the companies' ability to segregate conflicting duties; 2) top management's wider span of control and more direct channels of communication increase the risk of management override; and 3) the dynamic and evolving nature of smaller companies limits their ability to maintain well-documented static business processes.[10]

The Advisory Committee suggests these characteristics create unique differences in how smaller companies achieve effective internal control over financial reporting that may not be adequately accommodated in AS No. 2 or other implementation guidance as

[10] Final Report of the Advisory Committee on Smaller Public Companies to the United States Securities and Exchange Commission (April 23, 2006) (hereinafter "Advisory Committee Report") at 35-36, available at SEC.gov/info/smallbus/acspc.shtml.

currently applied in practice.[11] In addition, the Advisory Committee noted serious cost ramifications for smaller public companies stemming from the cost of frequent documentation change and sustained review and testing for perceived compliance with Section 404.

The Advisory Committee's final report set forth several recommendations for the Commission to consider regarding the application of the Section 404 requirements to smaller public companies. The Advisory Committee recommended partial or complete exemptions for specified types of smaller public companies from the internal control reporting requirements under certain conditions, unless and until a framework is developed for assessing internal control over financial reporting that recognizes the characteristics and needs of those companies. The Advisory Committee also recommended, among other things, that COSO and the PCAOB provide additional guidance to help facilitate the design and assessment of internal control over financial reporting and make processes related to internal control more cost-effective.[12] In addition, some commenters on the Advisory Committee's exposure draft of its report suggested that the Commission reexamine the appropriate role of outside auditors in connection with the management assessment required by Section 404.[13]

Further, in April 2006, the U.S. Government Accountability Office issued a Report to the Committee on Small Business and Entrepreneurship, U.S. Senate, entitled Sarbanes-Oxley Act, Consideration of Key Principles Needed in Addressing Implementation for Smaller Public Companies, which recommends that in considering

[11] Advisory Committee Report at 37, available at SEC.gov/info/smallbus/acspc.shtml.
[12] Advisory Committee Report at 52, available at SEC.gov/info/smallbus/acspc.shtml.
[13] See, e.g., letter from BDO Seidman, LLP (April 3, 2006), available at SEC.gov/info/smallbus/acspc.shtml.

the concerns of the Advisory Committee, the Commission should assess the available guidance on management's assessment to determine whether it is sufficient or whether additional action is needed. The report indicates that management's implementation and assessment efforts were largely driven by AS No. 2, as guidance at a similar level of detail was not available for management's implementation and assessment process.[14] Further, the GAO report recommended that the Commission coordinate with the PCAOB to help ensure that the Section 404-related audit standards and guidance are consistent with any additional management guidance issued.[15]

On May 10, 2006, the Commission and PCAOB conducted a second Roundtable on Internal Control Reporting and Auditing Provisions to solicit feedback on accelerated filers' second year of compliance with the Section 404 requirements. Although some participants expressed reservations about changing the processes they have already implemented, a number of the participants expressed at the roundtable and in their written comments the view that additional guidance was needed.[16]

COSO plans to publish additional application guidance on its control framework in the near future.[17] This guidance is intended to assist the management of smaller companies in understanding and applying the COSO framework. It is expected that COSO's new guidance will outline principles fundamental to the five components of

[14] United States Government Accountability Office Report to the Committee on Small Business and Entrepreneurship, U.S. Senate: Sarbanes-Oxley Act: Consideration of Key Principles Needed in Addressing Implementation for Smaller Public Companies (April 2006) (hereinafter "GAO Report") at 52-53.

[15] GAO Report at 58.

[16] See transcript of Roundtable on Internal Control Reporting and Auditing Provisions, May 10, 2006, Panels 1, 2, 3, and 5; letter from The Institute of Internal Auditors (IIA) (May 1, 2006); letter from Institute of Management Accountants (IMA) (May 4, 2006); letter from Canadian Bankers Association (CBA) (April 28, 2006); letter from Deloitte & Touche LLP (May 1, 2006); letter from Ernst & Young LLP (May 1, 2006); letter from KPMG LLP (May 1, 2006); letter from PricewaterhouseCoopers LLP (May 1, 2006) and letter from Pfizer Inc. (May 1, 2006).

[17] See letter from Larry Rittenberg, COSO (May 16, 2006) [File Number 4-511].

internal control described in the COSO framework. The guidance will define each principle and describe the attributes of each, list a variety of approaches that smaller companies can use to apply the principles, and include examples of how smaller companies have applied the principles. As noted in the May 17, 2006 announcement, we anticipate that this guidance will help organizations of all sizes to better understand and apply the COSO framework as it relates to internal control over financial reporting.

We are issuing this Concept Release to understand better the extent of public interest in the development of additional guidance for management regarding its evaluation and assessment of internal control over financial reporting. As noted in our May 17, 2006 announcement, so that this guidance might be helpful to all companies, the Commission currently intends that any future guidance we issue will be scalable and responsive to individual circumstances. We also are interested in understanding what additional guidance accelerated filers would find helpful.[18]

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?

[18] We emphasize that the publication of this Concept Release does not reflect a general dissatisfaction by the Commission with the assessments accelerated filers have completed to date. Rather, we are issuing this Concept Release because we are committed to doing as much as we can to reduce any concerns about the nature and extent of assessment procedures that management must establish and maintain, to assist in making the requirements scalable for companies of all sizes and complexity, and to help companies evaluate internal control over financial reporting in a practical and cost-efficient manner.

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?
3. Should additional guidance be limited to articulation of broad principles or should it be more detailed?
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?
5. Would additional guidance in the format of a Commission rule be preferable to interpretive guidance? Why or why not?
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?
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?
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?

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)"[19] that should be incorporated into any guidance the Commission might issue?

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?

III. RISK AND CONTROL IDENTIFICATION

While companies have been required to establish and maintain internal accounting controls since the enactment of the Foreign Corrupt Practices Act in 1977,[20] Section 404 of the Sarbanes-Oxley Act re-emphasized the importance of the relationship between effective internal controls and reliable financial reporting. An integral element of establishing and maintaining effective internal control over financial reporting involves identifying risks to reliable financial reporting and designing appropriate internal controls

[19] Available at www.sec.gov/info/accountants/controlfaq1004.htm.

[20] Title I of Pub. L. No. 95-213. The FCPA required the Commission to adopt rules requiring public companies to make and keep accurate financial records, and to maintain a system of internal accounting controls. See Exchange Act Section 13(b).

that address the risks. The controls that management identifies as addressing risks to financial reporting include those that operate at a company level and are pervasive to many individual account balances and disclosures, as well as those that are specific to certain individual account balances or disclosures. Echoing the Commission's statement in its May 16, 2005 guidance that management must bring reasoned judgment to the process, the staff stated that management should use its cumulative knowledge, experience, and judgment (applying both qualitative and quantitative factors) in identifying these controls and designing the appropriate procedures for their documentation and testing.

Feedback that the Commission has received indicates that, in implementing the requirements of Section 404, many companies did not efficiently and effectively identify risks to reliable financial reporting and relevant internal control functions, ultimately leading to the identification, documentation, and testing of an excessive number of controls.[21] We are also skeptical of the large number of internal controls that some companies have identified, documented and tested. While there were likely numerous contributing factors to these implementation issues, one cause may have been the overly conservative application of AS No. 2 by auditors in the initial years.

The Commission also has heard that companies had difficulty in determining how controls related to the prevention of fraud should be included in their risk assessment.[22] However, as noted in the May 16, 2005 staff guidance, while no system of internal control can prevent or detect every instance of fraud, effective internal control over

[21] See transcript of Roundtable on Internal Control Reporting and Auditing Provisions, May 10, 2006, Panels 2 and 3; letter from Protiviti Inc. (April 28, 2006); letter from Computer Sciences Corporation (CSC) (April 28, 1006); and letter from IMA (May 4, 2006).

[22] See letter from QUALCOMM Inc. (April 27, 2006); and letter from Diane Allen, 3M (Allen) (April 28, 2006).

financial reporting can help companies deter fraudulent financial accounting practices or detect them earlier.

As noted above, the Advisory Committee observed that the distinct characteristics of smaller public companies affect the financial reporting risks and the controls needed to address them. For example, the significant risk of management override that arises from wider spans of control and more direct channels of communication may create an increased need for entity level controls and board oversight. Moreover, the difficulty in segregating duties and changing business processes may impact the implementation of internal controls at these companies.

We anticipate additional guidance in this area would cover a number of the implementation issues that have arisen during the first two years of compliance. Guidance issued in this area would address how management should determine the overall objectives for internal control over financial reporting and identify the related risks. In determining the objectives for internal control over financial reporting, the guidance would discuss how management might address company-level, financial statement account and disclosure level considerations, as well as fraud risks. Additionally, we anticipate that we would provide additional guidance on how management identifies the controls to address the recognized risks. This would include guidance on common issues that exist in identifying controls (e.g. materiality considerations, multi-location issues, concept of "key" controls).

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?

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?
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?
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?
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?
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?

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"[23] useful in assessing these risks and controls?

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?

IV. MANAGEMENT'S EVALUATION

As noted, the Commission's and the staff's May 16, 2005 guidance emphasized that management's assessment should be based on the particular risks of individual companies, and recommended a top-down, risk-based approach to determine the accounts and related processes that management should consider in its assessment. Therefore, management's judgments about the significance and complexity of the risk areas it has identified should form the basis not only for determining what controls to evaluate, but also for determining the nature, timing, and extent of its evaluation procedures. A risk-based evaluation can allow management to assess whether the company's internal control over financial reporting is effective at a "reasonable assurance" level.[24]

---

[23] Management Antifraud Programs and Controls: Guidance to Help Prevent and Deter Fraud, commissioned by the Fraud Task Force of the American Institute of Certified Public Accounting's Auditing Standards Board (2002), available at http://www.aicpa.org/download/members/div/auditstd/AU-00316.PDF.

[24] See Rules 13a-15(f) and 15d-15(f) of the Exchange Act.

One of the reasons cited most frequently by accelerated filers for the higher than anticipated costs in their first year of compliance with the Section 404 requirements is that too much work was done to test and document low-risk areas.[25] The Commission continues to hear that management has difficulty applying a top-down, risk-based approach in their individual assessments and some believe that compliance costs are, and may continue to be, higher than necessary.[26]

The Commission's rules require that management's assessment be "as of" the company's fiscal year end, but the rules do not preclude management from obtaining evidence to support its assessment through cumulative knowledge it acquires throughout the year and in prior years. In fact, management's daily interactions with its internal controls may provide it with an enhanced ability to make informed judgments regarding the areas that present the greatest risk to the reliability of the financial statements, as well as how to evaluate the relevant controls. We have heard anecdotal evidence that, in some cases, management may have unnecessarily tested controls using separate evaluation-type testing in connection with its annual assessment, rather than relying on its ongoing monitoring activities, which may include, for example, cumulative knowledge and experiences from its daily interactions with controls.

In addition to testing, another key part of management's assessment process is the evaluation of control deficiencies it discovers in the process of its evaluation. Paramount to evaluating the significance of an individual control deficiency, or combination of

[25] See transcript of Roundtable on Internal Control Reporting and Auditing Provisions, May 10, 2006, Panels 2 and 3; letter from Watson Wyatt Worldwide (March 31, 2006); letter from QUALCOMM Inc. (April 27, 2006); and letter from Association for Financial Professionals (May 1, 2006).

[26] See transcript of Roundtable on Internal Control Reporting and Auditing Provisions, May 10, 2006, Panels 1 and 2; letter from Pfizer Inc. (May 1, 2006); letter from Sotheby's Holdings, Inc. (May 1, 2006); and letter from U.S. Chamber of Commerce (May 3, 2006).

control deficiencies, is to have a comprehensive understanding of the nature of the deficiency, its cause, the relevant financial statement assertion the control was designed to support, its effect on the broader control environment, and whether effective compensating controls exist.[27] Management must exercise judgment in a reasonable manner in the evaluation of deficiencies in internal control, considering both quantitative and qualitative factors.[28]

As noted above, the Advisory Committee observed that the distinct characteristics of smaller public companies affect the assessment of financial reporting risks and the controls implemented to address them. These characteristics may also affect how those companies evaluate their internal control.

Another area where the Commission continues to hear that companies are having difficulty in completing their assessment of internal control over financial reporting involves the impact of information technology (IT) processes. For example, some commenters have expressed concerns over the extent to which IT processes should be included in the scope of their assessment.[29] As the staff's May 16, 2005 staff guidance indicates, Section 404 is not a one-size-fits-all approach to assessing controls, and for that reason, while we believe that controls not related to internal control over financial reporting should not be included in the assessment, providing a list of the exact general IT controls that should be included in an assessment may not be practical. Given that

[27] See May 2005 Staff Guidance at B.

[28] Id.

[29] See transcript of Roundtable on Internal Control Reporting and Auditing Provisions, May 10, 2006, Panels 2 and 3; letter from IIA (May 1, 2006); letter from CSC (April 28, 2006); letter from Allen (April 28, 2006); letter from WPS Resources Corp. (May 5, 2006); and letter from R.G. Scott & Associates, LLC (April 8, 2006).

fact, we would like to explore whether there are specific areas related to IT where additional guidance could be provided.

Based on the cumulative feedback received, we believe that guidance on management's evaluation process and revisions to AS No. 2 may help reduce or eliminate the excessive testing of internal controls by improving the focus on risk and better use of entity-level controls. We anticipate that the guidance would cover topics such as the overall objective of evaluation procedures; methods or approaches available to management to gather evidence to support its assessment (i.e. on-going monitoring, benchmarking, and updating prior evaluations); and factors that management should consider in determining the nature, timing and extent of its evaluation procedures. This guidance would address whether and how entity-level controls may adequately address risk at the financial statement and disclosure level and considerations as to the extent information technology general controls are included in the scope of management's assessment. Further, we anticipate the guidance would cover considerations of management in determining the severity of an identified control deficiency.

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.
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?

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?
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?
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?
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?
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.

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.

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?

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

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

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?

V. DOCUMENTATION TO SUPPORT THE ASSESSMENT

Developing and maintaining an appropriate amount of evidential matter is an inherent element of effective internal control.[30] This evidential matter should provide

[30] Section 13(b)(2)(A) of the Exchange Act requires companies to "make and keep books, records, and accounts, which in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer." We have previously stated, as a matter of policy, that under Section 13(b)(2) "every public company needs to establish and maintain records of sufficient accuracy to meet adequately four interrelated objectives: appropriate reflection of corporate transactions and the disposition of assets; effective administration of other facets of the issuer's internal control system; preparation of its financial statements in accordance with generally accepted accounting principles; and proper auditing." Statement

reasonable support for the assessment of whether controls are designed to prevent or detect material misstatements or omissions; for the conclusion that tests to assess the effectiveness of internal control were appropriately planned and performed; and for the conclusion that the results of such tests were appropriately considered in management's conclusion about effectiveness.[31] Further, public accounting firms that attest to, and report on, management's assessment of the effectiveness of the company's internal control over financial reporting may review evidential matter supporting management's assessment.[32]

Feedback that the Commission received in connection with its 2005 Roundtable and other feedback on the first year of compliance indicates that, in implementing the requirements of Section 404 for the first time, many companies approached risk and control identification more formally than they may have historically and, consequently, companies may have incurred significant documentation costs.[33] This documentation consisted of, among other things, detailed process maps describing controls over initiating, recording, processing and reconciling account balances, classes of transactions, and disclosures included in the financial statements. Many companies also have indicated that in their initial implementation of Section 404, too many controls were

---

of Policy Regarding the Foreign Corrupt Practices Act of 1977, Release No. 34-17500 (Jan. 29, 1981) [46 FR 11544].

[31] Instruction 1 to Item 308 of Regulations S-K and S-B, Instruction 1 to Item 15 of Form 20-F and Instruction 1 to paragraphs (b), (c), (d), and (e) of General Instruction B.6 to Form 40-F provide that "the Registrant must maintain evidential matter, including documentation, to provide reasonable support for management's assessment of the effectiveness of the registrant's internal control over financial reporting."

[32] AS No. 2 sets forth the criteria auditors should use when evaluating whether management's documentation provides reasonable support for its assessment of internal control over financial reporting. See ¶¶42-46 of PCAOB Auditing Standard No. 2, An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements.

[33] See transcript of Roundtable on Implementation of Internal Control Reporting Provisions, April 13, 2005; letter from Mortgage Bankers Association (February 25, 2005); letter from Paula Jourde (March 4, 2005); letter from White Mountains Insurance Group (March 29, 2005); and letter from Intel Corporation (March 31, 2005).

identified, which resulted in excessive documentation.[34] Frequently, this excessive documentation was blamed, at least in part, on the auditors and their application of AS No. 2. Further, we have anecdotally heard that this documentation, in many cases, substantially exceeded that normally produced by financial institutions under the Federal Deposit Insurance Corporation Improvement Act of 1991,[35] notwithstanding substantially similar statutory language to that found in Section 404.

In its report, the Advisory Committee suggested that smaller public companies have unique characteristics and needs for flexibility that make the documentation elements of Section 404 particularly burdensome for those companies. In its opinion, the Section 404 internal control reporting requirements as currently applied in practice might impose a lack of flexibility on smaller public companies that would put them at a competitive disadvantage. We have also heard that excessive documentation demands might impose extra or particularly burdensome costs on smaller public companies.

The Commission anticipates that management would benefit from additional guidance on the appropriate and required levels of documentation to support their assertion on the effectiveness of internal control over financial reporting. Topics addressed might include clarifying the overall objectives of the documentation, including

[34] See transcript of Roundtable on Internal Control Reporting and Auditing Provisions, May 10, 2006, Panels 1 and 2; letter from IIA (May 1, 2006); letter from America's Community Bankers (May 1, 2006); letter from Stephan Stephanov (March 27, 2006); and letter from Institute of Chartered Accountants in England and Wales (March 28, 2006).

[35] 12 U.S.C. 1831m. Section 112 of the Federal Deposit Insurance Corporation Improvement Act of 1991 added Section 36, "Independent Annual Audits of Insured Depository Institutions," to the Federal Deposit Insurance Act. Section 36 required the Federal Deposit Insurance Corporation, in consultation with appropriate federal banking agencies, to promulgate regulations requiring each insured depository institution with at least $150 million in total assets, as of the beginning of its fiscal year, to have an annual independent audit of its financial statements performed in accordance with generally accepted auditing standards, and to provide a management report and an independent public accountant's attestation concerning both the effectiveness of the institution's internal control structure and procedures for financial reporting and its compliance with designated safety and soundness laws.

factors that might influence documentation requirements and other common documentation concerns (e.g. updating of previously created documentation or how to address controls for which operation does not result in documented evidence). We also anticipate that guidance might be helpful in addressing the flexibility and cost containment needs of smaller public companies in particular.

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?
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?
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?
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?

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?

VI. SOLICITATION OF ADDITIONAL COMMENTS

In addition to the areas for comment identified above, we are interested in any other issues that commenters may wish to address relating to companies' compliance with the SEC's rules related to management's assessment of internal control over financial reporting. For example, we are interested in whether commenters believe that there are additional topics not addressed in this Concept Release for which guidance would be useful. We also invite commenters to provide to us descriptions of, or actual process plans, that they have utilized or created for portions or all of management's assessment. Please be as specific as possible in your discussion and analysis of any additional issues. Where possible, please provide empirical data or observations to support or illustrate your comments.

By the Commission.

Jill M. Peterson
Assistant Secretary

Dated: July 11, 2006