I am a consultant for the Institute of Internal Auditors, teaching a seminar entitled "Sarbanes-Oxley Act: The Impact on Information Technology". I have taught this seminar over 17 times for over 400 companies. 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 exclusion of issues, which affect the "effectiveness, and efficiency of a company's operation" has 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.

The exclusion of effectiveness and efficiency allows us to eliminate some elements of the Information Technology environment from our Sarbanes-Oxley assessment such as the techniques for 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 are, therefore, 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 require assessment.

PO 8 – Ensure compliance with external requirements
PO 9 – Assess risks
PO 11 - Manage quality
AI 6 – Manage changes
DS 4 – Ensure continuous service
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 has been interpreted as **the definitive statement** on Information Technology General Controls, 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" (see attached document, pages 7 and 8). 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". In practice, I have been involved with E&Y auditors who utilized the ISACA white paper, directly. 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.

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. However, the accuracy of the resulting system will be verified through testing of the application, **regardless of the method of development**. Program development methodology, therefore, is a Management issue but not Sarbanes-Oxley

control weaknesses under the referenced SEC Ruling. My seminar attendees have related many situations where current development activities were audited even though the financial reporting systems were developed years ago or in some cases were being developed for future use and, therefore, not impacting the current financial reporting.

I have discussed this conflict between the PCAOB Standard No. 2 and the SEC Ruling 33-8328 representatives of the SEC and PCAOB. The SEC personnel agree that the SEC Ruling clearly excludes controls (including IT General Controls), which relate to effectiveness and efficiency of the operation of the organization. The PCAOB representative , however, failed to see the importance of this issue and further stated that no one she had talked to brought up the concern. This may indicate a problem that PCAOB does not have any Information Technology representatives focusing on this extremely important element of the Sarbanes-Oxley internal control assessment.

I believe this issue is of considerable importance and should be resolved with the publication of Implementation Guidance. 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