Georg Merkl
Sempacher Strasse 33/6
CH-8032 Zurich
Switzerland

September 18, 2006

Via e-mail to rule-comment@sec.gov

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

Subject: File No. S7-11-06

Subject: File No. S7-06-03

Dear Ms. Morris,

Thank you for the opportunity to comment on the SEC's concept release no. 34-54122 (file no. S7-11-06) on Management's Reports on Internal Control Over Financial Reporting.

I have worked both as an internal auditor and as a controller and have followed the SEC and PCAOB rules and guidance, comment letters and studies by various third parties. I hope that my comments will be useful in the SEC's and the PCAOB's efforts to make assessments of internal control over financial reporting more cost effective.

From a general philosophy point of view and to avoid costly duplication of work, section 404 should be a pyramid of assessments with decreasing amounts of work and sample sizes. Process owners (i.e. the person performing a certain financial reporting task or his superior) should perform a risk assessment and test the effectiveness of controls over financial reporting related to their tasks. Management or internal audit should review a sample of the process owner's risk assessments and reperform a sample of the process's owners tested sample or decide to select other sample elements (especially if they do not rely on the adequacy of the risk assessment). Finally, the public accountant should review a sample of the management's risk assessment and only reperform a sample of management's tested sample or decide to select other sample elements (especially if they do not rely on the adequacy of the risk assessment). Each group should be able to sufficiently rely on the work of the other groups lower in the pyramid.

Please find my comments on the SEC's individual questions below.

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?

I believe that guidance by the SEC on management's assessment of the effectiveness of internal control over financial reporting would carry higher authority than current indirect guidance by the PCAOB in Auditing Standard No. 2. SEC guidance is the natural place for guidance for issuers while PCAOB guidance should be primarily directed to the independent accountant.

However, the SEC needs to coordinate any SEC guidance on management's assessment of the effectiveness of internal control over financial reporting with the PCAOB to insure that there are no different requirements. Otherwise any efficiencies (cost savings) in management's assessment will simply be compensated by the independent accountant reacting with extended testing of his own.

There will be no cost reduction if Auditing Standard No. 2 establishes different standards for materiality, risk assessment, the effect of effective company level controls on the sample size for tests of process level controls and especially the use of the work of others (management, internal auditors, other employees of the entity, etc.) who have already assessed the effectiveness of internal control over financial reporting. If the independent accountant is not allowed to rely on management's risk assessment and test of controls, because management's standards are different or because the persons performing the tests are generally not considered "objective" or "independent" without considering the individual risk that they are actually not "objective" or "independent", then the independent accountant will simply extend his own testing to compensate for his perceived lack of reliable management's testing.

As a result, any guidance by the SEC would need to be fairly detailed and fairly long in order to allow management to translate abstract guidance into controls, that need to be tested, how often they need to be tested and sample size of the execution of the control that needs to be tested.

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?

Currently accounting and financial reporting by foreign private issuers tends to have more inherent complexity (and risk) than the accounting and financial reporting by domestic issuers. Foreign private issuers may keep separate versions of books or at least year-end reconciliations of books to different financial reporting standards. In the extreme case, a foreign private issuers in Europe may keep books according to and perform reconciliations to according to:

a. US GAAP (required for SEC filings of periodic reports and by U.S. securities exchanges)

b. International Financial Reporting Standards (IFRS/IAS) (primarily for information and investment decision making purposes and legally required for a listing on a stock exchange in the European Union or a public offering of securities in the European Union)

c. local GAAPs stipulated by the corporation law of the member states of the European Union in which the issuer or its subsidiaries are located (primarily relevant to determine the maximum amount of dividends and for public filing with the register of commerce)

d. local tax GAAPs stipulated by the tax law of the member states of the European Union in which the issuer or its subsidiaries are located (primarily relevant to determine the tax basis for corporate income tax)

This makes accounting systems and procedures more complex and a nightmare for the accounting staff of foreign private issuers. The convergence of US GAAP and IFRS and the removal of the reconciliation requirement will at least remove one level of extra work and complexity and one source of errors. Hopefully the European Union will make progress on a project to harmonise the tax base and thus tax GAAP to bring them closer to IFRS and local GAAP.

Foreign private issuers and their independent accountants are physically more removed from the U.S. and may have less access to news about changes in US GAAP and changes in SEC rules and regulations. It simply takes time until the information, training and any needed changes to financial reporting systems and processes get translated into all local languages and filter down from the issuer's headquarters to its subsidiaries and from the big 4 accounting firm's US national office to its international offices.

With the exception of the reconciliation from IFRS to US GGAP, domestic issuers with international subsidiaries share the rest of the complexities and problems mentioned above.

Possible solutions that the SEC can take are:

a. create a central internet based resource that collects the different sources of US GAAP

b. delay the effective date of any changes to US GAAP and SEC rules and regulation for issuers with international subsidiaries

c. ensure that all speeches and slides at conferences by SEC or PCAOB staff at conferences are promptly disclosed on the SEC's and the PCAOB's websites (this has historically not been the case, just look which SEC staff and PCAOB staff participated at the New York State Society of CPA's latest conference and what is on the websites. I hope SEC and PCAOB employees cannot privately receive speaker fees and thus have an incentive not to make all information public)

d. remove the reconciliation requirement between IFRS and US GAAP

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

I think it is illusory that a guidance based on broad principles only can be effectively translated into real world requirements for controls that need to be tested, the frequency of testing those controls and the sample sizes that need to tested. In the absence of SEC guidance the independent accountants will fill this void and dictate their own minimum standards (probably derived from PCAOB AS No. 2) for management's assessment of the effectiveness of internal control over financial reporting that they are willing to accept to use as the work of others.

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?

I think the federal government needs to look at the big picture and the incentives of the players, which have created this problem. The Sarbanes-Oxley Act also created an independent watch dog for public accountants, which can second guess the judgements of public accountants in inspections of audits and which can impose sanctions on public accountants. In addition, the remaining big 4 have seen what happened to Andersen. The result is that public accountants are risk averse for fear of being second guessed by the PCAOB and in civil law suits concerning alleged audit failures. It is no surprise to me that public accountants are afraid of taking a risk based approach to the audit of internal control over financial reporting because a risk based approach requires auditors judgement. In case of doubt they will avoid judgement and test even low risk transactions or err on the risk averse conservative side when making risk assessments.

The PCAOB's role is to ensure quality audits by public accountants. While it can verbally communicate to public accountants that they are too risk averse and could perform audits more efficiently and at a lower cost, it is not the competition authority for the audit industry.

I think there is an issue of a lack of competition between the big 4 audit firms, which has also been highlighted by a PCAOB study. The federal government should see what they could do to foster competition in the audit industry. Possible actions could be:

a. create an incentive to compare prices through a communication that it is the SEC's view that periodic requests for proposals and competitive bidding or at least a benchmarking of fees for audit engagements are a fiduciary duty of the respective audit committee members. In addition, the PCAOB and the SEC could create an audit committee best practices webpage that provides best-practice policies and procedures and model requests for proposals for selecting and managing public accountants.

b. improve price transparency in the audit market and make benchmarking easier by modernising the EDGAR database so that it is easy to identify the audit fees or other issuers in the same industry with a similar size in revenues, assets or market capitalization. It should be possible to easily analyze SEC filings without having to pay fees to private providers like auditanlytics.com that fill the gaps that the SEC has neglected.

c. improve transparency of audit firms on the supply side by a searchable database on the PCAOB website where issuers can look which audit firms audit other issuers in the same industry with similar sizes in revenues, assets or market capitalization and in geographic regions.

d. grow new competitors on the supply side by affirming that in principle all registered audit firms are considered to be able to provide quality audit services and that selecting an other audit firm than an established big 4 firm is a perfectly acceptable practice, by evaluating the effect on competition of any fees levied by the PCAOB and any rulemaking and auditing standards by the PCAOB. Auditing standards on the use of the work of another auditor and the related sharing of liabilities and international inspections by international audit watchdogs will play a key role in encouraging or discouraging the forming of new alliances and networks by audit firms in different countries, which is a precondition to be able to serve foreign private issuers or domestic issuers with international subsidiaries

In addition, further guidance on the difference between internal control over financial reporting (i.e. section 404 SOA) and disclosure controls and procedures (i.e. section 302 SOA and the assessment of the effectiveness of each should be provided. In one of its rules, the SEC stated that disclosure controls and procedures do not include 100% of internal control over financial reporting, but that there is only a substantial overlap. However, the SEC provided only one example of internal control over financial reporting that is supposedly not included in disclosure controls and procedures. I think the SEC's view is flawed and has been misguided by purely looking at the definition of internal accounting controls in the securities exchange act without looking at the legislative history. Internal accounting control is the old term of for internal control over financial reporting. It was used by the auditing standard that was in force when the foreign corrupt practices act was enacted. The definition in the securities exchange act has been copied word by word from the auditing standard. The primary objective of internal control over financial reporting is assuring accurate and reliable financial reporting. The prevention of fraud and the protection of assets (misappropriation/unauthorized use of or disposition of assets) is only relevant to the extent that the fraud or misappropriation of assets has a **material** effect on the financial statements (the SEC's Advisory Committee on Small Public Companies published an old SEC policy release commenting on internal accounting controls and the materiality of fraud). A dual signature requirement (e.g. involving a superior) may be relevant for the effectiveness and efficiency of operations objective of internal control, but may not even be primarily designed to prevent fraud, but rather that purchases are properly authorized so that there are certain authorities limited to the level in the corporate hierarchy and some preventive controls on staying withing spending budgets.

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

Legally binding guidance in the form of a Commission rule is preferable and will carry more authority. Interpretive guidance my be challenged by other parties, such as public accountants as not having a relevant level of authority. In the case of any conflict between the SEC guidance and the PCAOB guidance, public accountants will

rightfully refer to the PCAOB audit standard, so a coordination between SEC and PCAOB guidance is absolutely vital.

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?

While I cannot provide any experience as an accelerated filer, I can provide experience as a preparer of financial statements and as an internal auditor.

Preventive controls, such as hiring qualified, committed and ethical staff, clear communication of procedures and training are likely to be much more cost-efficient, than detective controls, such as a review and approval of transactions by a second person. However, it requires more judgement to assess the effectiveness of a preventive control and issuers and public accountants may have been reluctant to determine the resulting reduction in control risk and the elimination of or at least the reduction of the sample size and the extent of testing of process level controls.

The frequency and the extent of testing of controls should be risk based. There should be only be a minimum of requirement of an annual testing frequency. A base line approach that uses cumulative knowledge gained through assessments audits should also be possible to non-automated controls. While it is perfectly fine to review a larger extent of a recently hired employee's work to make sure that he understood the policies and training and has correctly performed his task, this can be reduced if the initial assessment has shown that there were no errors and that the employee can be relied upon. It should be up to the judgement of management and the public accountant to determine if the assessment of any material changes to controls have occurred since the last assessment and the assessment of the effectiveness of the changed controls (roll-forward testing) is more efficient (and results in a lower cost) then simply re-assessing the effectiveness of all controls in a process without assessing if they have changed or not.

As far as reviews/approvals of certain transactions are concerned, automated reports that select unusual transactions or transactions with a higher likelihood of fraud or error tend to be more efficient than having somebody review an endless list of all transactions and having that person pick random samples. A list of the number of uses of a particular expense account by each cost center sorted by ascending usage numbers is likely to efficiently identify the erroneous use of cost centers. Sorting entries on revenue accounts by amounts per day or per week will allow the identification of unusual activity shortly before the end of periods (quarters, months, etc.) and after the end of periods.

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?

No. Any Commission guidance can and should be updated if monitoring by the SEC turns out that certain elements of the guidance are not efficient.

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?

Traditionally, the US has been leading in publications on internal control over financial reporting. In addition, the COSO framework is older than Turnbull. Furthermore, the big 4 audit firm's methodologies for internal control audits seem to be dominated by their respective US national offices. COSO is much more detailed than Turnbull and offers more guidance.

However, the division of internal control into components by COSO is not very intuitive and does not follow a natural sequential process. A revision of COSO (COSO 2.0) to make it more user friendly and intuitive would be beneficial.

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?

Yes, the guidance should include the May 16, 2005 Staff Statement and all staff positions on frequently asked questions. The Comission Rule should be a clearly structured one stop shop without the need to consult a multitude of other sources, such as staff positions, etc. A Comission rule carries more authority and is less likely to be challenged.

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?

I think it is a misconception to associate section 404 with the Sarbanes-Oxley Act (SOA) in its entirety. Section 404 is just one out of many sections of the SOA. In addition, the Senate Committee on Banking, Housing and Urban Affairs report on

SOA in the legislative history of SOA makes it clear that congress did not intend section 404 (b) audit to cost any extra audit fees. While this may have been a naïve view by congress, it makes clear, that the section 404 should be not absolute must and that the SEC should step in if the costs of section 404, which are ultimately born by the investors do not justify the incremental benefits of section 404.

I think the SEC should clearly analyze the cost and benefit of management's assessment of internal control over financial reporting and the cost and benefit of the public accountant's attest on management's assessment. The analysis should be done for different sizes of issuers (e.g. micro-cap, small cap and large cap) and should include a sufficiently large sample of issuers, which are just above the threshold for accelerated filers and are already in their second year of 404 audits, because this group can serve as a proxy (forecast) of the costs for non-accelerated filers if the SEC considers extending 404 compliance to those issuers.

The analysis should use a metric that can be easily understood and judged by investors and their advisors (i.e. securities analysts and other investment advisors or investment managers). Measuring the cost as a percentage of revenues or assets is abstract and does not really allow any decision. The cost of section 404 is ultimately born by the investor, so the only useful metric is section 404 (a) and section 404 (b) costs as a percentage of net earnings per share before section 404 (a) and section 404 (b) costs (corrected for the tax deductibility effect of the section 404 (a) and section 404 (b) costs. This way if the SEC's office of Research and Analysis can easily interview a sample of securities analysts and investments advisors of micro-cap, small-cap and larger cap public issuers and say do you think that the reduction of x % of net earnings that you pay for section 404 (a) and section 404 (b) is worth the incremental benefits from section 404(a) and 404(b) considering that.

a. the securities act already requires issuers to have internal control over financial reporting (internal accounting controls

b. the public accountant is already required by existing auditing standards to test internal control over financial reporting during his audit of financial statements, but has the flexibility to exclude the testing of those areas of internal control over financial reporting, where he believes that the effort for substantive tests of the numbers produced by the financial reporting is lower than the effort to test internal control over financial reporting of those areas and any resulting savings in substantive testing

c. section 302 certifications of internal control by management

On the bottom line, investors only care if financial statements are reliable. It does not matter if the auditor used tests of internal control over financial reporting or substantive tests (e.g. accounts receivable balance confirmations with customers, observing or performing stock counts, etc.) to test a particular account or financial statement disclosure. The existing auditing standard SAS No. 55 allowed the auditor to judge whether tests of the effectiveness of internal control or substantive tests were more efficient (and thus less expensive) in a particular area. Substantive tests are particularly more efficient in smaller companies. If a substantive test discovers a discrepancy between the amount resulting from the test and the amount in the unaudited financial statements, this is usually an indicator of a control deficiency and

the root cause of the problem and any necessary changes to controls can be determined later. An important difference between SAS No. 55 and AS No. 2 is that material weaknesses and significant deficiencies did not need to be communicated to the shareholders (only to the audit committee and management) and that there was no separate opinion on the effectiveness internal control over financial reporting because the auditor could exclude certain parts of internal control over financial reporting and replace them with substantive tests in those areas. From an overall audit efficiency point of view, the older SAS No. 55 audit approach may be more cost efficient for smaller public companies. The SEC and the PCAOB could think whether material weaknesses and significant deficiencies that were discovered during the audit of financial statements (if no SOX 404 (b)/AS No. 2 audit is done) should also be communicated to the shareholders and whether the auditor should explicitly describe the areas of internal control over financial reporting relating to which accounts or disclosures (or assertations) were NOT tested for effectiveness of internal control, but through substantive procedures and whether substantive procedures resulted in any audit adjustments/restatements of unaudited numbers (i.e. put sunlight on the company's financial reporting problems instead of quietly fixing them before the financial statements are filed and published).

This results of the cost-benefit analysis and the related opinions by the interviewed parties and the reason for the SEC's policy decision should be clearly disclosed in any final SEC rule.

I think the SEC should consider an opting-out possibility for the public accountant's attestation for smaller public companies provided that this opt-out is disclosed and that the majority of the members of the audit committee are independent and that there is a minimum number of independent financial experts on the audit committee. As far as I know, the options backdating scandal was discovered by research of two academics who provided a tip to the SEC and not by internal controls. If you look at the Association of Certified Frau Examiner's reports on sources that led to the discovery of fraud, internal control is low on the list. Internal control or section 404 should not be made a holy cow, but be subject to a rational and rigorous empiric cost-benefit analysis.

Cfo.com has communicated, but sadly there seems to have been no official communication by the PCAOB and the SEC, that the PCAOB is already discussing revisions to Auditing Standard No. 2 with the SEC.

I certainly believe that AS No. 2 can certainly be made more efficient (at least for larger public companies) by removing prescriptive requirements that require certain tests to be made every year instead of using a baseline approach that uses cumulative knowledge from prior years and an assessment if any changes occurred since the last baseline testing and any roll-forward testing. In addition, the role of preventive controls and company level controls or the review of actual results to budgets and forecasts should be discussed in relation to process level controls.

The SEC and the PCAOB should consider the results of a recent Flash Survey by the Institute of Internal Auditors concerning the use of recent PCAOB guidance by public

accountants and implications for next year (www.theiia.org/download.cfm?file=33877).

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?

Any risk has two dimensions: the likelihood that an event is occurring and the magnitude of the impact on the financial statements. As a consequence, the guidance should begin stating that the objective of the assessment of the effectiveness of internal control over financial reporting is to provide reasonable assurance that the financial statements are free of material weaknesses. It should be made clear that the objective is ***not*** to identify significant deficiencies. The consequence is that planning materiality and resulting selected accounts, classes of transactions, controls and sample sizes are driven by the identification of material weaknesses and not by significant weaknesses. The question whether the aggregation of individual significant weaknesses results in a material weakness only becomes relevant if significant weaknesses become discovered ***by accident***.

This should be followed by the definition of a material weakness (which should rather use an "at least reasonable possible" likelihood rather than a "more than remote" likelihood).

Assessing the likelihood and the magnitude of an event requires judgement and the fear of that good faith judgements being second guessed. A difference in opinion on judgement between management and the public accountant should not automatically be construed as a material weakness on the part of management. Similarly a difference in opinion on judgement between the public accountant and PCAOB inspectors should not automatically be construed to be an audit deficiency by the public accountant.

Furthermore, an elaboration of the concept of materiality is necessary. While it is nice to recite that the investor ultimately decides what is material for his decisions, this concept needs to be made operational and translated into numbers. The investment decisions for the largest proportion of amounts invested in the public markets are probably being prepared or made by securities analysts, investment advisors and investment managers. The SEC should interview a sample of each of those groups how they actually use financial information to make investment decisions. Most analysts use historical financial information to create forecasts of future financial performance and use discounted cash-flow valuation or multiples based valuations. As a consequence, an issuer or an auditor could create a similar model and perform sensitivity analyses to determine which amounts would have a material impact on the resulting equity value. Obviously debt analysts use other information and bank covenants are also very relevant. Both the gap to earnings expectations by analysts and the amount it would take to breach bank covenants or to cause a possible reduction of a credit rating can lower the absolute materiality threshold. Auditor rules of thumb, such as percentage of revenues or percentage of earnings thresholds may not be relevant for growth companies or companies with liquidity difficulties.

SEC guidance should evaluate and answer the question whether materiality applies to quarterly financial statements or only to annual financial statements. Some auditors may simply have applied the same rule-of-thumb percentages of revenue or net profit thresholds to the lower absolute quarterly amounts (i.e. often one fourth of the annual amounts). However, as mentioned above, an investor or a securities analyst will extrapolate the historical quarterly financial statements to make forecasts of future **annual** amounts for future periods. In the case of issuers with a seasonal business (i.e. certain retailers with significant Christmas sales) with significant differences between individual quarters or growth companies with quarter-on-quarter growth driving the equity value, quarterly materiality will differ from quarter to quarter.

Inherent risks and control risks should be assessed both by the people in charge of executing a particular process and control and by any other persons performing the assessment of internal control over financial reporting. Since judgments about risk are subjective, there will frequently be discussions and disagreements about risks. A collection of empirical data on actual past problems (i.e. the occurrence of risks) on the SEC's website would be very beneficial. Sources of this information can be actual root causes and financial statements components for material weaknesses and significant deficiencies. Apart from SEC and PCAOB data from restatements and material weaknesses, other organisations, such as Financial Executives International, the Institute of Internal Auditors or the
Association of Certified Fraud Examiners (ACFE) could provide information for the SEC or PCAOB website. Issuers are reluctant to disclose information on fraud, but the ACFE collects anonymized information.

A top-down approach also implies the assessment of company-level (entity-level) controls and their effect on process level controls. The SEC should elaborate how effective company level controls reduce the control risk at the process level and can result in a lower effort of testing at the process level.

I think that there is currently no guidance on determining sample sizes for tests of controls other than the old AICPA Audit and Accounting Guide on Audit Sampling. However, the AICPA guide is fairly abstract. Ideally a modern guide should include spreadsheet based implementation tools and case studies and should allow to show the effect of how an assessment of materiality thresholds, inherent risk, of entity-level controls and preventive controls has an impact on sample sizes for tests of process-level controls. Any revised guidance on determining sample sizes for tests of controls should also discuss basic questions, such as how to define a "population" and when a set of data needs to be divided into several "populations" because they do not share the same risks and characteristics.

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?

Guidance on IT controls and which IT controls are relevant for financial reporting would be very beneficial. It should discuss situations and industries in which general IT controls, such as Server and PC operating system security, network security and backups and disaster recovery plans or fallback data centers are relevant. In addition, it should separately discuss application controls both for purchased standard applications (e.g. SAP, Oracle Financials, Peoplesoft, JD Edwards, etc.), which are typically customized to the business's particular processes through configuration tables and master data setting and in-house developed applications.

The SEC and PCAOB should look at historical occurrences of financial reporting problems linked to general IT controls and application controls and recommend whether testing by management ***and*** the public accountant in those areas is typically necessary. In my opinion, unless the industry has a higher risk of hacking, such as in industries with significant electronically intellectual saved intellectual property (e.g. compute games, music and film undustry), political exposure (e.g. defence contractors) or significant amounts of electronically accessible funds (e.g. banks and savings and loan associations), general IT access controls are less of a risk and testing by the public accountant in addition to management's assessment will generally not be necessary.

The SEC should also make clear that an issuer can expect that the issuers can expect in good faith that widely used standard applications (e.g. SAP, Oracle Financials, Peoplesoft, JD Edwards, etc.) allow the reliable processing of accounting transactions. It would not be efficient and highly duplicative to require management and the public accountants to perform black box testing that every function and every standard report produces the desired result. When a standard application is first installed and customized it is common practice to conduct end-user acceptance testing in a quality assurance system before moving the application to a live productive system. The issuer (and potentially the auditor) should assess whether a later change in customizing tables or later programming of own reports in the standard system, which are used for controls could have a reasonably possible likelihood of a material effect on the financial statements. The installation of new versions, upgrades or patches may require an assessment of risk and maybe testing before the transfer into the productive system.

In the case of an in-house developed application, the burden of testing that the application is reliable for financial reporting should be on the issuer and should be made at the time of installation of the software.

The SEC should define whether controls, especially IT controls only relate to the accuracy and reliability of financial statements or if they also should provide reasonable assurance that the financial statements are filed within the required deadlines. The SEC's view will be important in order to determine whether back up and disaster recovery controls and alternative data center controls are relevant for management's assessment and the public accountant's audit. In my opinion, the likelihood of disasters or power outages that are so extended that the filing deadlines will be missed by a significant amount of days is quite low. Katrina simply does not occur every year in New Orleans.

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?

The SEC and the PACOB should focus on areas and controls, where it presumes that the risk is low so that they can be excluded, less attention can be paid to them or that need not be audited by the public accountant.

To be frank, the COSO guidance is not very focused on smaller public companies. The number of pages focusing on the differences in controls between larger and smaller public companies is very limited. I think that the added-value of the forthcoming COSO guidance is negligible. Like the original COSO framework itself it was largely developed by staff from big 4 audit firms and not by preparers of financial statements or internal auditors. The criticism in the comment letters on the draft of the new COSO framework speaks for itself.

In a smaller business, management has a better overview and a better technical knowledge and ability to assess what is going on in the business. Management by wandering around and intimate knowledge of the business allow for more effective budget to actual reviews by management or to spot whether a particular financial ratio or amount does not seem to make sense. Segregation of duties is not always possible in smaller businesses. Segregation of duties is mostly a process level fraud issues and in my opinion the likelihood of fraud and the materiality is often very low anyhow. Independent review and approval of a sample of transactions and of exception reports can be an effective substitute for segregation of duties.

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?

I recommend that the SEC studies the typical accounts (areas) and the typical root causes of past material weaknesses and restatements and puts statistics sorted by number of occurrence and any clusters in certain industries on its website. In this way smaller public companies can more easily profit from the experience of accelerated filers with problem areas.

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?

If a study of the SEC shows that there are significant differences between restatements and material weaknesses at larger and smaller public companies, then it should point that out. GAAP expertise or at least consulting and advice on changes to GAAP and their impact on companies are sometimes outsourced by smaller public companies. The SEC should provide guidance if and when such outsourcing is permissible and is not automatically considered to be a material weakness. This also has an impact on the issuer-auditor relationship and auditor independence if GAAP advice is outsourced to the auditor.

I think the role of entity level controls should be discussed together with a top-down approach.

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?

Please refer to my answer to question 11. Smaller public companies often use standard software (and in-house developed Excel sheets) for accounting, so this question is also related to your questions and guidance on IT controls.

Smaller public companies often do not have the financial resources to spend much money on compliance consulting. As a consequent, my comments on free internet based guidance on empiric data, best practices, audit firms and audits by the SEC and the PCAOB are especially relevant for smaller public companies.

A risk assessment should include an assessment of inherent risk and an assessment of control risk. The Institute of Internal Auditors should be able to provide you with typical risk factors used by internal auditors in a top-down risk assessment. You also find examples of such factors on www.auditnet.org

Examples of risk factors for the likelihood of inherent risk:

a. inherent complexity of a transaction and the amount of technical knowledge and concentration it requires

b. inherent complexity of the accounting standard/treatment of a particular transaction

c. subjectivity for determining the appropriate amount or accounting treatment

d. past occurrences of errors in this area

e. change in processes and types of transactions

f. workload and level of stress

g. incentives through compensation tied to aggressive financial targets

h. likelihood of a breach of bank covenants or a reduction in the credit rating

etc.

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?

Any results of the past occurrence of fraud, its root causes and controls for preventing fraud should be included. The Association of Certified Fraud Examiners (ACFE) and the AICPA' Frau Task Force are certainly excellent sources. I also recommend findings from the National Commission on Fraudulent Financial Reporting (Treadway Commission/COSO)' s reports on the causes of fraudulent financial reporting. As far as I know there has been no recent study. The SEC and congress may consider to conduct a new updated study and report. I am sure there is tons of data from recent accounting scandals such as Enron, Tyco, Worldcom, Healthsouth, as well as the options backdating scandals around.

I think whistleblower hotlines for employees, customers and suppliers and related communications are certainly key. In addition, every person performing management's assessment and the public accountant should ask certain fraud related questions during every interview, which is done during the audit of internal control over financial reporting or the audit of financial statements (e.g. have you ever been asked to do something unethical or observed something unusual in your job or do you know of any colleagues having been asked to do something unethical or having observed something unusual?)

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?

Yes. The Guidance should also consider the case when an issuers consists of several small locations and groups (i.e. shop outlets) so that no small number of locations will already represent a material amount of relevant financial statement accounts or disclosures. In the case of a large number of small and individually insignificant, but homogenous locations, which are significant when aggregated, testing of a sample of locations should be permitted.

The guidance should also include whether the existing definition from the securities exchange act concerning the responsibility for internal accounting control for joint ventures and minority investments is also valid for the assessment of the effectiveness for internal control over financial reporting (i.e. if there are no shareholder agreements which include an audit clause for internal auditors of the issuer, an external AS No. 2 audit by public accountants, or a SAS 70 type 2 audit, then the issuer can exclude the subsidiary from the scope).

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.

Hiring competent and committed staff. Monitoring changes in GAAP. Providing adequate communication, information and training. Clear assignment of responsibility and authority (nothing falling through the cracks).

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?

On-going observations by a superior of the execution of a particular control by a subordinate just because they physically working close the each other clearly have value.

Preventive controls like adequate training and clear communication of policies and responsibilities should be important and reduce detective evaluation type testing. Regular comparison s of actual financial performance and ratios to (flexible) budgets, forecasts, external benchmarks or simply financial ratios that make sense based on experience (i.e. analytical reviews) should count as controls and are often useful to spot errors in actual financials, budgets or forecasts.

An assessment of the design effectiveness of preventive controls is judgemental in nature since they are designed to prevent errors or fraud from occurring. The operating effectiveness of preventive controls can only be indirectly be inferred from the absence of errors or fraud. This difficulty in assessment should not be construed to mean that there can be no reasonable assurance about the effectiveness of preventive controls.

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?

No comment.

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?

I think a definition of the terms “separate evaluations” and “evaluation type testing” and “ongoing monitoring activities” would be helpful.

This is linked to my general comments on the use of a baseline (or benchmark) audit approach and the use of cumulative (prior year(s)) audit knowledge. It is vital that management identifies any (planned or anticipated) changes to internal control over financial reporting, assesses the change to inherent risk and determines which controls are necessary or need to be retested to mitigate those risks.

The guidance should make clear that internal control over financial reporting is a ***process*** that should operate continually and that an assessment (opinion) of its effectiveness as of a particular point in time does not mean that the assessment needs to be performed at exactly that point in time. Depending on the identification of any changes since the last assessment and an assessment of the risks and potential impacts of those changes, retesting the controls impacted by those changes may be necessary.

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?

This point relates to both the testing before the as of date (i.e. the end of the financial year) and any necessary roll-forward testing and to using cumulative audit knowledge and relying on assessments from prior years and any necessary roll-forward testing.

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?

This is related to weaknesses in IT controls, which may have an effect on several accounts or disclosures or to fraud-related controls, where the size of a potential fraud is hard to judge. In any case statistics of the likelihood and magnitude of historical problems at other issuers will be vary helpful in discussions with internal audit and the public accountant. Potential compensating controls, such as variance analysis between budgeted and actual results may reduce the magnitude of a fraud without it being detected through the analysis to a level, where it is no longer material.

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.

I think the current change from a “more than remote” to an “at least reasonable” likelihood is already a good step in terms of a more intuitive plain English and reasonable definition.

There should be guidance that historical occurrences of problems can be used as indicators of a particular likelihood.

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. Controls during the financial statement close process are part of internal control over financial reporting. The fact that regular controls during the financial statement close process detect a material financial statement error should be seen as the effectiveness of the issuer’s detective and compensating controls. However if the error was discovered purely by accident and not through an established control (i.e. a review of the financial statements and comparison to some metric) it may be a material weakness.

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. Usually restatements are material, but if a restatement is not material, it cannot be a material weakness. In addition, a restatement, which is caused by fraud or an error, which happened because effective internal control over financial reporting only provided reasonable but not ***absolute*** assurance, should not be a material weakness. Furthermore, a restatement that was caused by a change in an accounting standard, which requires the retrospective application of the accounting treatment to prior periods should not be considered a material weakness. In addition, the issuance of new interpretive guidance in an area where management previously made a goof faith interpretation of the standard, which results in a revision of management’s interpretation based on the new guidance and which results in a restatement, should not be considered a material weakness.

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)?

Most standard applications for accounting (e.g. SAP) have built-in capabilities to perform analyses and reports (e.g. transaction SE16 data browsers, transaction SQVI

quick viewer, query builder, ABAP programs, etc.). Those capabilities can be used to create exception reports. Examples of exception reports are:

a. overdue production orders included in work-in-progress (risk of overstating work in progress)

b. overdue purchase orders with no goods receipt (risk of understating liabilities, inventories or expenses)

c. shipments of goods, which have not been invoiced yet (risk of understating revenues)

d. lists of failed transfers of invoices or credit notes from the sales module to the accounting module (transaction VFX3, risk of under- or overstating revenues)

e. list of material movements, which could not be posted due to errors (transaction COGI, risk of over- or understating of inventories)

f. accounts receivable aging (risk of overstating receivables)

g. vendor master records, where the duplicate invoice check is not switched on

h. product master tax/vendor master tax code combinations, which result in the application of an old value added tax (VAT) code from before a change in VAT rates, such as the one happening in Germany

i. purchasing info records using old VAT codes, accounting records using old VAT codes

j. changes to selected customizing tables with an impact on accounting

etc.

Such are much more effective to identify possible errors and fraud than blind random samples. Of course determining the data to check and the selection criteria to use is based on an assessment of possible risks.

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?

Typically general IT controls only have an indirect relation to the preparation of financial statements. It would be beneficial if the guidance could include a definition of “general IT controls” and “application controls” and examples for both types of controls or any other categorizations that the SEC wants to use.

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?

COBIT is widely used because it has been developed by the Information Systems Audit and Control Association (ISACA). However, criteria relating to the reliability of IT systems may not be that critical for financial reporting. Short delays in the availability of systems for financial reporting may be acceptable for many issuers.

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?

The absence of documentation should not automatically be considered to be a deficiency. Written documentation is simply an alternative to communicating information verbally. In many cases it may require more time to communicate the results of a policy or procedure, the results of a risk assessment, the transactions tested during a test of the operating effectiveness of a control and the conclusions from the tests verbally than to document them for later review by the internal auditors or the public accountant. Typically internal auditors keep workpapers of the tests they performed anyhow. So documentation of tests performed by internal auditors should not be an issue.

Auditors are sometimes obsessed with documentation and mistake keeping printed and dated copies of a report with tickmarks or initials as evidence of the actual performance of a control, such as the review of a report. Reports can be printed much later and backdated and artificial initials and tickmarks can be produced without any review and analysis ever having been performed. Only inquiry (i.e. an interview) and reperformance will actually allow the assessing person to determine if a control is actually performed and working effectively.

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?

Documentation of the risk assessment is preferred. If management is certain that they can remember the risk assessments for every account and disclosure then documentation will not be necessary, but this is unlikely. For documentation of risk assessment, a baseline documentation approach should be chosen. Only additions of new risks or the elimination of old risk or changes to the risk assessments should be documented or a new version of the updated risk assessments should be documented. Meetings minutes for meetings, which resulted in no to prior year's risk assessments should not be required to be documented.

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?

Management should be able to communicate all the information to the public accountant that he needs to assess the effectiveness of management's assessment and

to reperform samples of management's testing. If management cannot be sure that they will remember everything months later, written documentation will be the better option. Not being able to remember certain assessments may result in costly and inefficient extensive reperformance of tests of controls by the public accountant.

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?

Inquiry through an interview should suffice. The absence of written documentation of user-acceptance testing of every accounting relevant function at the implementation of a new accounting system does not imply that the users did not conduct the testing and are lying.

I think actual copies of reports that were reviewed are not necessary as long as the frequency of the reviews and the selection criteria of the reports can be communicated so that the review can be reperformed by the public accountant.

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?

If it takes less time to communicate it verbally to the auditor in an interview, then there should be no requirement to document it. However management should be sure that they can remember all the information which is necessary to reperform a sample of management's assessments if the auditors decides to do so.

I hope that my comments are of assistance to you. Please do not hesitate to contact me if you have any further questions concerning my comments.

Yours sincerely

Georg Merkl