From: Rod Scott -RGSA [mailto:rodscott@rgscottassoc.com]
Sent: Thursday, February 15, 2007 4:32 PM
To: Comments
Subject: PCAOB Rulemaking Docket Matter No. 021

Office of the Secretary
Public Company Accounting Oversight Board
1666 K Street, N.W.
Washington, D.C. 20006-2803
PCAOB Rulemaking Docket Matter No. 21

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 research and consulting experiences.

In general, the individuals assessing the IT controls have had to interpret the implications for information technology from the PCAOB Standards and SEC 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 Standards have done nothing to bridge this gap. 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.

Proposed Standard: *"**An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements**"*

Issue 1- Section 404 of the Act states *"each registered public accounting firm that prepares or issues the audit report for the issuer **shall attest to, and report on, the assessment made by the management of the issuer.**"*

The intent of this Section of the Act, clearly, was to require Management to understand their internal controls and provide assurance to the investors that the internal control of the organization resulted in accurate and reliable financial information.

The external auditors' role has been interpreted by PCAOB to be responsible for an independent audit of the internal controls of the organization, rather than attesting to and reporting on the assessment made by Management.

Section 103 of the Act states that *"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 audit fees for Sarbanes-Oxley which has subliminated the benefits of improved reliability and transparency of the financial reporting information.

In the Information Technology area, Section 103 has been responsible for innumerable tests, required by the external auditors, which do not contribute to Managements' understanding of their 'key' internal controls. External auditors have required the programming of routers to be tested, reviewed system development procedures when the financial systems are 25 years old and many other 'war stories' too numerable to mention.

This proposed Standard continues to make the public accounting firm responsible for assessing the internal controls of the business which is an interpretation of Section 103 and not supported by Section 404 of the Act. Instead, a more reasonable interpretation of the Act should require the public accounting firm to attest to the assessment made by Management. This is the single most costly impact of Standard No. 2 and has not been rectified in the proposed Standard. It has created excessive fees by the public accounting firms and has caused Management, in many cases, to incur excessive costs in trying to satisfy the inconsistent requirements of the public accounting firms. If not addressed, organizations face two internal control reviews, one by Management and one by the external audit firm. This will continue to impose excess costs on the process.

The proposed Standard should be amended to require only the attestation to the Management Assessment and not require an independent appraisal of the internal controls of the organization by the external auditor.

Issue 2- Additionally, the proposed Standard has been generalized and much of the detail in Standard No. 2 was eliminated. One of the major cost drivers to date has been the inconsistent interpretation by the external auditors of the requirements. It is certain that if the Standards continue to lack detail on critical issues the amount of interpretation done by the external auditors will increase and, if their role is not changed as suggested above, the costs of the Sarbanes-Oxley assessment will not be reduced.

Issue 3- The emphasis on the importance of risk assessment is the major improvement in the proposed Standard. While it is supported in the proposed Standard and in SAS No. 109 it is only discussed at a very general level. The 'devil is in the details' as far as information technology is concerned.

¶31 of AU sec. 319 states *"The auditor should consider whether specialized skills are needed in the performance of an audit."* 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. Even certification via a fifty dollar, two hundred question multiple-choice exam does not prepare such a person for the requirements of analyzing risk and testing the complex information technology environments of most organizations. This makes the achievement of meaningful risk analysis difficult. As a result, the auditor tends to follow a prescribed set of controls rather than apply ¶15 and ¶31 of AU sec. 319.

The proposed Standard does not provide an adequate level of guidance for assessing information technology risk. The staffing of the external audit teams is unlikely to change so the risk analysis of information technology will likely remain contentious and continue to be responsible for excessive costs.

Issue 4- The SEC definition of internal controls, in Ruling 8238, states *"… our definition of the term "internal control over financial reporting" reflected in the final rules encompasses the subset of internal controls addressed in the COSO Report that pertains to financial reporting objectives. Our definition does not encompass the elements of the COSO Report definition that relate to* ***effectiveness and efficiency*** *of a company's operations and a company's compliance with applicable laws and regulations, with the exception of compliance with the applicable laws and regulations directly related to the preparation of financial statements."*

Standard No. 2 did not recognize this exclusion in it's' definition of internal control and this has driven behavior in the assessment of information technology internal controls. Standard No. 2 included this statement:

"50. Some controls (such as company-level controls, described in paragraph 53) might have a pervasive effect on the achievement of many overall objectives of the control criteria. For example, information technology general controls over ***program development, program changes, computer operations, and access to programs and data*** *help ensure that specific controls over the processing of transactions are operating effectively."*

This section has been interpreted as **the definitive statement** on Information Technology General Controls, yet "program development" and "computer operations" are vague terms from a financial reporting perspective and are primarily issues of effectiveness and efficiency, which contradicts the SEC Ruling 33-8328.

The ISACA organization used this interpretation as the basis for the General Controls in their white paper “IT Control Objectives for Sarbanes-Oxley”. Price Waterhouse Coopers interpreted this wording similarly in their monograph “Sarbanes-Oxley Act: Section 404, Practical Guidance for Management July 2004”. KPMG similarly endorsed this concept in their document "Sarbanes-Oxley Section 404: An Overview of the PCAOB's Requirements". Deloitte has endorsed the PCAOB definition in its document, "Taking Control". Due the broad base of these organizations, a major impact has resulted on the Sarbanes-Oxley assessment effort throughout the country.

The proposed Standard no longer contains this statement but neither does it clarify that issues of efficiency and effectiveness are out of scope. This exclusion of efficiency and effectiveness issues requires emphasis in the proposed Standard to assure that the attestation to Management’s Assessment does not continue to suffer from the scope ‘creep’ that has occurred due to the application of a broader definition of “internal control”.

Issue 5- Standard No. 2 put a false reliance on SAS 70 reports and this has been continued in the proposed Standard. The Information Technology services that organizations use today vary from simple payroll functions to the complete outsourcing of hardware, software, security, etc... In many instances these services are provided by a service organization to hundreds, sometimes thousands, of clients. It is reckless to assume that a single sample of controls (SAS 70), by a CPA, could satisfy the assessment of all of the clients’ controls over financial reporting in a heterogeneous environment that characterizes most IT services organizations. Yet, B19-29, in the proposed Standard, continues to ignore this major problem. Instead, simple but infeasible alternatives are prescribed which have generally meant that internal controls over IT at service organizations is not subject to the same rigorous requirements that would be expected if the processing were done within the organization.

Proposed Standard: *“Considering and Using the Work of Others in an Audit”*

This entire proposed Standard supports the assessment of internal controls by the external auditor. As discussed above, this activity is interpreted as a requirement of the Act and the focus should be redirected to attesting to the Management Assessment of internal controls. The elimination of the requirement for principal evidence was a good start but there is a need to go further and eliminate the need for an internal control review by the external auditor under Sarbanes-Oxley.

The proposed Standard has an inappropriate tone to the view of the work of others. In the code of conduct example, competency and objectivity, by those assigned from the organization, allows the external auditor to rely on the determination of the existence of the code of conduct but NOT the judgment on how it is applied. If competency and objectivity are adequate, then judgment should be reliable as well. In the information technology assessment work, quite often the individual assigned by the organization is

the only competent individual to assess controls in their area of responsibility, such as a network engineer.
In my opinion, the proposed Standards are an improvement over AS2 but in their present form, will not achieve the goal of eliminating excessive costs of Sarbanes-Oxley Assessment of internal controls.

Sincerely,

Rod Scott
R.G. Scott & Associates, LLC
555 Ben Franklin Dr Unit 4
Sarasota, FL 34236
rodscott@rgscottassoc.com
941-388-9827

Rod Scott
R.G. Scott & Associates, LLC
Phone: 941-388-9827
rodscott@rgscottassoc.com
www.rgscottassoc.com