

COMMENTS ON THE PROPOSED AUDITING STANDARD AN AUDIT OF INTERNAL CONTROLS OVER FINANCIAL REPORTING

General Comments

This is a powerful document that should do much to deter, as well as detect the frauds and related behaviors that have been so costly to investors and have weakened confidence in the securities markets. Its strength is that it is comprehensive and definitive, and that it adds important new control features such as walkthroughs, Audit Committee oversight and attention to fraud controls.

The critical specific comments that follow are intended to improve an already strong document.

Framework Used by Management

Paragraph 14 and Appendix A illustrative reports

COSO and professional standards make it clear that financial reporting controls do not prevent or detect indirect effects on the financial statements of violations of laws and regulations or problematic operating controls. They also place limitations on the inclusion in financial reporting controls of those controls that are related to the acquisition, use and disposition of assets. The audit report should make these limitations clear to the public.

Reasonable Assurance

Paragraphs 16 and 18

Existing auditing standards do not state that "reasonable assurance" means "a high level of assurance". SEC Release 33-8238 does not define that term. Heretofore, the term "reasonable assurance" has been open to interpretation and a high level of assurance may not have always been sought, much less achieved.

Because management is not bound by this auditing standard, management might apply a lesser standard than "high". This potential problem should be dealt with by stating clearly that auditors will not affirm management's assessment of internal control effectiveness unless the auditor has a "a high level of assurance" that controls are effective.

Paragraph 153(h) and Appendix A illustrative reports

The scope paragraph should use the words "a high level of assurance" rather than "reasonable assurance".

Fraud Considerations in an Audit of Internal Control

2

Paragraphs 24 through 26

This standard should forge a stronger link to the fraud standards in AU 316 (or preferably SAS 99). This is needed because the fraud standard discusses control risks and those risks should be addressed early on in the audit of internal control. A minimum step would be to state that attention to the fraud risk factors mentioned might help to identify the controls to be tested and that high levels of fraud risk should increase the extent of controls testing.

It would be helpful to reference SAS 99, paragraphs 51 through 67.

Management Fraud

A separate section of the standard should deal with the internal control issues related to this pervasive cause of the financial statement restatements of recent years. Low level fraud or error is not the reason the Sarbanes Oxley Act was passed.

Under certain circumstances the auditor should intensify the auditing of controls related to the prevention or detection of management fraud and should exercise a heightened degree of professional skepticism. If the auditor has a high level of concern about management behavior, the auditor should consider whether and how to use forensic techniques to uncover management fraud.

The following are some of those circumstances:

- Weaknesses in Paragraph 24 controls point toward management
- Walkthrough discussions with company personnel have identified concerns about management, or find that control personnel are vulnerable to manipulation.
- There are unexplained discrepancies in the accounting records, unexplained conflicting or missing evidential matter, or serious problematic relationships between the auditor and management
- Unauthorized transactions involving management have occurred
- The auditor has concerns, even concerns that are intuitive, about management bias, integrity or ethics.

Authorization of Transactions

A separate section of the standard should deal with control issues related to authorization of transactions. Proper *authorization of receipts and expenditures* and *detection of unauthorized acquisition, use and disposition of assets* are imbedded in the definition of internal control.

The standard should require the auditor to consider the levels of authority appropriate for the authorization of the various types of transactions, the circumstances in which explicit authorization should be required, and the need for documentation of explicit approvals.

2

Examples of areas where effective authorization controls are especially important should be cited. Those include general ledger entries, transactions involving management or management compensation, changes in sales or loan terms, speculative derivative transactions, transactions subject to 8K reporting, and changes in computer systems.

Foreign Operations

Paragraph 39 or elsewhere

Mention should be made of the fact that the personnel of business units located outside the United States may sometimes lack comparable ethical standards and knowledge of US accounting standards, and therefore control risks are likely to be higher. The control and accounting requirements of the Foreign Corrupt Practices Act have not eliminated these higher risks.

Risk Assessment

Paragraph 50, 102 or elsewhere

More should be said about how:

- The auditor should use management's risk assessment
- The auditor should pursue his or her own observations about risk
- The level of risk should affect the selection of controls to be tested and the extent of testing.

There is specific guidance on identifying controls to be tested in the proposed standard. This may incorporate risk-based judgments by the draftsmen of the proposed standard. But, the auditor's judgment of risk should be another important determinant of the controls to be tested, and risk should always be considered in deciding on the extent of testing.

If risk of misstatement is a concern and control effectiveness is to be judged solely on the basis of tests of transactions, some additional guidance on the extent of testing should be included in the standard. When testing repetitive processing of transactions, the auditor should be required to sample at least enough transactions to detect, with a high level of confidence, one error if there are any errors in the process.

Audit Committee Effectiveness

Paragraph 56

The nature and extent of the relationship between the auditor and the Audit Committee enables the auditor to identify some of the conditions that indicate significant control deficiencies, but does not permit an affirmative conclusion about oversight effectiveness. This limitation should be more clearly stated. It is also necessary to state that the

auditor's responsibility to investors and other users of audit reports is paramount, and that functional responsibility to the Audit Committee should not interfere with nor limit the auditor's evaluation of conditions that indicate the possibility of significant control deficiencies.

Paragraph 57

The following should be added to or integrated with the bullets in the proposed standard:

- Level of involvement with the fraud controls mentioned in Paragraph 24, especially those that the Sarbanes Oxley Act and listing standards make the Audit Committee's direct responsibility, e.g. handling complaints.
- Level of concern with the scope of audits, and the degree of follow-up on the findings and recommendations of the auditors.
- Responsiveness to issues raised by the auditors, including those required by auditing standards to be communicated to the Audit Committee
- Level of involvement in accounting for complex transactions and in reviewing related party transactions.
- Competence of Audit Committee members, i.e. all members should be at least "financially literate" as defined by the 1999 Blue Ribbon Committee and one or more members should qualify as an "audit committee financial expert" as defined by SEC rule.

Paragraph 58

While laudable in its objective, this paragraph is not sufficiently operational in its present form. More should be said about how Audit Committee members' actions indicate lack of independence. And, what is said about the process of selecting members should be modified. The comments on the process are true, but the examples suggest processes that may not always be good indicators of independence. Qualifying words are needed. Also, "friends" should be replaced by a broader statement, such as the one in the third sentence of the following paragraph.

Listing standards establish a number of rules for independence, but otherwise give the Board of Directors the responsibility for making the independence determination. If the rules are not observed, that alone may indicate a lack of independence. Not addressed by the rules are the economic and interpersonal relations between company officers and directors unconnected with their company roles that can compromise independence. Auditors may learn of these relationships and should take them into account in evaluating the independence of Audit Committee members. But these relationships, without other evidence, are not ordinarily sufficient to conclude that there is a lack of independence.

Actions of the Committee can reinforce concerns about relationships. Or, actions alone may be sufficient to conclude that there is a lack of independence. Auditors may observe that members are unduly deferential to management, and auditors are often in position to observe Audit Committee members' reactions and follow up when issues involving management arise. Especially significant is lack of concern and follow up by members to those issues where the CEO or CFO may obtain an actual or potential economic benefit and there is a hint of bias or of questionable ethics or integrity.

Paragraph 59

Significant deficiencies should be communicated in writing to the full Board of Directors.

Information Technology and its Effect on Internal ControlParagraph 70 and elsewhere

Paragraphs 16 through 20 of AU 319 referenced in paragraph 70 describe some of the risks and other challenges an auditor faces in a computer environment. But these AU 319 paragraphs are not very helpful. Guidance elsewhere in the proposed standard indicates the importance of general controls, but doesn't deal with other control issues. Paragraph 107 appears to overstate the reliance that may be placed on general controls. Additional references should be made to AU 319.30 through .32, AU 319.68 and .69, AU 319.77 through 79, and AU 319.110.9. These paragraphs provide a better picture of the important control issues and what the auditor might do.

Because of the critical and overarching importance of IT controls in many companies, the auditor should seek to obtain a high of confidence in the design and operation of computer controls. These should normally include accounting related application controls as well as general controls. The standard should require the use of computer auditing techniques in most situations and, when complex systems are encountered, the use of experienced IT auditors to make the controls evaluation

Performing Walkthroughs and Related Documentation RequirementsParagraphs 79 through 83, and Paragraph 145 and elsewhere

The following ideas for improvement should be addressed:

- In following the process flow the auditor will encounter computer processing. In order to understand the flow it may be necessary to reprocess the documents that the auditor is using in the walkthroughs through the computer system.
- In tracing events, the auditor will need to understand how events that should lead to accounting are first identified, and whether that identification is timely.
- The potential for collusion, falsified documentation and controls override makes management fraud and unauthorized acts the most difficult control problem facing the auditor. Questioning company control personnel is an audit tool that should not be neglected. The questions in Paragraph 81 that the auditor may ask should also include whether control personnel think the controls they administer are effective, whether they have ever questioned the authenticity of documents and approvals, and whether they have ever been asked to overlook a control violation. This kind of questioning can be a very effective test and can help the auditor to identify management fraud. If these questions are included in the standard, auditors will be more inclined to ask them and potential management objections to the questioning will be muted.

- In tracing events and transactions auditors may find that there are insufficient accounting controls in one or more areas. In which case, auditors should explore whether adequate control is established by operating or compliance controls. But, in so doing the auditor should keep in mind that these controls may operate less stringently than accounting controls. In these situations the auditor should be alert to the possibility that operating personnel may be involved in collusion and/or creation of false documentation.
- Walkthroughs will expose the auditor to the economics of the business and provide an opportunity to determine or help to determine the substance of transactions
- The walkthroughs of processes are essentially systems evaluations and systems can be complex. Some companies will use computer-assisted techniques to document transaction flows, control points and related controls, and the control improvements needed. Others may use manually prepared flow charts with similar information noted on them. The auditor may find this documentation useful as a starting point for the audit. Other companies will rely on narrative descriptions that may not be satisfactory when systems are complex. The auditor should be prepared to utilize advanced documentation techniques that show (a) the control points, control objectives and related risks, (b) the controls in place and the tests made, and (c) the findings on effectiveness.

Signing the Auditor's Report

One member of the PCAOB suggested that the audit partner and the concurring partner sign the audit report. This would strengthen the sense of responsibility of those who make the ultimate decisions on how to apply this standard. It would also help to focus legal liability for a false report. This suggestion should be adopted by PCAOB.

Donald H. Chapin, CPA
October 31, 2003

Contact information

FAX: DonChapin@worldnet.att.net

Phone: 914-921-9003 until November 17

239-593-8533 after November 19