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 45 times, involving over 800 companies. My comments, in response to your solicitation June 15, 2007, are drawn from the experiences of these organizations and my own consulting experiences.

Specific comments:

1) AS5 does not provide guidance to auditors as to how to apply to control weaknesses that are defined in the Information Technology areas. In general, IT weaknesses can have considerable albeit indirect impact on materiality but as with other areas there is no recognition in the Standard of the differences between financial and IT weaknesses. Examples of IT weaknesses could provide baselines for the auditor.
2) Since the auditor should only be testing areas which can result in material misstatement, significant deficiencies encountered should be a by-product not a diversion.
3) It seems clear that multiple deficiencies are additive only if they are related or can interact. However, in the IT area the auditor frequently does not have enough experience to understand whether/how the deficiencies can interact.
4) The terms "reasonably possible" and "probable" are open to individual interpretation. This is another area where the lack of IT experience by the auditor has resulted in ultra-conservative, personal interpretation rather than risk-based judgment.
5) AS5 has perpetuated the notion that even if the work of others is done by competent and objective individuals, the auditor must perform the work in areas involving judgment. This may be defensible in issues of accounting since the auditor must have the requisite education and certification in this area. However, in issues of Information Technology the work of others has been done by individuals with considerably more experience and knowledge than the auditor so that auditors are not qualified to exercise better judgment. The Standard should recognize this difference in qualifications in IT related matters when defining conditions governing the use of the work of others.
6) Studies have indicated that smaller companies have recently experienced increased audit fees averaging more than 40% prior the application of SOX related effort. The impact on smaller public companies will depend on the avarice level of the external audit firms in the area of fee generation.
7) AS5 does not encourage auditors to scale audits through the establishment of minimum requirements. Therefore, there we can expect inconsistent scaling based on individual interpretation and conservatism. This is, again, particularly true in the area of Information Technology controls which have no level of detail discussed in AS5. Even worse would be the definition of non-critical or marginally important IT controls, which occurred in AS2 and drove excessive costs due to adoption of paragraph 60 as a basis for a defacto standard. Instead, smaller organizations need a 'top-three' list that would assure that critical controls affecting financial reporting would be assessed without overly burdensome cost.

> Experience has shown, for instance, that areas of access security, change control and data access are included in most SOX assessments and could form the nucleus of a minimum standard. Establishing a minimum set of critical controls for smaller organizations, based on the input of experienced Information Technology individuals would greatly assist the CFOs of smaller organizations who may not have Internal Audit or IT resources to analyze risks and define critical controls in their IT areas.

Overall, I do not believe AS5 is consistent with the intent of the Act. With respect to Section 404, the Act intended to encourage Management to focus on the internal controls of the financial reporting, if not the business, in general. The role of the external auditor is needed to assure that this Assessment by Management can be relied upon by investors. However, the Standard continues to define a larger role for the external audit firms which has driven the excessive costs, experienced by most firms.

As indicated in the above requested responses, AS5 has continued the direction of not providing specific, informed guidance related to Information Technology. AS2 was mute with respect to the significant differences in approach and qualifications between the financial reporting assessment and the IT assessment of internal controls. Meanwhile, studies have indicated between 21% and 60% of the ongoing SOX effort is IT related. The result has been, and will continue to be, that requirements are mandated in the IT area by the external auditors which consume the scarce resources, available to do IT assessments, but do not significantly add to Management's understanding of their IT 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