

For the attention of Jim Sylph
International Federation of Accountants
545 Fifth Avenue, 14th Floor
New York, NY, 10017
USA

7 July 2008

Dear Sir

IAASB Exposure Draft ISAE 3402 – “Assurance Reports on Controls at a Third Party Service Organization”

We appreciate the opportunity to comment on the IAASB’s proposed new International Standard on Assurance Engagements, ISAE 3402, *Assurance Reports on Controls at a Third Party Service Organization*.

Following extensive consultation with members of the PricewaterhouseCoopers network of firms, this response summarises the views of member firms who commented on this Exposure Draft. “PricewaterhouseCoopers” refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

Overall comments

We strongly support the development of this standard. We believe that it is important that there is a common basis for the conduct of engagements to report on controls in a service organization globally and, therefore, useful to fill this gap in international standards.

Differences in recognised standards governing such engagements globally would be unfortunate. Any significant differences would not only complicate the conduct of engagements that cross borders, but would also be difficult for users to understand – which could result in confusion, or even arbitrage, in the marketplace. Other pronouncements addressing this topic, such as Australia’s Guidance Statement GS 007, *Audit Implications of the Use of Service Organisations for Investment Management Services* (GS 007), the UK’s Technical Release AAF 01/06, *Assurance Reports on Internal Controls of Service Organisations Made Available to Third Parties* (AAF 01/06), and Germany’s IDW PS 951: *Auditing the internal control system of a service organisation*, are relatively recent and based on ISAE 3000. The US Auditing Standards Board is currently revising its AU 324, *Service Organisations* (SAS 70) and we have been encouraged by the liaison between the working parties. In our view, convergence among the final ISAE, the revised SAS 70 and other ISAE 3000 based national guidance is very important.

Overall, we believe that the direction being taken in IAASB’s proposed standard is sound. There are, however, certain proposals in the Exposure Draft that we do not support or believe need to be improved that are explained more fully in our letter – such as the proposed reporting when using the work of internal audit, and the proposed criteria. We strongly encourage IAASB to address these concerns in finalising the ISAE and would not support its release until these matters have been resolved.

Request for specific comments

1. The proposal that the ISAE be written for application to assertion-based engagements.

We support, in principle, the proposed ISAE being written on the premise that management of the service organization will confirm in a statement made available to intended users that accompanies the description of the system, assertions regarding the description, design and, for Type B reports, the operating effectiveness of the controls. This is broadly similar to Australia's GS 007 and the UK's AAF 01/06. It is not the model reflected in extant US SAS 70, although, in recent years, some reports issued under SAS 70 have voluntarily included a management assertion.

Although not required by ISAE 3000, including both management's assertion and the auditor's report thereon in the package made available to users has the advantage of making explicit the respective responsibilities of auditors and management and is consistent with current trends in reporting.

In light of the wording of paragraph 4, however, we were not entirely sure whether or not IAASB is proposing that only assertion-based engagements be accepted in these types of engagements (i.e., if direct reporting engagements are not permitted). Paragraph 4 of the standard is ambiguous on this point. If management refuses to provide an assertion, can the auditor accept the engagement and, if so, would the expected work effort be different than that described in the ISAE? We encourage IAASB to be explicit in this regard.

Implementation guidance needed to support the approach

Although we support the above proposal in principle, we believe that service organisation and user input is vital to ensuring that it is practicable. In particular, it will be vital that service organizations' management are aware of the assertions they will be asked to make, and understand the criteria on which they are based and the work effort expected as a basis for the assertions (e.g., what testing, if any, does management have to do to support the assertion?). Explanation of what may reasonably be expected from management in arriving at their assertion is, in our view, essential if this framework is going to gain acceptance. Additional guidance may well need to be developed, for which the involvement of service organisation management community would be important. We believe it is important for IAASB to initiate discussions with international oversight/regulatory bodies that may be appropriate sponsors for the development of the necessary practical guidance. In addition, the proposed ISAE is not yet sufficiently clear in some areas (for example, see further discussion below in relation to the proposed criteria).

One circumstance that we foresee where it may be difficult for management to make an assertion is where certain operations that are performed by a subservice organisation have been included in the report ("the inclusive method"). Such circumstances, which are relatively rare, could be addressed in the guidance on management's responsibilities discussed in the paragraph above.

We are also aware of situations where service organizations may not have designed the controls, but rather are processing user-designed controls. This is often the case, for example, when user organizations and service providers work under Business Transformation Outsourcing (BTO) models. The ISAE should allow for the assertion to be modified, in such circumstances, to reflect the facts and circumstances of the service relationship.

2. The inclusion in the proposed ISAE of a number of requirements based on ISAs. In particular, has the IAASB identified all such matters as are relevant? And should these matters be dealt with in proposed IASE 3402 or in ISAE 3000?

and

3. Whether ISAE 3000 should be amended with respect to auditor's external experts.

We believe that all relevant matters have been addressed in the ISAE. To the extent that the requirements and guidance are generic and would be expected to apply in all assurance engagements, they could be transferred to ISAE 3000 when it is next revised. This might be the case for the requirements on documentation, for example.

4. The proposed requirements of the minimum elements of suitable criteria.

The proposed approach for criteria is quite theoretical and, therefore, we are concerned that it might be difficult to apply for both auditors and service organisation management alike. In our view, the criteria need to be clear and it must be easy to understand how they relate to the conclusions that need to be made to form the necessary opinions on those matters. We are not convinced that the proposed criteria meet those aims.

In practice today, many have viewed the entity's control objectives, or the risks that threaten their achievement, as being the criteria around which the service organization designs, or at least measures and monitors, its control procedures. This is explicitly stated, for example, in AAF 01/06.

The proposed ISAE attempts to identify criteria that relate more directly to each of the specific opinions the service organization auditor may give in their report, that is, criteria for:

- Evaluating whether the description of the system is fairly presented.
- Evaluating whether controls are suitably designed.
- Evaluating whether controls have operated effectively.

We believe that articulating criteria for each of the objectives, and thereby, the opinions that the auditor expresses in the report, has merits and is entirely consistent with ISAE 3000. As drafted, however, some readers have found the proposed criteria quite theoretical. We anticipate that auditors and management may struggle with applying them in practice.

For example, particularly for the suitability of design, the proposed criteria sound more like a description of the process that would be followed in forming a conclusion on the suitability of design rather than the criteria against which suitability would be evaluated. Indeed, there is significant overlap with the proposed work effort to obtain evidence regarding the suitability of design in paragraph 35. Suitability of design relates more to whether there is appropriate linkage between the controls and the controls objectives, and whether those controls individually, or in combination, would provide reasonable assurance of the control objectives being achieved.

Also, in the case of both suitable design and effectiveness, the descriptions of the evaluation to be made (in the first sentences of paragraph 16 and 17) go beyond the wording of the opinions on those matters in the report. We believe they need to be aligned to avoid confusion (see further discussion on the need for alignment between the criteria and the opinions to be given in the first bullet under Other Comments).

We also believe that control objectives need to be given greater emphasis in the criteria for each of the opinions, so that it is clear that they provide an overriding framework for these engagements. This would be consistent with the prominence control objectives are given in other national standards.

For all of these reasons, we encourage IAASB to revisit the proposed criteria before the ISAE is finalised.

Consistent with our view that implementation guidance will be needed, we anticipate that there will be a need for more specific guidance on control objectives and their application. We acknowledge that it may not be practical for the proposed ISAE to specify or provide illustrative control objectives as is done in GS 007, AAF 01/06 and, to a lesser extent, SAS 70. However, we would hope that industry groups and national professional bodies will feel able to supplement the proposed ISAE with guidance on control objectives to provide some degree of standardisation.

5. Whether the description of tests of controls included in a Type B report should include the disclosure of sample sizes determined by the service auditor only when a deviation from controls is found.

We agree with the proposal that the report should include a description of the tests of controls performed when the service auditor expresses an opinion on operating effectiveness. As these reports are used by user organization auditors who do not, ordinarily, have an opportunity to instruct the service auditor about the nature, timing and extent of tests of controls to be performed, a description of the tests performed assists them in making appropriate decisions in planning and performing the audit of the user organization's financial statements.

We also support the proposal that the description need not include disclosure of the sample sizes used unless a deviation from controls is found. In such circumstances, the sample size provides important context for the user auditor to be able to evaluate the implications of that deviation.

Identifying the tests performed by internal audit and the service auditor's procedures with respect to that work

We are concerned, however, about the proposal that if the service auditor uses the work of the internal audit function in obtaining audit evidence about the operating effectiveness of controls, the report should describe internal audit's work and the service auditor's procedures with respect to that work. Whilst the report should include a description of the tests performed, we are not convinced that the description should identify that internal audit conducted certain tests, nor describe the service auditor's procedures with respect to that work.

Regardless of the extent of use made of the work of internal audit, the service auditor has sole responsibility for the opinion expressed in the service auditor's assurance report, and the wording of the report and opinion should not give the impression otherwise. We can see that disclosure around the use of internal audit may provide some degree of transparency. However, we believe that the approach adopted in a financial statements audit whereby the auditor does not refer in the audit report to the work of internal audit that has been used as audit evidence is equally applicable in these engagements, and are concerned that including additional disclosure will simply cause confusion. Indeed, user organisation auditors may not feel that they are able to draw as much assurance from that work, and the net result could be an environment where there is a reluctance to use the work of the internal audit function. Thus, the proposed approach could build in structural impediments to efficiency.

There is a valid question about the extent to which a service auditor can use the work of the internal audit function and retain the ability to take sole responsibility for the opinion expressed. However, this matter would be better addressed through establishing thresholds regarding *principal evidence* that must be obtained by the service auditor directly.

Support for other proposals in the Exposure Draft

- **Reasonable assurance engagement** – We support the proposal that these engagements be “reasonable assurance” engagements and that the ISAE does not contemplate “limited assurance” engagements. “Reasonable assurance” is equivalent to an “audit” level of assurance, and requires the auditor to obtain sufficient appropriate audit evidence. As reports on controls at a third party service organisation are used as evidence by auditors of financial statements of user organizations, this is entirely appropriate.
- **Types of reports** – The two types of report: Type A, which is limited to opining on the description of the controls and on their design, and Type B, which includes an additional opinion on their operating effectiveness, are similar to those in existing national standards. Although Type B reports are more common in practice and of more value, there are circumstances when a Type A report can be useful, such as in the first year of operation of a service organization. Therefore, we support the ISAE addressing both types of report.

However, we believe that there would be merit in the ISAE emphasising that a Type A report does not provide the user auditor with evidence regarding the operating effectiveness of controls. Thus, although a Type A report may be helpful to the user entity auditor in obtaining an understanding of internal control relevant to the audit of the user entity, it does not provide evidence in response to assessed risks of material misstatement. Although this point is made in proposed ISA 402, *Audit Considerations Relating to an Entity Using a Third Party Service Organisation*, we believe it is a point worth reinforcing in the ISAE as well.

- **Direct opinion on the description, design and operating effectiveness** – We support the proposed approach to the auditor's report whereby the service auditor's opinion is directly on the description, design and operating effectiveness of controls even though the report will include management's assertions.

We appreciate that there are arguments for wording the opinion so that the auditor gives his or her view on the credibility of management's assertion – indeed, doing so would further reinforce auditor's and

management's respective responsibilities. However, it is not the easiest model from a user's perspective. In particular, it could be more difficult for users to interpret when there are control deficiencies and there is a risk that such an opinion could be misinterpreted.

Other comments

We encourage IAASB to address the following matters in finalising the ISAE.

- **Alignment of the proposed objective, opinion wording and criteria**

We are concerned that the proposed wording of the objective of the auditor, the auditor's opinions, and the requirements on criteria is not sufficiently aligned.

The illustrative report for a Type B report in Appendix 2 proposes that the auditor's opinion be that, in all material respects:

- The description fairly presents the system that had been designed and implemented throughout the period.
- The controls related to the control objectives stated in the description were suitably designed throughout the period; and
- The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period.

Neither the auditor's objectives nor the requirements on assessing the suitability of the criteria make reference to the period. Presumably this is because IAASB was attempting to define them generically so that they apply to both Type A and Type B reports (the auditor's focus in a Type A engagement being on a point in time)

We do not believe that this approach is appropriate. It is important that the relationship between the stated objectives of the service auditor, the criteria, the proposed work effort and the opinions expressed is very clear in the standard—even if that means that it is necessary to provide different, or at least incremental, requirements as between Type A and Type B reports.

Furthermore, we do not believe that ISAE sufficiently defines the work effort expected by auditors to form the conclusions above as they relate to being "throughout the period" in a Type B engagement. This is a serious flaw in the draft.

At present, auditors focus on verifying the controls in effect at a point in time, but, in addition, through inquiries and evidence obtained from the tests of operating effectiveness over the period, seek to identify whether there have been significant changes in the controls during the period. If so, it would be expected that those changes be included in the description of the controls. We believe that this is an appropriate approach and provides user auditors with relevant information. In the absence of the expectations of the work effort needed to support the proposed opinion wording, there is a risk that there will be confusion regarding the work that is necessary, with the possible implication that considerably more testing is required than is done in practice today. We question whether the cost/benefit of additional work would be warranted.

Therefore, we strongly recommend that the ISAE be more explicit in describing the work effort needed to support the proposed opinions in order to clarify expectations.

- **Other comments on the objective of the service auditor in performing an ISAE 3402 engagement**

The proposed wording of the objective in the standard was based on the wording of the overall objective of an audit in the Clarity Exposure Draft of ISA 200. The construct of that ISA 200 wording has changed in light of respondents' comments on the Exposure Draft. The approach to the objectives ought to be the same and IAASB should revisit the wording of this objective now that ISA 200 has been finalised.

In addition to the opinions on the description of the controls, the suitability of their design, and, for Type B reports, their operating effectiveness, both SAS 70 and GS 007 include opinions regarding whether the identified controls have been placed in operation (SAS 70)/or have been implemented (GS007). ISA 315 paragraph 13 requires the auditor to evaluate the design of the controls and *determine whether they have been implemented* when obtaining an understanding of controls that are relevant to the audit. Thus,

we believe that evidence regarding their implementation is relevant to user auditors and question why this is not recognised in the proposed ISAE.

▪ ***Assessing the risk of intentional misrepresentation***

One of the objectives of the service auditor is to obtain reasonable assurance about whether, in all material respects, based on suitable criteria, management's description of the system is fairly presented. In an audit of financial statements, the auditor is required to assess the risk of misstatement due to fraud or error in planning and performing the audit. Explicit consideration of the risk of misstatement due to fraud is believed to be important. In the context of an assurance report on controls at a third party service organization, there are two perspectives in relation to fraud that may be relevant:

- The proposed criteria for evaluating whether the description of the system is fairly presented includes whether the description does not omit or distort information relevant to the scope of the service organization's system being described, which could be due to unintentional or intentional misrepresentation. The requirements and application guidance related to obtaining evidence regarding the description do not directly discuss the risk of intentional misrepresentation and we recommend that IAASB consider, at a minimum, adding a bullet in paragraph A11 that a further question for consideration is whether there are possible incentives for service organisation management to misrepresent its system and controls.
- User auditors are required to obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risks of material misstatement of the financial statements whether due to fraud or error. An important consideration for the service auditor is consideration of the risk that the stated controls objectives would not be achieved due to intentional acts by service organization personnel, and whether the service organization has adequate controls in place to reduce that risk to an appropriate low level.

The ISAE would be strengthened if it included procedures designed to identify and assess these risks, which could include, for example, inquiries of management and others to obtain their views about such risks, and evaluating management's risk assessment process and how the service organisation addresses such risks.

▪ ***Limited use and distribution and conditions of use***

The proposed reporting requirements include a requirement to "identify the purpose(s) and intended users of the service auditor's assurance report". The application material goes on to explain that when the criteria are available only to specific intended users, or are relevant only to a specific purpose, ISAE 3000 requires that the assurance report should include a statement restricting the user of the assurance report to those intended users or that purpose. The illustrative reports include wording for this paragraph that is placed at the end of the report, consistent with how these matters are addressed in audits of special purpose financial statements (ISA 800).

We can see the merits of including this section of the report in the same place in this report as in other audit reports. However, we are concerned that the proposed ISAE does not deal with this topic adequately.

The ISAE is silent regarding the conditions of use of the report or limitation of liability. In both GS 007 and AAF 01/06, the guidance and illustrative reports are more extensive. Inclusion of such statements are common in these sorts of engagements and are clearly in the public interest as they guard against the possibility of unwarranted reliance on the report by prospective users of it.

We strongly encourage IAASB to at least acknowledge in the ISAE this wide-spread reporting practice in jurisdictions where allowed by relevant law or regulation by recognising that the auditor may want to insert additional wording to reflect any liability arrangements agreed between the service auditor, the service organisation and other users, including confirmation of the purpose for which the service auditor's report has been prepared and the basis on which other parties may use the report.

Furthermore, we find the illustrative wording of the paragraph regarding intended users and purpose in the illustrative reports to be inadequate in the context of these engagements. If IAASB does not believe it appropriate to provide more comprehensive illustrative wording, it would be preferable for the illustrative reports to leave this section of the report open to enable service auditors in different jurisdictions to draft this part of the report as is appropriate in their jurisdiction and the circumstances of the engagement.

- ***Inherent limitations***

Similarly, the description in the illustrative reports of the inherent limitations of internal controls at a service organisation is more limited than the descriptions in the other national standards. We believe there is merit in encouraging a consistent description of the limitations and encourage IAASB to consider the approach adopted in GS 007 and AAF 01/06.

- ***Completeness of criteria***

In assessing the suitability of the criteria in accordance with ISAE 3000, the practitioner is directed to the characteristics of suitable criteria in the International Framework for Assurance Engagements. Those characteristics include completeness, as well as relevance, reliability, neutrality and understandability. The need to consider if the control objectives are “relevant and complete” or are “reasonable in the circumstances” is specifically discussed in other national standards for these engagements. Although the proposed ISAE is premised on the fact that ISAE 3000 applies, we believe consideration of the completeness of control objectives is of sufficient importance that it should be explicitly addressed in this ISAE in the requirements or guidance on suitable criteria.

Obviously, user auditors need to read the reports carefully to understand the control objectives covered by the report. Indeed, we believe that the ISAE should emphasise the importance of management’s assertion needing to have a clear description of the scope of the report. However, the service auditor should also be satisfied that the scope of the control objectives is not misleading, from the perspective that they are logical and there are no obvious gaps. If the service organisation has “cherry picked” the control objectives covered in order to convey a less than complete story, the description of the controls could be misleading. We believe the ISAE should address this matter more fully.

- ***Definition of internal audit function***

The ISAE discusses using the work of the “internal audit function” in obtaining evidence. The proposed definition describes the “internal audit function” as internal auditors or *others who perform similar activities*, and provides a compliance or risk department as examples. In having a focus on a department or function, the definition seems unduly restrictive. There may be others in the organisation working under the direction of management or an audit committee whose work provides evidence about internal control. More important than their organizational structure, is their competence and objectivity. We recommend that the definition be revised to focus more on those attributes than on their function, per se.

- ***Lack of concept of “significance” in required written representation***

The proposed written representation in paragraph 42 includes disclosing to the auditor “instances where controls have not operated as described”. The wording does not seem to allow for any consideration of the concept of materiality or significance to users, nor does it appear to take into account the existence of compensating controls. The requirement for subsequent events in paragraph 47, on the other hand, introduces a concept of events that “could have a significant effect on the service auditor’s assurance report”. We believe it would be appropriate to bring a similar sort of concept into the written representation, or alternatively, a concept of “other than clearly trivial” (as is used elsewhere in the ISAs) in order for it to be practicable.

- ***Materiality***

In the discussion of materiality in paragraph A6, we recommend that the guidance acknowledge that it is preferable for the reports on operating effectiveness to include all exceptions identified subject to an “other than clearly trivial” or “clearly inconsequential” threshold. The judgment of whether or not an exception is “material” should be left to the users of the report.

- ***“Attribute sampling”***

Paragraphs 39 and A23-24, as well as the subheading above paragraph 39, refer to “attribute sampling”. This term is not used in ISA 530, *Audit Sampling*, and might be misinterpreted. Some readers interpreted the phrase to be a reference to substantive testing rather than tests of controls. We suggest that the reference to “attribute” be deleted.

- **Other information provided by the service organisation**

The requirements for the content of the service auditor's report allows for the introduction to the report to identify parts of the description of the system that are not covered by the service auditor's opinion. We believe the report should go further and disclaim an opinion on that other information provided by the service organisation. As this is a common situation, including illustrative wording would be useful.

- **Approach to subservice organisations**

The definitions section defines a subservice organisation and the carve-out method and inclusive method of dealing with the services provided by a subservice organization. The reporting requirements also include disclosure in the assurance report if a subservice organisation performs certain services. Within the requirements that discuss engagement acceptance and the work effort, however, there is little discussion. We question whether there is sufficient guidance on the implications of these models, such as the engagement acceptance considerations, or the need to obtain appropriate representations if adopting the inclusive method.

- **Additional clarification re: evidence regarding effectiveness of controls**

We believe it would be useful to include additional application guidance on matters to consider when deciding whether it is necessary to obtain evidence supporting the operating effectiveness of indirect controls. Relevant consideration include whether those indirect controls are automated or manual. Manual controls should be tested to evaluate their integrity. We suggest adding the sentence "and key automated or manually produced reports" after the reference to "indirect controls" in paragraph 37(b).

In addition, it would be useful for the ISAE to clearly state that the fact that evidence obtained through substantive procedures does not overcome an identified control weakness. In addition, although ISA 402 recognises that a service auditor may perform substantive procedures for the benefit of user auditors, these procedures do not provide evidence for the opinions on the controls.

- **System**

Throughout the proposed ISAE, including management's assertion and the service auditor's report, reference is made to the service organisation's "system". In the ISAE, this is intended to refer, for example, to the services, procedures, policies, control objectives and controls. Many people equate the term "system" with an entity's IT system. To ensure a common understanding, it would, at a minimum, be useful to include a definition of the term in the ISAE. It may also be useful for the illustrative reports to refer to the entity's "internal control system".

- **Date of written representations**

Paragraph 43 proposes that it be required that written representations from management must be dated on the same date as the service auditor's assurance report. We recommend that this requirement be aligned with the recently approved ISA 580, *Written Representations*, which requires that the date of the written representations should be as near as practicable to, but not after, the date of the auditor's report on the financial statements.

- **Benefit in providing further discussion of application to other subject matters**

We support the approach of drafting the requirements in this ISAE for controls at third party service organizations relevant to financial reporting by user entities. The ISAE has clearly been drafted with this particular context in mind. Recognition that the requirements in the ISAE may also be applied, adapted as necessary in the circumstances of the engagement, for engagements to report on other controls is useful. In practice, demand is growing for engagements addressing other aspects of controls at service organisations. However, the phrase, on its own, provides little insight into how an auditor would apply and use the ISAE in another context. For this reason, we believe that additional guidance is needed on the areas within the ISAE that may be particularly important to consider when "adapting" the requirements to other subject matters. For example, guidance could emphasise the importance of clearly identifying the subject matter and the type of opinion expected to be given, and of evaluating whether there are suitable criteria to enable the auditor to be able to form that opinion.

- **Testing conducted in a Type A examination**

In the Explanatory Memorandum, the discussion of the Type of Report makes the point that, “since no tests of controls are undertaken for the purposes of Type A report, there is no basis upon which a user auditor may choose to rely on the controls”. There will be a certain level of testing involved to support the opinion on the design of controls and their implementation. The important point is that in a Type A report, the service auditor has not performed any procedures regarding the operating effectiveness of controls. Although we recognise that the Explanatory Memorandum does not comprise an integral part of the final ISAE, we thought it important to bring this point to IAASB’s attention in case wording from the Explanatory Memorandum is included in the IAASB’s final Basis for Conclusions.

- **Terminology**

In a number of places, the proposed ISAE introduces terminology that is not consistent with terminology used in other national standards and in practice today. Where such changes are necessary to ensure alignment with ISAE 3000 or other IAASB pronouncements, the changes may be justified. Where they are not, we encourage IAASB not to introduce different terms as it will only cause confusion for auditors and service organisations alike.

For example, the ISAE proposes to refer to the two types of reports as Type A and Type B. Existing national standards refer to Type I and Type II reports and, as a result, these labels have recognition in practice and in the marketplace. It is unclear why IAASB needs to change from those conventions.

We would be happy to discuss our views further with you. If you have any questions regarding this letter, please contact Roger Marshall (+44 20 7804 4866), Tony Pedari (+1 416 941 8226) or Alun Richards (+44 20 7804 2706).

Yours faithfully,

PricewaterhouseCoopers