INSTITUT
DER
WIRTSCHAFTSPRÜFER

IDW

September 18, 2006

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

USA

By E-Mail: rule-comments@sec.gov

Dear Ms. Morris:

Re: File No. S7-11-06

IDW Comments on SEC Concept Release Concerning Management's Reports on Internal Control Over Financial Reporting

We would like to thank you for the opportunity to comment on the SEC Concept Release Concerning Management's Reports on Internal Control Over Financial Reporting (hereinafter referred to as the "Concept Release").

The IDW seeks to comment on the Concept Release because any changes to the requirements in relation to management reports on internal controls over financial reporting pursuant to the Sarbanes-Oxley Act of 2002 (SOX) will also have an impact on the requirements for auditors to audit management's assertion in relation to internal control and the audit of internal control as required by the SOX. Furthermore, such changes may also influence auditing standards on internal control on a worldwide basis.

Institut der Wirtschaftsprüfer
in Deutschland e.V.
Tersteegenstr. 14
40474 Düsseldorf
Postfach 32 05 80
40420 Düsseldorf

Telefonzentrale 0211 / 45 61-0
Fax Geschäftsleitung 0211 / 4 54 10 97
Fax Fachabteilung 0211 / 45 61-233
Fax Bibliothek 0211 / 45 61-204
Internet www.idw.de
E-Mail info@idw.de

Geschäftsführender Vorstand:
Prof. Dr. Klaus-Peter Naumann,
WP StB, Sprecher des Vorstands
Dipl.-Kfm. Klaus-Peter Feld, WP StB CPA
Dr. Wolfgang Schaum, WP StB

Bankverbindung:
Deutsche Bank AG
Düsseldorf
BLZ 300 700 10
Kto.-Nr. 7480 213

We had previously written to the SEC on the issue of the audit of internal control in relation to Release No. 34-49544 in a letter dated May 17, 2004 prior to the SEC's approval of 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". We had also written directly to the PCAOB commenting on the draft of that standard in a letter dated November 21, 2003. A number of the issues we raised in these letters were discussed during the round table discussion on second year experiences with internal control reporting and auditing provisions held on May 10, 2006, because they had been specifically identified as having led to certain problems and are therefore being addressed in this Concept Release. We therefore refer to our previous letters and would, in addition, like to address issues that may result in amendments to AS-2.

In this letter, we would first like to raise matters of a general nature, before addressing specific matters and our responses to those questions raised in the concept release to which we are able to respond, in particular as to their impact on the audit function. The latter we have included in Appendix 1. Questions to which we are not in a position to respond because they may not be directly relevant to us are marked "not applicable" in the response.

General matters

Support for the issuance of guidance for management

Management is required by Section 404 of the SOX to include, within the issuer's annual report, an internal control report containing "an assessment…of the effectiveness of the internal control structure and procedures of the issuer for financial reporting". We welcome and are supportive of the SEC's intention to provide guidance to management on its reports on internal control over financial reporting pursuant to the SOX because, as we had noted in our previous comment letter dated May 17, 2004, it would be an untenable situation if AS-2 applied only to auditors and not to management, so that audits of internal controls were subject to more stringent criteria than those that apply to the design, implementation and maintenance of internal control by management and to management's assertion thereon. Hence, in conducting their audits, auditors applied AS-2 in determining whether the internal controls established by management are effective, which by default drove management into applying AS-2, even though it is an auditing standard, rather than a direct requirement for

SEC registrants. We had pointed this out in our comment letter to the SEC.[1] Consequently, we consider it appropriate that rules and guidance be issued on management's design, implementation, and maintenance of internal control over financial reporting and on management's assertion with respect to such internal control.

However, we would like to emphasize that there are necessarily certain fundamental similarities between the assessment management is obligated to carry out and the auditor's independent examination of internal controls, which must be reflected in any such guidance. In particular, the stringency of the rules and guidance in relation to internal control and reports thereon by management must be at least as great as that for audits of these controls, or auditors would be accepting greater responsibility for management's internal controls than management is, which would result in an inappropriate reversal of roles between management and the auditors. This also implies that the scope (nature and extent) of management's assessment of internal control must be at least the same as, or greater than, the auditor's examination of that assertion and of internal control. In particular, management needs to prepare documentation to support its assessment in at least as much detail as that required of the auditor pursuant to the PCAOB's Auditing Standard No. 3 (AS-3).

With the exception of the matters mentioned below, we believe that the guidance contained in the additional SEC and PCAOB pronouncements[2] issued in May 2005 appear to have given useful guidance to SEC Registrants and auditors, respectively,

---

[1] Extract from page 2 of our letter dated May 17, 2004 "… we believe that the Rule as currently proposed by the PCAOB appears to be inconsistent with the Securities and Exchange Act of 1934, and either sets requirements for management in relation to internal control (which we believe may be beyond the mandate of the PCAOB) or imposes responsibilities upon auditors in relation to control that exceed those of management (which we surmise may be incongruous with the relative roles of management and the auditors)." Extract from page 4 of our letter dated May 17, 2004 "… relating reasonable assurance just below absolute assurance or to a remote likelihood of a risk of material misstatement is fundamentally misleading. Both preparers and auditors face making many decisions that can only be made on the basis of what the legal profession terms "the preponderance of the evidence" or "clear and convincing evidence" as opposed to "beyond and reasonable doubt" or even a "remote likelihood of being wrong". Consequently, we believe that the application of the test "remote likelihood of a material misstatement" is effectively inconsistent with the "reasonability test" in relation to "prudent officials" applied in the SEA."

[2] Commission Statement on Implementation of Internal Control Reporting Requirements, Staff Statement on Management's Report on Internal Control over Financial Reporting, PCAOB Policy Statement regarding Implementation of AS-2 and PCAOB Staff Questions and Answers Auditing Internal Control over Financial Reporting

on their reporting in relation to internal control. In our view, the SEC pronouncements helped clarify a number of important issues, and we would certainly support aspects of the additional SEC guidance being included in rules and guidance for SEC Registrants, but some of the guidance may need revision, as we note in our response to question 9. Furthermore, we would encourage the PCAOB to consider whether our comments in relation to this Concept Release may be of benefit in any revision of AS-2, particularly if changes are made to the rules and guidance issued by the SEC for management.

Form of guidance

We believe that guidance will be most useful if it is based on broad principles and criteria, rather than in the form of detailed rules, because no set of detailed rules can apply to the varied business and financial reporting situations that exist among the wide range of businesses that SEC Registrants operate. Consequently, any rules or guidance issued by the SEC on management reports on internal controls over financial reporting need to be at a high level.

Specific Matters: Definitions of Key Terms Used

Reasonable assurance

In our previous comment letter to the SEC[3] we had commented on discrepancies between the definition of reasonable assurance set forth in the Securities and Exchange Act of 1934 applicable to management and AS-2's discussion of the concept of reasonable assurance applicable to the auditor. While the additional guidance in the Commission Statement on Implementation of Internal Control Reporting Requirements together with the Staff Statement on Management's Report on Internal Control over Financial Reporting alleviated this discrepancy, the additional guidance did so not by amelioration of the deficiencies in AS-2, but rather by extending those

---

[3] Please refer to the comments on pages 2 through 5 of our letter dated May 17, 2004, in particular "Our first concern is that the PCAOB definition of reasonable assurance (a remote likelihood that material misstatements will not be prevented or detected on a timely basis; a high, but not absolute, level of assurance) appears to be inconsistent with the definition of reasonable assurance in the Securities and Exchange Act of 1934 (SEA) unless, by implication, one accepts the contention that prudent officials are *always* capable of reducing the likelihood of a material misstatement not being prevented or detected on a timely basis by means of controls to a *remote* level. To use more legalistic terminology, the PCAOB definition appears to contend that prudent officials are *always* able to use controls to obtain a burden of persuasion equivalent to a "*remote* likelihood of being wrong"."

deficiencies to the guidance for management. We are particularly concerned that AS-2.17 uses the term “remote likelihood” in connection with “high” within the discussion of reasonable assurance. As we noted in our comment letter, we firmly believe that the use of either of these terms is inappropriate since most of the decisions that preparers and auditors make are not susceptible to Bayesian analysis and often involve decisions where the weight of the evidence is almost evenly distributed between the alternatives. We refer to our letter dated May 17, 2004 for a further discussion of this issue and would like to reaffirm our opinion that this wording should be amended as suggested in that letter.

Material weakness and significant deficiency

The roundtable discussions held on May 10, 2006 reveal that the definitions of “material weakness” and “significant deficiency” in AS-2 and their interaction with restatements have proven problematical. In this context, we would also like to refer to our letter dated May 17, 2004, in which we had discussed certain aspects of the definitions. In particular, we voiced our concern that the wording of the definitions may lead to situations where management or the auditor (or both) are blamed for situations beyond their control, stemming from the definition of reasonable assurance as a “remote likelihood” of risk. Again we refer to our previous comment letter.

We hope you find our comments helpful and would be pleased to be of assistance to you if you have any questions about these comments.

Yours very truly,

Klaus-Peter Feld
Executive Director

Wolfgang P. Böhm
Director, International Affairs

494/541/538

Appendices

Appendix 1

IDW responses to questions raised in the concept release

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?*

As noted above in our general comments, we support the SEC's proposal to issue guidance to management on how to evaluate the effectiveness of a company's internal control over financial reporting and report thereon. This type of guidance should be based on principles and criteria applicable to all companies, rather than tailored to specific types of entity. The limitation of such guidance is that it must be at a high level, for detailed guidance cannot be applicable to all kinds of companies.

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?*

We have no issues.

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

It would be more appropriate for guidance to be based on broad principles and criteria, since it would then be more likely to be capable of application by all types of issuers than would detailed rules.

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?*

As noted in our letter, the concept of reasonable assurance as it relates to the auditor and to management needs to be improved by being brought into line with reality. We also refer to our previous letter to the PCAOB, in which we have argued the need for guidance on effectiveness criteria and for further guidance on IT related controls.

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

To the extent that AS-2 retains detailed guidance as rules, we believe that management guidance should likewise include such a detailed level of guidance as rules. However, we would prefer the guidance for management to be at a high, less detailed level and then for AS-2 to be "condensed" to match this guidance. In our view, much of the guidance ought to be explanatory and so it would not be appropriate for this to be included within a rule. This would not preclude a few additional rules from being adopted, as long as they are at a very high level.

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?*

Not applicable.

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 believe that guidance will be treated de facto as a rule unless it is explanatory – rather than mandatory – in nature. For this reason, we would like to suggest that guidance be based on principles and criteria; rules, if any, should be at a very high level.

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?*

It appears to us that the majority of companies who have completed an assessment selected the COSO framework rather than one of the other frameworks available because AS-2 was based on the COSO framework. In order to remedy this situation, the PCAOB would probably have to amend AS-2 to be framework neutral.

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?*

Please refer to Appendix 2.

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?*

Unless Section 404 (a) or (b), or both, are changed, we do not believe that there can be any significant change in the role of auditors in relation to their attestation of management's assessment or their attestation of internal control. In any case, the nature and extent of management's assessment must be at least equal to that of the external auditor's examination because both are required to obtain reasonable assurance and any other constellation would reverse the roles of management and the auditor.

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?*

Without presupposing what guidance management believes it needs to implement a top-down risk-based approach, management guidance on these aspects should be the same as that applying to auditors.

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?*

We are convinced that identification of controls that address risks of material misstatement, as well as the risk assessment, is driven by the actual and required contents of the financial statements of a particular entity and the nature of its business and accounting processes. We therefore believe it would be difficult to develop additional guidance that applies to all entities.

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?*

See our answer to question 12.

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?*

Not applicable.

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?*

The existence of effective entity level controls has an impact on risk assessment, and may mean that it is appropriate for management to reduce the extent of tests of detail in certain areas; however, management cannot reasonably replace tests of detail at the significant account and transaction level entirely. The issues do not differ according to the size of the issuer, as the risk assessment will vary between individual entities. Therefore, we do not believe that guidance can be given to suit the circumstances of every kind of entity.

It is essential that any guidance for management be the same guidance as that for the auditor.

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?*

Such guidance would be useful, in particular in regard to qualitative factors. We do not believe that quantitative factors can be useful. It is essential that management be given the same guidance as the auditor. Guidance should be based on principles and criteria, so as to be capable of application to all sizes of issuers. Since the likelihood of error is not susceptible to Bayesian analysis, we suggest that instead one speaks of reducing the risk of material misstatement to an acceptably low level.

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?*

Fraud controls are an area in which capital market participants are likely to have a specific interest, but such controls may be largely ineffective, particularly in relation to potential management fraud. It is essential that management be given the same guidance as the auditor. Guidance should be based on principles and criteria, so as to be capable of application to all sizes of issuers. For this reason, we believe that it will be difficult to provide other than high-level guidance applicable to all entities.

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 we pointed out in our answer to question 12, it is difficult to provide detailed guidance on risk assessment applicable to all entities other than at a high level, since the risk assessment is driven by the actual and required contents of the financial statements of a particular entity and the nature of its business and accounting processes. In any case, the guidance provided to management cannot be different to that provided to the auditor.

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.*

Please refer to our response to question 18.

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?*

Please refer to our response to question 18.

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?*

Please refer to our response to question 18.

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?*

Please refer to our response to question 18.

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?*

Please refer to our response to question 18.

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?*

Please refer to our response to question 18.

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.*

Please refer to the specific matters addressed in our letter.

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.*

Yes because this would ensure such circumstances are addressed in a more uniform fashion between different companies and different auditors.

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?*

Yes, to ensure such circumstances are addressed in a more uniform fashion between different companies and different auditors.

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)?*

Not applicable.

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?*

We believe that such guidance should clearly state that only those IT general controls that can be demonstrated not to be at all related to financial reporting may be excluded. This is seldom likely to be the case. In addition, it may be necessary to specifically state that general controls relating, for example, to changes to existing financial reporting systems, or the introduction of new financial reporting systems, etc. will always be subject to assessment.

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?*

Not applicable.

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?*

Management's documentation should incorporate at least the same degree of detail and be of the same extent as that needed by the auditor for purposes of the audit.

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?*

See our response to question 31.

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?*

See our response to question 31.

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

Yes, guidance as to both is needed. Documentation requirements relating to controls will be broadly similar, irrespective of whether related to IT or "other" controls. Otherwise, see our response to question 31.

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?*

Not applicable.

Appendix 2

Response to question No. 9

We agree with much of the guidance given in the SEC pronouncements issued in May 2005, and believe that management would benefit from guidance based on principles and criteria reflecting the following extracts from these pronouncements. We have highlighted in greay those areas with which we have concerns by annotating them in gray accordingly.

Extracts, without accompanying footnotes, from the Commission Statement on Implementation of Internal Control Reporting Requirements that could be reproduced in guidance material for management

An overarching principle of this guidance is the responsibility of management to determine the form and level of controls appropriate for each company and to scope their assessment and the testing accordingly. Registered public accounting firms should recognize that there is a zone of reasonable conduct by companies that should be recognized as acceptable in the implementation of Section 404

Both management and external auditors must bring reasoned judgment and a top-down, risk-based approach to the 404 compliance process. A one-size fits all, bottom-up, check-the-box approach that treats all controls equally is less likely to improve internal controls and financial reporting than reasoned, good faith exercise of professional judgment focused on reasonable, as opposed to absolute, assurance.[Note: This may cause confusion, as the reference to absolute assurance appears to imply that reasonable assurance is high assurance. Consequently, we suggest deleting the phrase “as opposed to absolute”.]

Internal controls over financial reporting should reflect the nature and size of the company to which they relate. Particular attention should be paid to making sure that implementation of Section 404 is appropriately tailored to the operations of smaller companies. Again, this is an area where reasoned judgment and a risk-based approach must be brought to bear.

We encourage frequent and frank dialogue among management, auditors and audit committees with the goal of improving internal controls and the financial reports upon which investors rely. Management of all companies - large and small - should not fear that a discussion of internal controls with, or a request for assistance or clarification from, the auditor will, itself, be deemed a deficiency in internal control. Moreover, as long as management determines the accounting to be used and does not rely on the auditor to design or implement the controls, we do not believe that the auditor's providing advice

or assistance, in itself, constitutes a violation of our independence rules. Both common sense and sound policy dictate that communications must be ongoing and open in order to create the best environment for producing high quality financial reporting and auditing; communications must not be so restricted or formalized that their value is lost.

Extracts from the Staff Statement on Management's Report on Internal Control Over Financial Reporting that could be reproduced in guidance material for management

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 [Note: this should be amended to read “free of material misstatement”]. 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 [Note: Please refer to our accompanying letter in relation to this term. We prefer the phrase “lead to a greater than acceptably low level of risk of”.] 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.

The establishment and maintenance of internal accounting controls has been required of public companies since the enactment of the Foreign Corrupt Practices Act of 1977 (FCPA). The significance of Section 404 of the Act is that it re-emphasizes the important relationship between the maintenance of effective internal control over financial reporting and the preparation of reliable financial statements. Effective internal control over financial reporting can also help companies deter fraudulent financial accounting practices or detect them earlier and perhaps reduce their adverse effects. However, due to their inherent limitations, internal controls cannot prevent or detect every instance of fraud. Controls are susceptible to manipulation, especially in instances of fraud caused by the collusion of two or more people including senior management. Nonetheless, that limitation does not undercut the need for Section 404 and the improvements it has engendered and will continue to engender.

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.

Reasonable Assurance, Risk-based Approach and Scope of Testing and Assessment

The Concept of Reasonable Assurance

Management is required to assess whether the company's internal control over financial reporting is effective in providing reasonable assurance regarding the reliability of financial reporting. Management is not required by Section 404 of the Act to assess other internal controls. Further, while "reasonable assurance" is a high level of assurance, it does not mean absolute assurance [Note: As mentioned above we believe it is misleading to refer to reasonable assurance as a high level of assurance. Furthermore it is essential that AS-2 clarify that management's reasonable assurance should not differ from the auditor's reasonable assurance. We would prefer this sentence to be deleted; a replacement definition is not necessary since it is already provided below in relation to prudent officials ".]. As noted earlier, internal control over financial reporting cannot prevent or detect all errors, misstatements, or fraud. Rather, the "reasonable assurance" referred to in the Commission's implementing rules relates back to similar language in the FCPA. Exchange Act Section 13(b)(7) defines "reasonable assurance" and "reasonable detail" as "such level of detail and degree of assurance as would satisfy prudent officials in the conduct of their own affairs. The Commission has long held that "reasonableness" is not an "absolute standard of exactitude for corporate records."

In addition, the staff recognizes that while "reasonableness" is an objective standard, there is a range of judgments that an issuer might make as to what is "reasonable" in implementing Section 404 and the Commission's rules. Thus, the terms "reasonable," "reasonably" and "reasonableness" in the context of Section 404 implementation do not imply a single conclusion or methodology, but encompass the full range of potential conduct, conclusions or methodologies upon which an issuer may reasonably base its decisions. Different conduct, conclusions and methodologies by different issuers in a given situation do not by themselves mean that implementation by any of those issuers is unreasonable. This also suggests that registered public accounting firms should recognize that there is a zone of reasonable conduct by issuers that should be recognized as acceptable in the implementation of Section 404. While that zone is not unlimited, the staff expects that it will be rare when there is only one acceptable choice in implementing Section 404 in any given situation.

The desired approach should devote resources to the areas of greatest risk and avoid giving all significant accounts and related controls equal attention without regard to risk.

The assessment of internal control over financial reporting will be more effective if it focuses on controls related to those processes and classes of transactions for financial statement accounts and disclosures that are most likely to have a material impact on the company's financial statements. Employing such a top-down approach requires that management apply in a reasonable manner its cumulative knowledge, experience and judgment to identify the areas of the financial statements that present significant risk that the financial statements could be materially misstated and then proceed to identify relevant controls and design appropriate procedures for documentation and testing of those controls. For instance, the application of judgment by management and the auditor will typically impact the nature, extent and timing of control testing such that the level of

testing performed for a low risk account will likely be different than it will be for a high risk account. In performing these steps, management and auditors should keep the "reasonable assurance" standard in mind.[Note: Therefore, as we note in our accompanying letter, the definition of reasonable assurance applicable to management and to the auditor has to be the same: this ought to be stated explicitly.]

Scope of Assessment

As previously discussed, the staff believes that management should use a top-down, risk-based approach in determining significant accounts and related significant processes and relevant assertions. The natural result of such an approach is that management would devote greater attention and resources to the areas of greater risk.

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, as discussed previously. 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.

Once the significant accounts and their related significant processes are identified, management must focus on the controls to be tested that are relevant to those processes. We believe that some of the large numbers of controls identified for testing during the first year of implementation may, in part, represent individual steps within what may constitute a broader control. In performing future assessments, management may wish to step back from focusing on the detail to consider whether combinations of controls previously identified individually constitute the actual control that contributes to financial statement assurance. Rather than identifying, documenting, and testing each individual step involved in a broader control definition, management's focus should be on the objective of controls, and testing the effectiveness of the combination of detailed steps that meet the broader control objective. Management may determine that not every individual step comprising a control is required to be tested in order to determine that the overall control is operating effectively.

The staff also expects that through the natural learning process management will achieve efficiencies as they complete future assessments of internal control. For example, as discussed above, management's knowledge of the prior year's assessment results will impact its current year risk-based analysis of the significant accounts and the related required documentation and testing that may be necessary. Management may determine that certain controls require more extensive testing, while other controls require little testing in a given year. Additionally, in reaching its conclusion of reasonable assurance, management may find it appropriate to adjust the nature, extent and timing of testing from year to year - in some years delving deeply into selected internal control areas while performing less extensive testing in other areas and changing that focus from year to year.

The staff believes that efficient and effective assessments depend on internal audit and other company personnel and external auditors who are "on the ground" closest to the assessment. It is at that level where the unique circumstances of any particular situation can best be evaluated. It is thus critically important that company and auditor personnel have the requisite skills, training, and judgment to make reasonable assessments. The staff believes that the ability to make such assessments in a consistent and sound manner will improve with experience and that it is the exercise of judgment which makes the audit a professional responsibility.[Note: we do not understand the context of this text]

Financial Periods Used to Assess Account Significance versus Periods Used to Assess Significance of a Deficiency

When management uses a top-down approach that begins with the financial statements, it will necessarily use qualitative and quantitative assessments to identify significant accounts and plan the scope of management's testing. 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.

Timing of Management's Testing

The feedback also indicated that some auditors have been unwilling to accept management's testing and other procedures performed during the year as evidence that management's assessment of the effectiveness of internal control over financial reporting is fairly stated. While Section 404 of the Act and the Commission's rules require that management's and auditor's reports must be "as of" year-end, this does not mean that all testing must be done within the period immediately surrounding the year-end close. In fact, we believe that effective testing and assessment may, and in most cases preferably would, be accomplished over a longer period of time. In its adopting release, the Commission expressly noted that testing may be done over a period of time.[Note: The key issue is the reliability of the financial statements, and ensuring that systems changes are addressed appropriately.]

Management's daily interaction with its internal control system provides it with a broad array of opportunities to evaluate its controls during the year and, in many cases, to use that work as its basis, at least in part, to reasonably conclude that its controls are in place and operating effectively as of the end of its fiscal year. For example, management might determine that controls operate effectively through direct and ongoing monitoring of the operation of controls. This might be accomplished through regular management and supervisory activities, monitoring adherence to policies and procedures, and other actions. As a result, management may be able to test a substantial number of controls at a point in time prior to its fiscal year-end, and determine through its direct and ongoing monitoring of the operation of the controls that they also function effectively as of the fiscal year-end date, without performing further detailed testing.

Evaluating Internal Control Deficiencies

If control deficiencies are identified, an important part of the assessment of internal control over financial reporting is the consideration of the significance of those deficiencies and whether the risk is mitigated by compensating controls. As with determining the scope of the assessment, management must exercise judgment in a reasonable manner in the evaluation of deficiencies in internal control over financial reporting, and such evaluations may appropriately consider both qualitative and quantitative analyses. Among other things, the qualitative analysis should factor in 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 other compensating controls are effective.

One particular area brought to the staff's attention involved financial statement restatements due to errors. Neither Section 404 nor the Commission's implementing rules require that a material weakness in internal control over financial reporting must be found to exist in every case of restatement resulting from an error. Rather, both management and the external auditor should use their judgment in assessing the reasons why a restatement was necessary and whether the need for restatement resulted from a material weakness in controls. Such an evaluation should be based on all the facts and circumstances, including the probability of occurrence in light of the assessed effectiveness of the company's internal control, keeping in mind that internal control over financial reporting is defined as operating at the level of "reasonable assurance."

Disclosures about Material Weaknesses

A number of companies have reported material weaknesses in their internal control over financial reporting in this first year of implementation. When a company identifies a material weakness, and such material weakness has not been remediated prior to its fiscal year-end, it must conclude that its internal control over financial reporting is ineffective. The Commission's rule implementing Section 404 was thus intended to bring information about material weaknesses in internal control over financial reporting into public view. The staff believes that, as a result, companies should consider including in their disclosures:

- the nature of any material weakness,
- its impact on financial reporting and the control environment, and
- management's current plans, if any, for remediating the weakness.

Disclosure of the existence of a material weakness is important, but there is other information that also may be material and necessary for an overall picture that is not misleading. There are many different types of material weaknesses and many different factors that may be important to the assessment of the potential effect of any particular material weakness. We received feedback suggesting that some companies believe that they are not permitted to distinguish among reported material weaknesses. While management is required to conclude and state in its report that internal control over financial

reporting is ineffective when there is one or more material weakness, companies may, and are strongly encouraged to, provide disclosure that allows investors to assess the potential impact of each particular material weakness. The disclosure will likely be more useful to investors if management differentiates the potential impact and importance to the financial statements of the identified material weaknesses, including distinguishing those material weaknesses that may have a pervasive impact on internal control over financial reporting from those material weaknesses that do not. The goal underlying all disclosure in this area is to provide increased investor information so that an investor who chooses to do so can treat the disclosure of the existence of a material weakness as the starting point for analysis rather than the only point available.

Information Technology Issues

Information Technology Internal Controls

The feedback revealed different views that may have developed as to the appropriate extent of required documentation and testing necessary for information technology, or IT, internal controls, particularly with respect to general IT controls (e.g. controls over program development, program changes, computer operations, and access to programs and data). While the extent of documentation and testing requires the use of judgment, the staff expects management to document and test relevant general IT controls in addition to appropriate application-level controls that are designed to ensure that financial information generated from a company's application systems can reasonably be relied upon. For purposes of the Section 404 assessment, the staff would not expect testing of general IT controls that do not pertain to financial reporting. A company's finance and IT departments should interact closely to ensure that the proper IT controls are identified.

We have also been asked whether those companies that decide to use proprietary IT frameworks as a guide in conducting the IT portion of their overall COSO framework assessment are required to apply all of the components related to general IT controls that may be included in such frameworks. While the use of a separate, specific IT framework is not required, the staff understands that management of some companies has found certain parts of available frameworks to be useful. In establishing the scope of its IT assessment, management should apply reasonable judgment and consider how the IT systems impact internal control over financial reporting. Because Section 404 is not a one-size-fits-all approach to assessing controls, it is not possible for us to provide a list of the exact general IT controls that should be included in an assessment for Section 404 purposes. However, the staff does not believe it necessary for purposes of Section 404 for management to assess all general IT controls, and especially not those that primarily pertain to the efficiency or effectiveness of the operations of the organization but are not relevant to financial reporting.

Information Technology System Implementations and Upgrades

the staff does not believe it is appropriate to provide an exclusion by management of new IT systems and upgrades from the scope of its assessment of internal control over financial reporting.[Note: We believe it would also be useful to refer to the fact that there may also be additional general controls that need to be considered when, for example, a new computer system is implemented.]

Communications with Auditors

The auditor's discussing and exchanging views with management does not in itself violate the independence principles, nor does it fall into one of those nine prohibited categories of services. The staff supports a strong audit profession where a hallmark of its professionalism is to exercise sound judgment in both the audit and in ongoing dialogue with management.

The staff recognizes that questions arise in certain circumstances as to the proper application of accounting standards. Investors benefit when auditors and management engage in dialogue, including regarding new accounting standards and the appropriate accounting treatment for complex or unusual transactions. The staff believes that as long as management, and not the auditor, makes the final determination as to the accounting used, including determination of estimates and assumptions, and the auditor does not design or implement accounting policies, such auditor involvement is appropriate and is not of itself indicative of a deficiency in the registrant's internal control over financial reporting. Further, timely dialogue between management and the auditor may positively impact audit quality and the quality of financial reporting.

The staff believes that management should not be discouraged from providing its auditors with draft financial statements (including drafts that may be incomplete in certain respects). Providing draft financial statements promotes communication between the auditor and management, and all parties should recognize the draft nature of the information. In the staff's view, errors in draft financial statements in and of themselves should not be the basis for the determination by a company or an auditor of a deficiency in internal control over financial reporting. Rather, as with all cases of identifying deficiencies, management and auditors should determine whether a deficiency exists in the processes of financial statement preparation. That identification is essentially independent of whether an error exists in draft financial statements and who found it.