DON M. PALLAIS, CPA 14 Dahlgren Road Richmond, Virginia 23233
Telephone: (804) 784-0884
Fax: (804) 784-0885

November 18, 2003

Office of the Secretary
PCAOB
1666 K Street, NW
Washington, DC 20006-2083

Re: PCAOB Rulemaking Docket Matter No. 008

Gentlemen:

The proposed standard on auditing internal control is an ambitious attempt to forge comprehensive standards under the time pressure of a Sarbanes-Oxley-imposed deadline and the PCAOB is to be commended on the attempt. However, while the draft is an excellent approach to implementation guidance, it tries to accomplish too much. It attempts to set standards, make recommendations, suggestions and observations, and provide examples regarding auditing internal control; set standards for a financial statement audit; and even set standards for management.

To be successful the standard must be consistently read, understood, and implemented by practitioners, which requires a clear conceptual cohesiveness that establishes as standards only those matters that are critical to the public interest. Including additional implementation guidance, as this does, lengthens the document and diffuses the message, raising the risk that practitioners will view it as a list of procedures rather than the core of a professional service. Accordingly, I suggest the draft be pared back to those elements that are necessary for standards for audits of internal control. This would allow readers to focus on the important issues involved and allow the PCAOB to direct its full attention to setting this important standard.

Scope of the Standard

The draft proposes to establish a lot of standards in addition to the core issue. Unless you have a highly effective plan for issuing, codifying, and cross-referencing the standards, there is a significant danger practitioners will not find or focus on these new requirements. For example,

- The discussion of independence in ¶ 33-34 seems out of place here. I'm not sure a practitioner would ever think to look for a discussion of independence in this standard. If this is intended merely to reiterate rules contained elsewhere, it is redundant.
- Paragraph 139 amends SAS No. 56, with absolutely no rationale for the change has no connection with an audit of internal control. It appears to change the requirements

for analytical procedures only for auditors who are also reporting on internal control. I think practitioners are unlikely to realize it is here.

- Paragraph B32 adds requirements to those already in SAS No. 70. Again, the need for the change is not clear and the placement of this requirement will not make it readily apparent.
- Paragraph 138 is subtly, but significantly, different from SAS No. 55 (as amended) without explanation or justification.
- The illustrative combined report in Appendix A-6 indicates that audit reports will no longer refer to GAAS. This seems to be a significant issue that users would be interested in commenting on. However, the draft does not draw attention to this provision or to the implicit revision of SAS No. 58. It's also not clear why the change is necessary. One possibility is to differentiate the PCAOB's standards from AICPA-issued GAAS. But, of course, both FASB and GASB standards are called GAAP without any apparent confusion.
- Paragraphs 33, 173, and 184 all seem to set standards for management, which would appear to be beyond PCAOB's authority.

Criteria

The draft calls for the use of a suitable framework, consistent with the existing attestation standards. But then it calls into question how one judges suitability.

It says the COSO framework is suitable but then adds criteria not found in COSO, suggesting COSO doesn't meet the completeness attribute in ¶ 12. The specific audit committee requirements in ¶ 57 and the documentation requirement in ¶ 43 do not appear in COSO. The draft calls a failure to adhere to the additional requirements a deficiency, which is described in the report as a failure to comply with COSO even though COSO does not specify them.

The draft (¶ 13) says that other criteria might also be suitable. In fact, the PCAOB apparently has identified other suitable criteria ("other suitable criteria have been published…") but has chosen not to tell us what they are, leaving it to the auditor to figure out which ones have already passed muster. It would be more helpful if the draft explicitly named the suitable criteria. Instead, the auditor has to judge other criteria using the attributes articulated in the draft. Two of the attributes as described are likely to cause problems:

- The criteria must be published by a body of experts that followed due process procedures, including the broad distribution of the framework for public comment. The requirement for broad distribution, which had been in SSAE No. 1 was dropped in SSAE No. 10. Ironically, one of the considerations was a concern as to whether the distribution of the COSO draft was sufficiently broad to fulfill this requirement. It is also difficult for a practitioner after the fact to determine how broadly a draft was distributed by the body of experts. It also raises other questions, such what does distribution mean? Simply making something available on the internet is not the same as distributing it.

- The criteria have to encompass, in general, all the themes in COSO in addition to being sufficiently complete (the third bullet in ¶ 12). COSO identifies components, objectives, factors, issues, and points of focus. But I don't know what the themes are. The draft should direct the reader to them so the practitioner can determine if all the themes are addressed.

Internal Control Deficiencies

The concept of significant deficiencies is problematic. A deficiency (¶ 7) is a factor that does not allow (that means, I suppose, *prevents*) management from preventing or detecting misstatements on a timely basis. The examples in appendix B do not prevent the entity from achieving its objectives, but merely don't ensure it. I suspect this paragraph meant something like "does not assure prevention or detection." Paragraph 8 defines *significant deficiency*, saying it "could be [a single deficiency or combination of deficiencies] that results in more than a remote likelihood that a misstatement … that is more than inconsequential in amount will not be prevented or detected." I suspect the use of "could be" was meant to indicate that the deficiency could be either single of a combination, but as written it says that it could be something that results in an undetected misstatement.

Beyond these editorial matters, however, there are significant conceptual questions about characterizing deficiencies.

- Effective internal control only yields reasonable assurance—that is, a relatively low risk that material misstatements will not be prevented or detected on a timely basis. On the other hand, the borderline for significant deficiency is remote possibility, which I interpret to be far less likely than reasonable assurance. (The draft takes one term from the auditing literature and another from the accounting literature, making comparability difficult.) Combining this with an extraordinarily low materiality cutoff, inconsequential, substantially lowers the threshold. The goal of effective internal control, then, is an acceptable level of risk that's a quantum level above significant deficiency. This suggests a level of control far beyond what anyone would design to achieve reasonable assurance. I imagine that there are few controls that, based on this definition and the level of work done to assess it, wouldn't have a significant deficiency. I wonder if drawing the audit committee's attention to weaknesses at the bottom of this level will improve financial reporting or create an unnecessarily distraction.
- Paragraph 191 would create communications responsibilities for deficiencies that don't rise to the level of significant. It's hard to imagine the public interest that is served by mandating written communications of deficiencies that represent only remote risks, inconsequential amounts, or both.
- The concept of combining deficiencies is alluded to, but not explained. For multiple deficiencies to be combined, do they all have to deal with the same account? The same assertion? If various minor problems in different areas of the financial statements all failing at once would significantly misstate the financial statements is that a significant deficiency or material weakness? Example D-3 in the appendix does

not shed significant light on this. That example is really just a single weakness with no compensating controls.

- Paragraph 46 says that inadequate documentation of control is a deficiency. I don't see how that follows from the definition in ¶ 7 or the criteria in COSO. It goes on to say that this might also be a scope limitation, though there is no indication of what would go into that decision.

Walkthroughs

The section beginning at ¶ 79 presents a list of detailed requirements for walkthroughs. I'm not sure why this has been elevated to such a level of importance. I certainly agree that walkthroughs are helpful and, in general, a good thing. And the requirement exists in the current SAS No. 55. But the rationale for its inclusion in the SAS does not apply here. In SAS No. 55 the auditor might do no more than obtain the understanding of internal control. If no testing is done, the auditor has done nothing to confirm that understanding unless the auditor does walkthroughs. In an audit of internal control, however, there will be a substantial level of testing; in fact all of the important controls will be tested, which will confirm the auditor's understanding. Also, in the context of SAS No. 55, the auditor's documentation of controls might be the only place they are actually written down, so the walkthrough helps make sure the description is accurate. In audits of internal control, management has already documented and assessed internal control, making this step much less imperative.

Accordingly, I think this set of requirements places an unnecessary requirement on the engagement. Further, the language is unnecessarily onerous. Paragraph 80 says the walkthrough should be sufficient to "*determine* whether the processing procedures are performed as originally understood and on a timely basis" (emphasis added). My conception of a walkthrough would be insufficient to accomplish this; only a test of controls would be enough. Paragraph 81 dictates specific questions and suggests to whom they should be directed and what order to ask them. While helpful in an implementation guide, this guidance is unjustified as a standard.

Requirement for the Financial Statement Audit

Question 2 to your transmittal letter asks whether it is necessary to do the financial statement audit to audit internal control. As I read Sarbanes-Oxley it seems to require that they be done as a combined service ("shall not be the subject of a separate engagement"). If, however, you have determined that it is legal to separate them, I see no reason for the requirement, although economics and practicality will probably drive practice to combine them. In practice, it is likely that many firms will assign different staffs to the two services either for efficiency or competence considerations. If the firm uses two sets of auditors for the two services each team will have intimate knowledge only of its engagement and will have to communicate certain matters to the other to make sure important items are considered. I expect they would formally communicate control weaknesses, misstatements, fraud or illegal acts, and other audit committee-type

communications. If two auditing firms coordinated in the same manner there would be no loss of effectiveness.

Other Matters

There are a number of other issues of more-than-editorial concern:

¶	Comment
24	The second and fourth bullets are not elements of the control environment. Neither are many of the controls that comprise the first bullet.
26	This paragraph introduces the concept of fraud identification. How is identification different from detection? What additional controls are envisioned here?
41	Management is allowed to rely on the work of the service auditor in fulfilling its responsibilities. What if the auditor is also the service auditor? Is the auditor then auditing his or her own work when considering management's assessment? Would the independence rules described in SAS No. 70 still apply?
61	The ramifications of the second half of this paragraph are unclear. It seems to suggest that a material weakness could exist in an account in which there could not be a quantitatively material misstatement. Thus, the implication is that the auditor is concerned with designing procedures to detect misstatements that are only qualitatively material. (Although it speaks only to controls over certain smaller accounts, it is hard to argue that the concept is much different.) This is a stark departure from SAS No. 47.
75	The linkage requirement implies, but does not state, a specific documentation requirement. This should be clarified.
93	This paragraph provides a real-life problem, but the solution in the final sentence doesn't solve it. Reperforming the control does not provide evidence that the supervisor performed the necessary review, which was the control to be tested. It only shows the auditor would have approved it.
101	The paragraph requires the auditor to vary the nature, timing, and extent of tests of controls each year. I'm not sure this improves the quality of the service. If the extent of tests is appropriate in one year, to change it the next year would require the auditor to do insufficient work or to over-audit unless the nature of the tests also changed. But of course, the type of control generally dictates the nature of the test, so changing that might provide a less effective test. Increasing the extent of a less-effective test seems an inefficient, and possibly less effective, approach to require. The example in the paragraph also seems to confuse the time period tested with the timing of the test. I understand the concern this paragraph was trying to address, but I think the requirement seems unduly inflexible. Perhaps the goal can

¶ Comment

be accomplished by warning auditors against too much predictability in choosing time periods, locations, and the like.

105 The second bullet implies the auditor has assessed the risk of control failure (that is, effective design but ineffective operation). The standard should refer to where it discusses such an assessment of individual controls. How does one judge this? Is it based solely on the results of tests of the controls (that is, a high deviation rate) or other things, such as complexity or subjectivity. (The discussion in ¶119 talks about risks in a different context—identified deficiencies—but perhaps some of the same concepts might apply here.)

126 The auditor's discovery of a material misstatement is described as a "strong indicator" of a material weakness. I think this doesn't go far enough. A material misstatement should be presumed to be the result of a material weakness. The auditor should have to justify any conclusion that it isn't.

140 The last sentence is not universally true. There are many times that analytical procedures are more effective in finding fraud than looking at the details, particularly when the completeness assertion is involved. (Analytical procedures might not be adequate for quantifying the fraud once it is detected, though.)

146 This paragraph confuses some concepts. Control risk is defined only in the context of audits of financial statements, not in the audit of internal control. (Actually, in this context control risk would reasonably refer management's assessment of its controls.) So, it's unclear whether this is talking about the financial statement audit or the audit of internal control. Further, under the existing SASs, control risk is assessed for assertions, not, as suggested by the second sentence, account balances.

I would be happy to discuss these comments with you in more detail if you'd like.

Sincerely,