

**Assurance Reports on Controls at a Service Organization—  
Issues and IAASB Task Force Proposals****A. OUT-OF-SESSION FEEDBACK**

1. The Task Force prepared a revised draft ISAE 3402<sup>1</sup> following the feedback it received at the June 2009 meeting and, as agreed at that meeting, distributed that draft for out-of-session feedback from IAASB Members and Technical Advisors prior to finalizing agenda papers for the September 2009 meeting. The Task Force is grateful for the feedback it received through that process (particularly acknowledging that a number of members provided a response while on summer holidays). Substantive issues raised in that feedback process have been addressed through revisions to the draft or are elaborated on in this issues paper.

**B. THE RELATIONSHIP BETWEEN RISKS, CONTROL OBJECTIVES AND CRITERIA**

2. At the June meeting, the IAASB discussed the relationship between risks, control objectives and criteria, including whether the identification of risks leads to the formulation of control objectives or whether risks are identified after control objectives have been determined. The Task Force was asked to consider whether further explanation of the relationship between risks, control objectives and criteria should be added to ISAE 3402.
3. Subsequent to the June meeting, a member who had spoken to this issue at the June meeting wrote to the chair of the Task Force further explaining the views expressed. That letter was discussed in considerable detail by the Task Force. The Task Force understands the view expressed was advocating a process whereby:
  - (a) The service organization should identify the risks that could jeopardize the reliability of the services being provided;
  - (b) The service organization should then develop control objectives for each of those risks; and
  - (c) The adequacy of the design of the controls should be evaluated in the context of the significance of the risks identified.
4. While the Task Force agrees that (a) and (b), which imply a formal, sequential risk analysis, may describe how some service organizations could go about developing control objectives, the Task Force did not support requiring such an approach because, apart from the fact that the IAASB does not have a mandate to require management to take particular actions, the approach described is not the only way control objectives can be developed. In the Task Force's experience, it is common for risks and control objectives to be identified in an iterative way, rather than as outlined above. As stated at paragraph A10:

---

<sup>1</sup> Proposed International Standard on Assurance Engagements (ISAE) 3402, "Assurance Reports on Controls at a Service Organization."

The service organization is responsible for identifying the risks that threaten achievement of the control objectives stated in the description of its system. The service organization may have a formal or informal process for identifying relevant risks. A formal process may include estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. However, since control objectives relate to risks that controls seek to mitigate, thoughtful identification of control objectives when designing and implementing the service organization's system may itself comprise an informal process for identifying relevant risks.

5. There appears to be a concern about whether service organizations are responsible for identifying the risks that threaten achievement of the control objectives, or the risks that could jeopardize the reliability of the services being provided. In the Task Force's view, this is a semantic difference only – if the control objectives are not achieved, then the reliability of the services will be jeopardized, and vice versa. Nonetheless, from the user auditor's point of view, it makes more sense to think of risks in terms of the control objectives rather than in terms of the services as a whole, because this is how a user auditor evaluates which controls he or she may seek to rely on.
6. There also appears to be an underlying concern about the completeness of control objectives, and it was argued that the approach advocated would assist the service auditor in evaluating whether the control objectives identified by the service organization are complete. The Task Force has added the following text to paragraph A23 to clarify the role of the service auditor with respect to the completeness of control objectives:

While a complete set of control objectives can provide a broad range of user auditors with a framework to assess the effect of controls at the service organization on the assertions commonly embodied in user entities' financial statements, the service auditor ordinarily will not be able to determine how controls at a service organization specifically relate to the assertions embodied in individual user entities' financial statements and cannot, therefore, determine whether control objectives are complete from the viewpoint of individual user entities or user auditors. It is the responsibility of individual user entities or user auditors to assess whether the service organization's description addresses the particular control objectives that are relevant to their needs.

7. The Task Force believes this reflects the reality of service organization engagements, and the underlying substance of user auditors' responsibilities in accordance with ISA 402.<sup>2</sup>
8. A point was made at the June meeting in connection with this matter that service organizations may need guidance on how to implement their implied responsibilities under ISAE 3402. Further, in feedback on the out-of-session draft, it was suggested that additional consultation with service organizations may be necessary about, for example, their willingness to give representations and make assertions in the form required, before

---

<sup>2</sup> International Standard on Auditing (ISA) 402, "Audit Considerations Relating to an Entity Using a Service Organization."

the draft ISAE is approved as a final standard. Suggestions for consultation were to: organize stakeholder groups to discuss the practicality of the standard before finalizing it; launch the document as interim guidance; or launch it as ‘final’ but with a set review date in the not too distant future.

- (a) With respect to guidance, the Task Force is of the view that as the document is currently drafted, it is sufficiently flexible to accommodate the various ways that service organizations go about identifying risks and control objectives in practice already. It is noted nonetheless, that the American Institute of Certified Public Accountant (AICPA)’s Guide to the AICPA’s new Statement on Standards for Attestation Engagements (SSAE) “Reporting on Controls at a Service Organization”, which in this respect is likely to be identical to ISAE 3402, is expected to be issued before the operative date of the ISAE. Ms Esdon has been invited to join the AICPA Task Force working on the Guide, as has Rick Wood, a member of the IAASB Task Force. This will provide an appropriate opportunity to develop implementation guidance at level of detail beyond that appropriate for a standard.
- (b) With respect to further consultation with service organizations, the Task Force is satisfied, based on their knowledge of the industry as well as other feedback such as the experiences of the AICPA Task Force related during the course of the joint meeting held in March 2009, that delaying approval of the ISAE so as to consult further with service organizations is not warranted. The Task Force also notes the practical difficulty in obtaining the collective view of service organizations (for example, there appear to be no mature industry bodies) or even the views of individual service organizations (the Exposure Draft was sent to 37 service organizations identified by IAASB members, firms and member bodies around the world, only 5 of which responded).

C. SCOPE OF ISAE 3402

- 9. At the June meeting, the IAASB asked the Task Force (a) whether it is feasible to amend the draft to cover engagements where the service organization is not responsible for the design of the system; and if not, (b) whether ISAE 3402 should continue to state that it may provide guidance for such engagements under ISAE 3000<sup>3</sup>. Such situations mostly occur in “one-to-one” engagements where the service organization is operating a system that has been designed by the user entity or is stipulated in a contract between the user entity and the service organization.
- 10. The Task Force considered this matter, and even experimented with drafting assurance reports to accommodate such engagements, but came to the view that it is not feasible to amend ISAE 3402 at this stage to cover these situations. As noted in paragraph A1, the absence of an assertion with respect to the suitability of design will likely preclude the service auditor from opining on the operating effectiveness of controls. This is because, as explained in footnote to paragraph A1, the service auditor needs to be satisfied that

---

<sup>3</sup> ISAE 3000, “Assurance Engagements Other Than Audits or Reviews of Historical Financial Information.”

controls have been suitably designed as a precondition to concluding, on the basis of testing whether controls are operating as designed, that those controls provide reasonable assurance that the control objectives have been met.

11. It was noted when the draft was circulated out-of-session, that in some cases a service organization, while not responsible for the design of the system, may nonetheless be able to provide an assertion about the suitability of its design, and in those cases ISAE 3420 could be applied. Paragraph 2 has been amended to recognize this possibility.

D. CLOSELY RELATED CONTROLS

12. It was noted in the out-of-session comments received that in some jurisdictions it is common for engagements that are primarily focused on controls over financial reporting to also include closely related controls, for example, controls over regulatory compliance. A literal reading of the draft circulated out-of-session would require the work done on the closely related controls to be performed under ISAE 3000, not ISAE 3402, and it was argued that this would necessitate a separate assurance report, or at the least a two-part assurance report, which is likely to lead to unnecessarily cumbersome communication.
13. Following some useful suggestions made in the out-of-session comments, the Task Force has:
  - (a) Amended what is now paragraph 3 to state that the ISAE does not apply to engagements to report separately on non-financial controls; and
  - (b) Added paragraph A2, which notes that engagements under ISAE 3402 to report on financial controls, may also include closely related controls.

E. INTERNAL AUDIT

14. The IAASB has discussed whether it is appropriate to identify, in that part of the service auditor's report that describes the service auditor's tests of controls, the work performed by the internal audit function. While it was noted that this may be interpreted as a division of responsibility (which is not intended), it was also noted that removing this requirement may lead to a decrease in transparency and intended users being misled into thinking service auditors themselves had done work that was actually performed by internal auditors.
15. The Task Force noted that type 2 reports are different than other assurance reports, in that they include a factual description of the tests of controls, in a separate part of the report, for the benefit of user entities and user auditors. The Task Force had proposed that the description clearly indicates who performed the tests of controls (service auditor or internal audit) because the service auditor cannot represent that he or she has performed tests of controls when this is not the case. However, the Task Force acknowledged that the service auditor has sole responsibility for the opinion expressed in the service auditor's report, and that responsibility is not reduced by the service auditor's use of the work of internal audit. In order to avoid any unintended suggestion that the service auditor is dividing responsibility for the work performed by internal audit, the Task Force has removed the requirement to identify the work performed by internal audit. The

wording of the assurance report has also been modified to eliminate references to “we” in reference to tests of controls.

F. REQUIREMENT TO COMPLY WITH ISAE 3000

16. The June draft included the following requirement: “In addition to this ISAE, the service auditor shall comply with ISAE 3000.” The draft of ISAE 3410<sup>4</sup> discussed in June had a similar requirement. It was noted that this requirement seems to read the wrong way around because it is a subsidiary standard requiring adherence to a higher-order standard.
17. An alternative formulation has been used in the drafts of ISAE 3402, ISAE 3410, and ISAE 34XX<sup>5</sup> to be discussed at this meeting: “The service auditor shall not represent compliance with this ISAE unless the service auditor has complied with the requirements of this ISAE and ISAE 3000.” This formulation is modeled on paragraph 20 of ISA 200<sup>6</sup>: “The auditor shall not represent compliance with ISAs in the auditor’s report unless the auditor has complied with the requirements of this ISA and all other ISAs relevant to the audit.” The three draft ISAEs mentioned above have slight variations with respect to the content and placement of related guidance.

G. OTHER MATTERS

18. It was suggested in the comments received on the out-of-session draft that it may be appropriate to include a responsibility for the service auditor to take action if the service auditor becomes aware of fraud that may affect one or more user entities but has not been communicated appropriately to those user entities. This is the same as the responsibility with respect to non-compliance with laws and regulations. The Task Force agrees that this is appropriate, and has amended paragraph 56 accordingly.
19. At the June meeting, the Task Force was asked to consider whether the requirement to identify the period to which items tested relate is necessary. The Task Force is of the view that the service auditor has a responsibility to test controls over the entire period covered by the assurance report, and has consequently deleted this part of paragraph 54.
20. An issue raised in response to a response to the out-of-session draft is whether this ISAE should be mandatory or optional. The document was exposed as a proposed standard, and the Task Force believes the comments received support it being issued as a standard. The Task Force is also of the view that changes made since exposure do not warrant re-exposure.
21. The Task Force has included a new requirement in paragraph 13 for the service auditor to determine the appropriate person(s) within the service organization’s management or governance structure with whom to interact on various matters. This was introduced to

---

<sup>4</sup> ISAE 3410 “Assurance on a Greenhouse Gas Statement.”

<sup>5</sup> ISAE 34XX “Assurance Reports on the Proper Compilation of Pro Forma Financial Information Included in Prospectuses.”

<sup>6</sup> ISA 200 “Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing.”

overcome any confusion that may arise from use of the term “service organization” rather than “management” or “those charged with governance.” In responses to the out-of-session draft, a concern was expressed about the sentence “This shall include consideration of which person(s) have the appropriate responsibilities for and knowledge of the matters concerned.” The Task Force notes that this wording is intended to align with ISA 580<sup>7</sup>.08 “The auditor shall request written representations from management with appropriate responsibilities for the financial statements and knowledge of the matters concerned.”

22. In the version of the ISAE distributed for out-of-session consideration, the Task Force had moved the content of paragraph 17(c) into the lead-in sentence of the paragraph. This attracted a number of adverse comments and the change has now been reversed.

#### **H. AICPA AUDITING STANDARDS BOARD (ASB)’S REVISION OF STATEMENT OF AUDITING STANDARDS (SAS) 70<sup>8</sup>**

23. As mentioned in paragraph 8 of this Paper, the ASB is developing an SSAE, that is intended to replace SAS 70. The latter standard has been accepted in many jurisdictions as the de facto international standard for assurance reports on controls at a service organization, in the absence of an IAASB pronouncement.
24. The IAASB Task Force and the AICPA Task Force have been liaising with the intention of eliminating, or reducing to the extent possible, differences between ISAE 3402 and the AICPA’s SSAE. At the June 2009 IAASB, the Task Force reported that most differences had effectively been eliminated, with the only remaining issues of substance being how the following matters are treated:
  - (a) Intentional acts;
  - (b) Subsequent events;
  - (c) Restriction on use of the service auditor’s report; and
  - (d) Description of the tests of controls.
25. A verbal report on the status of the AICPA’s SSAE will be given at the September Board meeting.

---

<sup>7</sup> ISA 580 “Written Representations.”

<sup>8</sup> Statement of Auditing Standards 70, “Reports on the Processing of Transactions by Service Organizations.” A proposed auditing standard, based on ED-ISA 402, was issued at the same time.