April 8, 2006

Sirs:

I am a consultant for the Institute of Internal Auditors, teaching seminars on the subject of assessing general controls in Information Technology for Sarbanes-Oxley. I have taught over 25 of these seminars in the past two years. One of the major issues I have tried to help the attendees understand is the impact of SEC Ruling 33-8328 on the scope of the Sarbanes-Oxley assessment for Information Technology General Controls. The Ruling states:

"We recognize that 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."*

This position was further strengthened in the SEC's "Staff Statement on Management's Report on Internal Control Over Financial Reporting" (Section F. Information Technology Issues, *Information Technology Internal Controls*), dated May 16, 2005.

"In establishing the scope of its IT assessment, management should apply reasonable judgment and consider how the IT systems impact internal control over financial reporting. Because Section 404 is not a one-size-fits-all approach to assessing controls, it is not possible for us to provide a list of the exact general IT controls that should be included in an assessment for Section 404 purposes. However, the staff does not believe it necessary for purposes of Section 404 for management to assess all general IT controls, and ***especially not those that primarily pertain to the efficiency or effectiveness of the operations of the organization*** *but are not relevant to financial reporting."*

This exclusion of issues, which affect the "effectiveness, and efficiency of a company's operation" can have a dramatic affect on the scope of the work required to assess an organization's internal controls in the area of Information Technology General Controls and the resulting costs.

The exclusion of effectiveness and efficiency allows us to eliminate some elements of the Information Technology environment from our Sarbanes-Oxley assessment such as how a program is developed or how the operations division of Information Technology provides service to their customers. To be sure, these are important issues to Management but relate primarily to the efficiency or effectiveness of the organization and, therefore, are not required to be assessed for compliance based on SEC Ruling 33-8328.

In terms of the Information Technology framework, CobiT, this exclusion of effectiveness and efficiency reduces the high-level control objectives required to be assessed from thirty-four separate objectives to those twelve, which relate primarily to the information criteria of Confidentiality, Integrity, Availability, Compliance and Reliability. Based on this logic, following are the resulting CobiT high-level control objectives that may require assessment based on relevance to Sarbanes-Oxley. Risk associated with the issuing organization may further reduce the control objectives required.

PO 8 – Ensure compliance with external requirements
PO 9 – Assess risks
PO 11 - Manage quality
AI 6 – Manage changes
DS 5 – Ensure system security
DS 6 – Identify and allocate costs
DS 11 - Manage data
DS 12 - Manage facilities
M 2 – Assess internal control adequacy
M 3 – Obtain independent assurance
M 4 – Provide for independent audit

However, PCAOB Standard No. 2 included the following wording:

"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 is being interpreted as the definitive statement on Information Technology General Controls, by the 'Big Four', yet "program development" and "computer operations" 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" (see pages 51, 65-67). Due the broad base of these organizations it can be assumed that a major impact has resulted on the Sarbanes-Oxley assessment effort throughout the country. Many of the companies attending my seminars have been guided by their external auditors to use this defacto standard and are not open to frameworks, which are more relevant to Sarbanes-Oxley Section 404 and the risks existing in the issuing organization.

The result of using these four areas as the basis for the IT General Control assessment is that effort will be spent assessing controls which impact the effectiveness and efficiency of an IT function but do not contribute directly to the accuracy of the financial reporting.

In addition, due to resource and time constraints, this focus will reduce the effort and attention to control issues that more directly relate to financial reporting accuracy.

As an example, issues of program development methodology (such as are contained in the System Development Life Cycle) may result in inefficiencies in the development and support of the systems but assessing this process does not eliminate the need to verify the accuracy of the resulting system through an application control review and the financial reporting review. Any time spent by the Assessment team or the external auditors contributes only to knowledge of the probability that the systems are accurate, reliable and stable not the verification of those conditions. Program development methodology, therefore, is a Management issue but not Sarbanes-Oxley control weaknesses under the referenced SEC Ruling 8328.

Yet, I have heard from many companies that the external auditors spend significant effort or require significant effort of the issuing company to review areas of program development. In some cases, reviewing development activities when the financial reporting is done by a 20 year-old 'legacy' system, which is never modified or reviewing program development activities of a new financial system which is not being used to provide the current financial reporting.

This conflict, caused by PCAOB Standard No. 2, has been discussed with PCAOB and, as shown in the SEC Staff Statement above, is supported by the SEC. However, there has been no recognition of the problem caused by this Section 50 of the Standard and ISACA 'whitepaper' continues to be used by the external auditors as the defacto standard for IT general controls.

This problem will severely impact small businesses as they begin to plan their Assessment activities for 2007. Most of these companies do not have internal audit functions for Information Technology and will probably have severe resource, time and skill set limitations in the area of Information Technology. It is critical that PCAOB reconsider the statement in Section 50 of the Standard and redirect their emphasis base the scope of general controls for Sarbanes-Oxley on controls which primarily impact reliability, availability (of financial systems), compliance (with Sarbanes-Oxley), integrity and confidentiality (which supports integrity of information).

I stand ready to provide whatever additional discussion or explanation is needed to clarify and resolve this apparent conflict.

Thanks for your consideration.

Rod Scott
R.G. Scott & Associates, LLC