Comments on guidance for companies

Here are some observations and suggestions applying to both the draft guidance from the SEC and the draft AS2 from the PCAOB.

1) Quantitive vagueness

Despite the new guidance the amount of work needed by companies and their external auditors, and the assessment of controls reached, will continue to depend on negotiation rather than definition.

The guidance writes as if COSO's internal controls framework defines effective control, but it does not. It lists things to consider, but it does not quantify what should be in place in such a way as to provide a definition.

It is analogous to defining a "Long" piece of string without ever saying exactly how long a piece of string has to be to be considered "Long". Trying alterative phrases and referring to existing pseudo-definitions does not solve the problem.

This is consistent with the conventional approach of external auditors, but there are examples of regulatory regimes that have defined such things as billing accuracy using precise numbers, showing that it can be done using well known statistical techniques.

Progress should be made towards quantifying the requirements.

2) Technically narrow guidance

The guidance explicitly calls for assessing two things: (a) the design of the control system, and (b) the operating effectiveness of controls within it. Operating effectiveness is considered one control at a time and focuses one whether the control is being carried out as originally designed.

While these assessments are relevant and likely to form a part of any competent evaluation there are other approaches that can be used as well and are used by sophisticated companies and their auditors. The drafts as they stand leave sophisticated companies and their auditors with the impression that some of their most useful techniques are ignored or even contrary to the official requirements.

Other approaches that can be useful, and highly efficient in the right circumstances, include:

- Putting test transactions through a system and measuring the error rate.
- Collecting and analysing figures on discovered errors and backlogs.

- Testing the reliability of those figures using analytical tests.

- Gathering evidence to confirm initial views about inherent risk levels. (E.g. if inherent risk from software changes is thought to be low this can be confirmed by looking at records of software changes or comparing files.)

In addition, the guidance describes an approach that is intended to be top down and risk focused, but only achieves that to a limited degree. Again, people who have already learned to employ more whole-heartedly risk focused, responsive methods could feel their skills are ignored or contrary to the requirements. For example, before 2002 PricewaterhouseCoopers adopted an audit approach globally called "Towards Performance Audit" that involved continuous planning throughout the audit as teams shared the results of every meeting and set of tests, as input to planning the next steps.

The methods of more sophisticated companies and auditors should at least be recognised and given approval in some way, even if detailed guidance is not feasible. This would allow and even encourage people to move towards more effective and efficient evaluations.

3) Attestation on management's assessment

Before 2002 external audit firms assessed internal controls to the extent that they thought it a contribution towards more efficient auditing of financial statements. The major value of sections 404 and 302 was to focus on what *management* should be doing.

Removing the requirement for auditors to comment on management's evaluation lessens the focus on management's activities and cements the idea of an external audit of ICFR.

Now is the time to reconsider the case for an external audit of ICFR. Over the last two years it has become increasingly clear that management have access to information that external auditors do not have, and can therefore put in place an efficient, integrated evaluation as part of normal monitoring activities.

Just asking the external auditor to audit ICFR directly is asking the auditor to do something that has never seemed worthwhile in the past. However, asking the auditor to review management's evaluation is quite different because of the special qualities of management's evaluation and the importance of getting management to do things themselves.

Far from taking the focus off management's evaluation we should be increasing the focus on it and removing the requirement for an external audit of ICFR.