02/15/2007
Securities and Exchange Commission
File Number S7-24-06
Sirs:
I developed and teach a seminar entitled "Sarbanes-Oxley Act: Assessing IT (Information Technology) Controls" for the Institute of Internal Auditors. I have taught versions of this seminar over 40 times, involving over 700 companies. My comments and suggestions are drawn from the experiences of these organizations and my own consulting experiences.

In general, the individuals assessing the IT controls have had to interpret the implications for information technology from the Standards and Rulings, which are written from a financial perspective and knowledge base. They have also had to deal with external auditors who lack the skill set to adequately understand the risks involved in the information technology of the organization. Yet it is estimated that 30-60% of the assessment work requires information technology expertise. The proposed Ruling 33-8762 has done nothing to reduce this interpretation. The following comments and suggestions are provided in the hope that the scope and responsibilities for Sarbanes-Oxley can be clarified while continuing to achieve the benefits of assuring reliable financial information.

**Issue 1-** Section 103 of the Sarbanes-Oxley Act continues to be interpreted as requiring an independent opinion by the external auditors on the internal controls of the organization.

*"each registered public accounting firm shall…*
*(iii) describe in each audit report the scope of the auditor's testing of the internal control structure and procedures of the issuer, required by section 404(b), and present-…*
*(II) an evaluation of whether such internal control structure and procedures…*
*(aa) include maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;*
*(bb) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer;"*

This Section has led to the excessive involvement of the external auditors in the assessment of internal controls which has made the benefits of Sarbanes-Oxley, improved reliability and transparency of the financial reporting information, more costly. The Management Assessment (Section 404) was an integral part of the Act, requiring Management to be actively involved in the internal controls surrounding the financial reporting, yet, for fear of incurring excessive audit fees, many organizations have let the external audit firms dictate the scope and depth of the Assessments.

To rectify this situation, **it is imperative that the role of the external audit firm be confined to attesting to the competency and objectivity of the Management Assessment**, **NOT dictating the myriad of details involved in scoping and testing.**

Hopefully, this can be done through revised interpretation in SEC Rulings and PCAOB Standards, rather than waiting for a political solution.

**Issue 2-** In attempting to loosen the grip of past Rulings, the Guidance proposed is extremely vague which will do nothing to reduce the contention between the internal groups doing the Assessment of information technology internal controls and the external auditors. In many cases, this contention has been between one of the 'Big 4' doing the assessment work and another 'Big 4' firm performing the external audit. There does not appear to be sufficient detail to eliminate the individual interpretation that has been rampant to date.

There does not appear to be any consensus even within offices of the external audit firms on what constitutes adequate controls in information technology. This lack of a consistent understanding of risk in IT is magnified by the assignment of accounting trained individuals to the information technology aspects of the Assessment. As a result, we have 'war story' after 'war story' of demands made by the external auditors like testing the programming of routers, reviewing system development procedures when the financial systems are 25 years old and 'untouchable', etc.

---

**Issue 3-** Program development is rated as a critical control by many of the external auditors, either due to the comfortable nature of the work or the classical role this kind of work has played in an Audit context. It is not consequential to the Sarbanes-Oxley Assessment of internal controls because 1) no matter what the conditions were for the system development, the 'key' controls of the system must be tested for their reliability, stability and integrity and 2) most of the benefits of procedures like System Development Life Cycle (SDLC) relate to the efficient and effective use of IT resources and the process does not sufficiently guarantee results. It simply increases the probability of success.

Additionally, "operations" of information technology continues to be defined as "relevant" controls in the evaluation of ICFR (Internal Controls of Financial reporting). This term is so broad that elements such as 'help desk' controls have been included in the Assessment work. While clearly a valuable technique in some organizations to provide efficient and effective use of the IT resources, rarely would such 'operations' elements have the potential for a material impact on the organizations financial reporting.

By specifying program development and operations on page 28, Ruling 33-8762 has perpetuated this emphasis. *"Ordinarily, management should consider whether, and the extent to which, general IT control objectives related to program development, program changes, computer operations, and access to programs and data apply to its facts and circumstances."*

If this is not clarified, these "relevant" controls will continue to waste limited resources by pursuing controls which do not provide assurance of general IT controls over financial reporting.

**Issue 4-** On page 28-29 of 33-8762, it is stated that *"Documentation of the design of the controls management has placed in operation to adequately address the financial reporting risks is an integral part of the reasonable support" for its assessment.* This perpetuates the emphasis on documentation which has also been a contention point with the external auditors, both in form and content. This now appears to conflict with the PCAOB proposed Standard which has stated on page 44 that *"The absence of documentation evidencing the operation of a control is not determinative that the control is not operating effectively."*

In the assessment of internal controls of information technology, documentation is most importantly, the evidence of a functioning control NOT the design of that control which can involve severely complex logic, as in the case of operating system based controls. Frequently, documentation methods used to describe manual controls are required by the external auditors to be applied to information technology controls involving operating systems, database management systems and network controls. Controls in IT such as 'user authentication' have commonly held definitions in the IT community but may not be equally understood by the external auditors. Cases have been documented where IT procedures are required to be re-documented into a format used for manual procedures which resulted in information which was inferior to the original documentation. The result is excessive costs, diverting of resources from critical testing and the end result does not improve the understanding of the internal controls of information technology. The documentation requirements of 33-8762 should address the unique conditions in information technology and not expect that flowcharts, 'walkthroughs' and other documentation methodology for manual procedures would be appropriate.

**Issue 5-** The emphasis provided by 33-8762 on restricting the Assessment to risks of material misstatement (key controls concept) has the potential to significantly reduce the Assessment burden. On page 24-25, 33-8762 states:

*b. Identifying Controls that Adequately Address Financial Reporting Risks*
*"… the objective of this evaluation step is to identify controls that adequately address the risk of misstatement for the financial reporting element that could result in a material misstatement in the financial statements."*

The application of this principle to information technology controls will be more problematic due to the general lack of appropriate skill sets on the external audit teams. This will make risk analysis have less impact and the external auditors will most likely continue to rely upon the 'cookie-cutter' approach to assessing information technology.

In the absence of resolution of who assesses internal controls (Management or the external auditors), specific guidance is needed to remedy the lack of *"specialized skills … needed in the performance of an audit."*(¶31 of AU sec. 319) As a practical matter most external audit teams assign the responsibility for information technology to a person trained in accounting and little or no in-depth knowledge or job experience in Information Technology. Certification via a fifty dollar, two hundred question multiple-choice exam is many times used to exaggerate the level of IT skill and does not prepare

such a person for the requirements of analyzing risk and testing the complex environments of most organizations.

**Issue 6-** The chart on page 32 provides a conflicting message on risk analysis. If we are to only consider *"controls that adequately address the risk of misstatement for the financial reporting element that could result in a material misstatement in the financial statements"* then the two lower quadrants are not relevant to Sarbanes-Oxley and the note as to "Less Evidence" creates confusion over the critical concept of using risk analysis to limit scope.

As stated previously, this confusion is magnified in information technology where specialized skills are generally not available on the external audit team. This chart should be amended to support the analysis of risk of material misstatement.

---

In my opinion, the proposed guidance in 33-8762 is well meant but in the present form, continues to support a duplication of effort and responsibility between the external auditors and Management in the assessment of internal controls. Additionally, the failure to address the unique conditions in information technology continues to permeate this guidance. If not resolved, the excessive costs will not be contained and the discontent over this aspect will result in a dilution of the goals of the Act.

**Sincerely,**

**Rod Scott**
**R.G. Scott & Associates, LLC**