
From: Matthew Leitch [m.leitch1@ntlworld.com]
Sent: Saturday, November 08, 2003 8:36 AM
To: Comments
Subject: Docket 008

A more modern audit technique would be more efficient and effective

The proposed rule shares a significant deficiency with the AICPA's guidance on the same topic which had previously been influencing companies' approaches to SOX 404 compliance. Its audit approach to internal controls is rather old fashioned, being based on the old model of control objectives, controls, and tests of the operation of controls.

An audit approach based on more modern ideas of risk assessment and management, and a wider understanding of "testing" would produce more convincing evidence of controls effectiveness at lower cost to everyone.

An evaluation based solely on assessing design effectiveness and operation of individual controls is unreliable because it is extremely hard to assess design effectiveness accurately. Inherent error and fraud rates are hard to estimate to within an order of magnitude and it is very easy to be surprised by obscure and indirect errors and frauds. In practice, when control systems are designed it is vital to gather and study information on actual errors and frauds discovered and modify the design.

The rules should emphasise the importance of direct evidence of the effectiveness of controls from statistics about actual errors and frauds discovered. This might be done by expanding the concept of testing and by commenting on the value of direct evidence in other parts of the document. This should be presented as one more form of evidence that could be used, rather than a requirement. The principle involved is already in the rule, where it says that mis-statements found during audit of the financial statements should be considered when assessing the effectiveness of internal controls.

The main benefit would be with large scale financial processes, which is where the main costs of audit lie. With these many companies should be able to provide *measured effectiveness* to back up their assessments of their control activity. Work that might have taken weeks can be done more effectively in days.

There are a number of limitations and points to consider. They are explained in my document: "Sarbanes-Oxley Act section 404 and 302: *efficient* compliance (updated)" which is at <http://homepage.ntlworld.com/m.leitch1/icd/effectiveness/index.html>.

Matthew Leitch
Matthew Leitch Associates Limited

About the author of this comment

Matthew Leitch is an independent consultant in risk management and internal control. Until late 2002 he was an internal controls specialist and external auditor with PricewaterhouseCoopers. His experiences on an early SOX 302 project for a major US company convinced him that there was a better way to do the reviews than relying exclusively on documenting and testing operation of individual controls.