INSTITUT
DER
WIRTSCHAFTSPRÜFER
IDW

Düsseldorf, November 21, 2003

Public Company Accounting Oversight Board
(PCAOB)
Office of the Secretary
1666 K Street, N.W.,
Washington, D.C.
20006-2803

USA

By E-Mail: comments@pcaobus.org

Dear Sir(s):

Re: PCAOB Rulemaking Docket Matter No. 008
IDW Comments on the PCAOB Proposed Auditing Standard – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements

We would like to thank you for the opportunity to comment on the PCAOB Proposed Auditing Standard – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements. The Institut der Wirtschaftsprüfer (IDW) represents approximately 85 % of the German Wirtschaftsprüfer (German Public Auditor) profession. The IDW seeks to comment on the proposals by the PCAOB noted above because we believe that this Proposed Rule will affect not only the development of auditing standards in the United States, but also influence auditing standards on internal control on a worldwide basis. Furthermore, a significant number of German Wirtschaftsprüfer are or will be subject to the requirements of the Sarbanes-Oxley Act.

General comments

Comment Period

We were disappointed to see the very short exposure period in which comments can be provided to the PCAOB. A comment period of 45 days is too short for a standard

Institut der Wirtschaftsprüfer
in Deutschland e.V.
Tersteegenstr. 14
40474 Düsseldorf
Postfach 320580
40420 Düsseldorf

Telefonzentrale 0211/4561-0
Fax Geschäftsleitung 0211/4541097
Fax Fachabteilung 0211/4561233
Fax Bibliothek 0211/4561204
Internet http://www.idw.de
E-Mail info@idw.de

Geschäftsführender Vorstand:
Prof. Dr. Klaus-Peter Naumann,
WP StB, Sprecher des Vorstands
Dr. Gerhard Gross
Dipl.-Kfm. Peter Marks, WP StB

Bankverbindung:
Deutsche Bank AG
Düsseldorf
BLZ 300 700 10
Kto. Nr. 7 480 213

of such length and importance in an international environment, since many organizations would like to have the opportunity to consult with their stakeholders. We would suggest that 90 days might be more appropriate for longer proposed standards of greater complexity, such as this one.

We are convinced that, if we had had the opportunity to consult our stakeholders and analyze this standard with greater diligence, we would have found additional significant issues that might require your attention.

Comments on Particular Technical Matters

The Audit Opinions Required

Section 404 of the Sarbanes-Oxley Act (SOX) requires the annual report " …to contain an internal control report, which shall … contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." Furthermore, …"each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer". Section 103 states that the Board "…shall include in the auditing standards that it adopts, requirements that each registered public accounting firm shall … describe in each audit report the scope of the auditor's testing of the internal control structure and procedures of the issuer required by Section 404 (b), *and* [italics added] present (in such report or in a separate report) (I) the findings of the auditor from such testing; (II) an evaluation of whether such internal control structures and procedures … ." Based on the wording in Section 103(2)(A)(iii), it appears to us that two opinions are being required of the auditor in relation to internal control: one on management's assessment and one on internal control directly.

We would like to point out that, contrary to the view expressed in footnote 3 of the proposed standard, an "audit of internal control over financial reporting" is not the same as "attestation of management's assessment of the effectiveness of internal control over financial reporting", nor does the former just refer to the process and the latter to the result of that process. We will provide our reasons for this assertion in the following paragraphs.

Presumably, management's assessment of the effectiveness of internal control would have to have the same scope (and cover the same period) as an audit of internal control performed by an independent third party so that management's assessment can be expressed at the level of reasonable assurance as described in paragraph 16 of the standard (this appears to be consistent with our reading of the requirements for management's assessment under the SEC's Release No. 33-8238 on Management's

Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports). This means that there is some residual risk that management's assessment had been appropriately performed but concludes that the internal control system is effective, even though it is not (the risk of incorrect acceptance). Hence, an independent auditor's attestation of management's assessment may conclude that management's assessment was appropriately performed, even though the internal control system is not effective.

This is different from the situation in which the independent auditor reaches an independent conclusion as to whether the internal control system is effective because, even thought the scope of the audit performed by the auditor may be the same as the assessment conducted by management, the auditor may, for example, choose different sample items on a random basis and thereby come to different conclusion than management.

In other words, we believe that SOX actually requires three separate opinions by the auditor: 1. on the fairness of the financial statements, 2. on the assessment of the effectiveness of internal control made by management and 3. on the effectiveness of the internal control. While these opinions may be closely related, they need not, by any means, lead to the same conclusion in all circumstances. For example, because internal controls only provide reasonable assurance that material misstatements will be prevented or detected on a timely basis, both management and the auditor may conclude that internal control is functioning effectively even though management or the auditor detect a material error in the financial statements by means other than the functioning of the internal control system. Likewise, in situations where the internal control system is not operating effectively and the audit of the internal control system by the auditor detects this, management may have appropriately conducted its assessment of the internal control system and concluded that the internal control system is operating effectively. Other combinations of opinions are conceivable. However, we suspect that some combinations will not be as relevant as others. For example, if management's assessment came to the conclusion that internal control is not effective, the auditor will examine the basis for that conclusion and it is very unlikely that he or she will reach a conclusion that is at variance with that of management in this case.

While the SEC's Release No. 33-8238 only addresses the auditor's opinion on management's assessment of the effectiveness of internal control, we believe that this does not preclude the PCAOB from requiring an opinion on internal control by the auditor beyond an opinion on management's assessment. The current draft standard is based on merging the opinion by the auditor on management's assessment of internal control with the opinion by the auditor on the effectiveness of internal control.

In our view, this approach is fundamentally flawed for the reasons given above. We therefore recommend that the standard be amended to provide for the auditor expressing three separate opinions, as noted in the previous paragraph. Furthermore, the standard should make clear that management's assessment should have the same scope (and cover the same time period) as an audit of internal control performed by an independent third party.

Reasonable Assurance

Paragraph 16 of the proposed standard states

> "Management's assessment of the effectiveness of internal control over financial reporting is expressed at the level of *reasonable assurance*. The concept of reasonable assurance is built into the definition of internal control over financial reporting and also is integral to the auditor's opinion. Reasonable assurance includes the understanding that there is a relatively low risk that material misstatements will not be prevented or detected on a timely basis. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance."

We are disappointed that the PCAOB is attempting to address a concept as fundamental, complex and important as the meaning of "reasonable assurance" as an "afterthought" within the confines of a proposed operational standard without having properly analyzed the issues surrounding the use of the term or exposed a separate issues or discussion paper to allow stakeholders adequate input before standards or rules dealing with fundamental auditing issues are proposed in this regard. We are particularly disappointed in this respect because we are aware that the AICPA had requested the PCAOB on more than one occasion in writing to commence a project on the meaning of "reasonable assurance".

With respect to the meaning of reasonable assurance, footnote 7 in the proposed standard refers to the "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Securities and Exchange Commission Release No. 33-8238 (June 5, 2003)" for further discussion of reasonable assurance. Our review of this Rule indicates that the term "reasonable assurance" is addressed primarily in "II. Discussion of Amendments Implementing Section 404", "F. Periodic Disclosure about the Certifying Officer's Evaluation of the Company's Disclosure Controls and Procedures and Disclosure about Changes to its Internal Control over Financial Reporting", "4. Conclusions Regarding Effectiveness of Disclosure Controls and Procedures". In this Rule reasonable assurance is not defined: rather, footnotes 101 and 102 make reference to Sec-

tion 13(b)(2) of the Exchange Act (15 U.S.C. 78m(b)(2)) and the Codification of Statement on Auditing Standards AU §319.18, respectively.

We believe that the reference to AU §319.18 is erroneous: the concept of reasonable assurance in relation to internal control is actually discussed in AU§ 319.21 to .24. In any case, the discussion of reasonable assurance in relation to internal control in AU §319 does not speak of "relatively low risk that material misstatements will not be prevented or detected", nor suggest that reasonable assurance represents a "high level of assurance". Rather this part of the AU §319 actually discusses the limitations of an entity's internal controls and cost-benefit relationships, etc. We also note that the AICPA standard on performing attest engagements on internal control (AT §501) refers to neither reasonable assurance nor high assurance, but does discuss the inherent limitations of internal control.

Based on our reading, 15 U.S.C. 78m(b)(2) actually only refers to the provision of reasonable assurance by the internal control system without defining it. We note that 14 U.S.C. 78m(b)(7) defines reasonable assurance as "…the degree of assurance as would satisfy prudent officials in the conduct of their own affairs". There is no mention of "relatively low risk" or "high assurance".

We would like to point out that the issues surrounding the meaning of "reasonable assurance" are both politically and technically very complex and a treatise on the subject could fill volumes. In this respect we would like to refer to the discussion on the meaning of assurance and levels of assurance in the FEE Issues Paper "Principles of Assurance: Fundamental Theoretical Issues With Respect to Assurance in Assurance Engagements". Nevertheless there is one issue that deserves mention to help focus on the practical problems involved.

Because audit or assessment risk is not separable from the uncertainties associated with the application of criteria to the subject matter, high inherent risks often cannot be alleviated through controls or an assessment or audit. This problem is often termed "consilience" by academics.

For example, a complex sales contract may be the basis for the determination of revenue recognition. Even after having obtained a legal opinion on the legal rights and obligations currently extant under the contract at year-end, both the preparer of the financial statements and the auditor may find that, in their view, the weight of evidence supporting recognition under applicable accounting standards is only slightly greater than that not supporting recognition: the situation is grey rather than black and white. Yet, both the preparer and auditor must reach a decision on the matter. In these circumstances, for example, neither can claim to have achieved a high level of assurance that, on balance, at least a slight majority of preparers and auditors would have agreed with their decision or that they had reduced the converse to a relative

low level of risk (in measurement theory, this is known as the "equivalence" aspect of reliability).

Hence, relating reasonable assurance to high or to just below absolute assurance or to relatively low risk is fundamentally misleading because both preparers and auditors face many decisions that can only be made on the basis of what the legal profession terms "the preponderance of the evidence". This thought ties in to the concept that audit evidence is persuasive rather than conclusive or convincing.

The other main problem with the application of the reasonable assurance concept as currently suggested by the draft standard is the tendency for third parties to apply 20-20 hindsight to the concept of reasonableness. In other words, third parties (neither management nor the auditors) will tend to take the view that if a catastrophe occurs, then the controls that were designed and implemented to prevent that catastrophe could not have been reasonable or reasonably effective. This stance, which is in itself unreasonable, can only be countered by a technically and politically sound treatment of the meaning of reasonable assurance.

The definition of reasonable assurance also ties into the definition of a "significant deficiency", which we will address in the following section.

The definition of significant deficiency

Paragraph 8 defines significant deficiency as follows:

> "A *significant deficiency* is an internal control deficiency that adversely affects the company's ability to initiate, record, process or report external financial data reliably in accordance with generally accepted accounting principles. A significant deficiency could be a single deficiency, or a combination of deficiencies, that results in a more than remote likelihood that a misstatement of the annual or interim financial statements that is more than inconsequential in amount will not be prevented or detected."

The use of the term "remote likelihood" is referred by footnote 5 to paragraph 3 of FASB Statement No. 5 Accounting for Contingencies (FAS No. 5), which defines the terms probable, reasonably probable and remote for events in relation to contingencies.

As we have pointed out in our discussion on reasonable assurance, the consilience between audit risk and the uncertainties associated with the application of criteria (accounting standards) to subject matter (events and circumstances) often reduces preparers and auditors to obtaining only a preponderance of the evidence to support decisions they have made with respect to the application of accounting principles in

particular circumstances. In these circumstances, the application of controls, assessments or audits will not necessarily enable an increase in assurance nor a concomitant decrease in the risk that a material misstatement occurs. Consequently, we question whether it is appropriate to apply the standard of “more than a remote likelihood” that controls should be able to prevent or detect a material misstatement in all circumstances.

In this matter, it should be noted that the application of the probability concepts (probable, reasonably probable and remote) to evaluate events leading to loss contingencies is an entirely different matter than using these probability concepts in determining the likelihood (what level of assurance has been obtained) that the appropriate probability concept was chosen, which is what is being asked of the internal control system, and hence of management’s assessment and the auditors. Consequently, the application of the concept “remote” can only lead to situations where management or the auditors (or both) are blamed for situations beyond their control.

In this connection, we would like to point out that the term “remote” also has legal meaning that suggests its application for identifying significant deficiencies in internal controls is inappropriate (e.g., “remote possibility”, which refers to a limitation dependent upon two or more facts or events that are contingent and uncertain, or a double possibility). Another legal meaning relates possibilities to the burden of persuasion required in criminal courts of law: beyond any reasonable doubt, which is defined as “ … not a mere possible doubt; because every thing relating to human affairs, and depending upon moral evidence, is open to some possible or imaginary doubt” (Commonwealth v. Webster, 59 Mass. (5 Cush.) 295, 320 (1850)). On this basis a remote possibility represents a standard either higher than or equivalent to beyond any reasonable doubt, which, in turn, is a standard usually higher than that expected either of internal control, management assessments, or audits.

Consequently, we suggest that a significant deficiency be defined as “an internal control deficiency, that either singly or in combination with other deficiencies, adversely affects a company’s ability to initiate, record, process or report external financial data reliably in accordance with generally accepted accounting principles and thereby hinders management from obtaining reasonable assurance that a misstatement that is more than inconsequential in terms of the annual or interim financial statements will not be prevented or detected”.

Of course, such a change in the definition of a significant deficiency means that the definition of a material weakness ought to be amended accordingly.

Effectiveness

Both management's assessment and the auditor's opinion (on the assessment and on the internal control system) are in relation to the effectiveness of the internal control over financial reporting. While the concept of reasonable assurance that material misstatements will be prevented or detected on a timely basis is a useful standard, in practice, both management and auditors will require concrete effectiveness criteria. We would like to point out that it is a basic tenant of both assurance engagements (see ISA 100) and attest engagements (see AT §101) that criteria must be suitable before an assurance or attest engagement can be performed. In our view, the lack of suitable effectiveness criteria in this standard for internal control precludes the performance of a meaningful assessment by management and hence audit of effectiveness of internal control.

The Use of Work of Management and Others

While we agree, to the extent the auditor must form his or her own opinion, that tests performed by the auditor cannot be replaced by tests performed by management and others, we consider it to be dysfunctional to not allow the auditor to use information obtained from the work of management and others in designing and performing the auditor's work. For example, management may have detected a weakness in internal control. It would be dysfunctional for the auditor not to be in a position to apply a risk-based approach and use the information, obtained by management or others, that there may be greater risks in some areas, to the extent that the auditor has evidence to support the view that the work can be relied upon. In any case, because the auditor is expressing an opinion on management's assessment of internal control, the auditor is in a position to obtain evidence to support whether management's work in this regard is reliable.

IT-related controls

In our view, the proposed standard does not provide enough guidance with respect to IT-related controls. For example, in Example B1 of Appendix B (Daily Programmed Application control and Daily Information Technology-Dependent Manual Control), it is suggested that the auditor is in a position to conclude that computer controls operate in a systematic manner. In our view, the procedures performed by the auditor prior to the walk-through do not support such a conclusion. For example, in addition to the procedures mentioned, the auditor should have obtained some evidence to support conclusions with respect to relevant IT security controls (e.g., how does the system ensure that during the filing of information by the bank to the company others

INSTITUT
DER
WIRTSCHAFTSPRÜFER
IDW

do not obtain information that they are not authorized to have, authorization checks to ensure that the bank rather than some other person or entity communicated that information, and other procedures to address privacy risks, etc.). Beside the risks arising in an e-business environment, in principle, computer aided commercial activities that are automatically interfaced with the entities accounting system affect assets or liabilities, results or expenses or income or lead to events requiring disclosures in the financial statements. Therefore, the reliability of accounting information depends on the reliability of the IT-aided transactions. The auditor has to assess the reliability and security of IT-aided transactions processing based on principles for appropriate accounting information processing (further guidelines with respect to this issue are provided by IFAC in; “E-Business and the Accountant: Risk Management to Accounting Systems in an E-publication Environment”).

We hope you find our comments helpful and would be pleased to be of assistance to you if you have any questions about these comments.

Yours very truly,

Klaus Peter Naumann
Chief Executive Officer

Horst Kreisel
Technical Manager

495/532