500 McCarthy Boulevard
Milpitas CA, 95035

February 23, 2006

Request by SEC and PCAOB for comments on §404 lessons learned

I appreciate the opportunity to provide feedback on lessons learned and the opportunities to improve the efficiency and effectiveness of managements' and auditors' assessments of internal control over financial reporting, as required by §404. I am writing as an individual, providing personal opinions obtained as a member of the management teams at two large companies implementing their programs for the first two years, as well as a contributor to the Institute of Internal Auditors' related activities.

In general, I would like to commend both the Commission and the PCAOB for the movement they have generated with their 2005 statements, Q&A's, etc. The May 16th documents were landmark events, and the November 30th report was right on target. Progress has been made as both management and external auditors have become more knowledgeable and efficient. The criticality of a top-down, risk-based approach cannot be over-emphasized.

Yet, while progress has been made there remains a considerable distance to travel before, in my assessment, the work performed by the auditor (and what the auditor requires of management) are consistent with the expectations of management and Audit Committees for an efficient process. I have a few suggestions that you may find of merit.

1. Planning by the external auditor should not only be done early, but shared with management to enable more effective use of and reliance on management testing. There should not be any secrets about the external auditor's detailed risk assessment or methodology.

2. The work of the external auditor will become more efficient when management's assessment process becomes more efficient. I suggest the SEC consider finding ways to provide more assistance to management (whether through additional Q&A's or other means).

3. Firms continue to include areas in scope that are highly unlikely to be the source of a material misstatement. While the PCAOB has indicated that the scope of work for §404 should be focused on areas where there is an inherent, at least reasonable possibility of a material misstatement, the same should be said about the scope of the whole integrated audit.

4. As a matter of detail regarding the above, one firm's methodology for establishing planning materiality for determining significant accounts (as reported to me by a partner) involves determining a materiality level based on quantitative and qualitative factors, then taking a 15%-25% "haircut", then another 15%-50% haircut based on the

assessment of overall risk (generally the partner's assessment of prior periods' internal controls). This results in accounts being considered significant that are quite small relative to what would be considered a material error.

5. The CPA firms' interpretation of the "rules" for §404 have (anecdotally) varied not only from firm to firm, but office to office and partner to partner. This is the shared impression of a number of CFO's and heads of internal auditing. In addition, my experience with the national office of one major CPA firm resulted in the belief that the senior partners were not comfortable using judgment in assessing individual facts and circumstances. For example, they were reluctant not to conclude there was a material weakness when the financials were restated because of a rare event – because they said they have not yet seen a restatement that did not have a related material weakness. The same firm was reluctant to apply the benchmarking practice in year two, placing very significant hurdles in front of management because (they stated) they had little or no experience with benchmarking. Can the PCAOB perform more reviews of each firm's:

    a. Methodologies, policies and procedures
    b. Training, and
    c. National office interpretations and decisions?

6. There is no easy, commonly-known way for registrants to dispute interpretations by their external auditors' national offices, or to make a complaint (perhaps anonymously). The SEC and PCAOB might consider addressing this issue.

7. We need a definition of a key control, as this is the center of the §404 testing. I suggest the definition that will be included in an upcoming *Guide for Management* that will be issued by the IIA:

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

8. There continues to be a significant amount of bottoms-up risk identification, especially when determining what IT General Controls issues should be in scope. One firm identified a number of key risk areas that it said had to be addressed by every client, even though they were not the result of a top-down risk-based approach. The same firm has standard tests it runs, even when the tests are not linked to key controls.

9. Taking that point further, both management and the external auditor need guidance on what constitute key controls within IT General Controls. How does management or the auditor continue their top-down risk-based assessment from significant accounts to individual IT General Controls? There are initiatives under way, notably by the IIA, and the active participation by both the SEC and the PCAOB would be valuable.

10. Continuing with IT General Controls, there is a tendency, due to the misused and overused term "pervasive," to ascribe too much significance to IT General Control risks. While IT General Controls as a whole may affect multiple applications and multiple key automated controls, in practice individual key controls within IT General Controls do not have a "pervasive" or ubiquitous affect (which is how people are translating pervasive) but may only affect a limited number of applications or locations. Further clarification would be valuable on the use and meaning of *pervasive*, as well as on the related topic of aggregation. I suggest something that is based on risk – where multiple controls are reasonably likely to fail at the same time because of a shared attribute, such as being performed by the same individual or impacted by the same IT general control.

11. The topic of "reasonable assurance" continues to be problematic. Unfortunately, the clarification that reasonable assurance represents a high level of assurance is not particularly useful. The SEC and the PCAOB need, in my opinion, to address the fact that systems of internal control are not perfect. They will fail, even if infrequently, and when they do that does not necessarily indicate a control deficiency – even if a material error results. It is not logical to conclude there is an ineffective system when exactly the same monthly control, operated with the same people and systems, performs perfectly for three years before failing a single time. Neither the quality of the system of internal control, nor the assurance it provides relative to the financial statements, have changed. Guidance should direct management and the auditor to consider the likelihood of failure in the future.

12. When the external auditor identifies an exception, they do not always expand the sample size – and do not always add management's testing to the population tested – to determine whether the exception is isolated.

13. There is not a consistent understanding of fraud risk that should be considered. While guidance is clear that only frauds (or thefts) that result in a material misstatement need be addressed, that is not consistently applied. Further, there is not clarity on the application of the portion of the definition of internal control over financial reporting relative to "receipts and expenditures are being made only in accordance with authorizations of management and directors of the company." Should this only be assessed if there is a risk of material misstatement of the financials?

14. When firms perform tests for SAS 99, they do not always do so based on the results of any fraud risk assessment performed or reviewed as part of the §404 assessment. The SAS 99 work should be integrated with the §404 work.

15. Based on comments made to me by a number of partners with different CPA firms, there is a perception that some of the PCAOB regulations are onerous – leading to increased costs that are passed on to clients. In addition, comments have been made by these partners that the PCAOB inspectors' approaches are not always consistent with the principles and guidance of Auditing Standard Number 2. I cannot validate these

comments, but the fact that they came from multiple partners from multiple firms in varying geographies indicates there is at least smoke, if not fire.

Again, I appreciate the efforts and results achieved by both agencies and am looking forward to additional guidance and progress in the future.

Norman D. Marks, FCA, CPA
Vice President, Internal Controls and Process Assurance
Maxtor Corporation

---

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

[ii] The *timely* detection of an error is critical. Otherwise, detection may occur after the financial statements have been filed with the SEC, leading to the potential need for restatement.