



International Federation of Accountants

545 Fifth Avenue, 14th Floor, New York, NY 10017 USA

Tel +1 (212) 286-9344 Fax +1 (212) 286-9570 www.ifac.org

Agenda Item H.2

Committee: IAASB Consultative Advisory Group

Meeting Location: Toronto

Meeting Date: September 4-5, 2008

Proposed ISAE 3402, “Assurance Reports on Controls at a Third Party Service Organization”

Objectives of Agenda Item

To review a preliminary staff analysis of the responses to ED-ISA 3402, “Assurance Reports on Controls at a Third Party Service Organization.”

The IAASB will consider a summary of significant comments and the Task Force’s recommendations, and the proposed ISAE at its December meeting. **Approval of the final ISA is planned for the March 2009 IAASB meeting.**

IAASB Task Force

The IAASB Task Force members are:

- Denise Esdon (Task Force Chair), IAASB member and Chair of ISA 402 Task Force
- Romek Lubaczewski, PwC, Poland
- Calum Thomson, Deloitte, UK
- Karsten tom Dieck, KPMG, Germany
- Rick Wood, Grant Thornton, Canada
- Correspondence member: Claire Grayston, AUASB, Australia

Background

1. The IAASB commenced this project in 2006 concurrently with a project to revise extant ISA 402.¹ The IAASB recognized the growing use of service organizations by user entities and the need for a service organization to be able to provide user entities and their auditors with a service auditor’s assurance report on its controls. This proposed ISAE will provide the standards for such assurance reports. It is intended to complement proposed ISA 402 (Revised and Redrafted),² in that reports prepared in accordance with proposed ISAE 3402 will be

¹ ISA 402, “Audit Considerations Relating to Entities Using Service Organizations.”

² Proposed ISA 402 (Revised and Redrafted), “Audit Considerations Relating to an Entity Using a Third-Party Service Organization,” as discussed in Agenda Item H.1.

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

- capable of providing appropriate evidence under proposed ISA 402 (Revised and Redrafted).
2. The IAASB believes that the proposed ISAE will enhance the consistency of auditor performance in relation to assurance reports on controls at third party service organizations, particularly in those jurisdictions that have adopted IAASB standards and have not, to date, had a specific standard on this topic. It is expected that proposed ISAE 3402, in conjunction with proposed ISA 402 (Revised and Redrafted), will enhance the consistency of auditor performance in relation to the audit of the financial statements of user entities.
 3. The proposed ISAE is drafted on the assumption that a service organization has many customers (user entities) and each user entity and its financial statement auditor receive a copy of the description of the system and the service auditor's assurance report. For this reason, the proposed ISAE assumes a direct relationship between user entities and user auditors, and between service organizations and service auditors, but does not assume any direct relationship between the service auditor and either user entities or user auditors. The proposed ISAE can also be applied, however, to other situations, where a direct relationship between the service auditor and the user entity or user auditor may exist.
 4. ED-ISAE 3402 was issued in December 2007. The comment date was May 31, 2008. Forty-four comment letters were received. (ED-ISAE 3402 and the comment letters are available at <http://www.ifac.org/Guidance/EXD-Details.php?EDID=0099>).
 5. Staff has conducted a preliminary analysis of the comments received on the exposure draft and, in consultation with the Task Force Chair, identified the significant comments summarized in the this paper for discussion with the IAASB CAG. **The Task Force and the IAASB have not yet deliberated any of the comments received on the exposure draft.** Consequently, the paper does not contain any recommendations with regard to the identified significant comments.
 6. Approval of the final ISAs is planned for March 2009. Staff therefore considers it appropriate to obtain the views of Representatives at this meeting to provide assistance to the IAASB in its consideration of the identified significant comments.
 7. Overall, respondents were in agreement with the proposed ISAE. While numerous suggestions for improvements were made, only a relatively small number of major issues were raised.

Responses to Requests for Specific Comments

8. In the explanatory memorandum accompanying ED-ISAE 3402, the IAASB requested respondents to comment on five specific matters, each of which is discussed below.

Assertion-Based Engagements

9. The IAASB requested views on the proposal that the ISAE be written for application to assertion-based engagements, i.e., where management of the service organization confirms, in a statement made available to intended users that accompanies the description of the system, that the description of the system is fairly presented, the controls are suitably designed and, in

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

the case of a Type B report, the controls have operated effectively. In particular, the IAASB asked whether there are situations in which it would not be possible or practicable for management of a service organization to provide an assertion.

10. Thirty-nine respondents commented on this proposal. The preliminary staff analysis indicates that:

- (a) Thirty-four respondents supported the proposal. Some of those made additional suggestions or comments including:
 - (i) The ISAE should include an expectation that management has a sound basis for the assertion it makes. A number of respondents also suggested that the IAASB should provide guidance for use by management on the nature and extent of the work it should undertake to support its assertion (or should initiate discussions with other bodies who may provide such guidance). Related to this is the question of whether management, when making its assertion, is entitled to rely on the work undertaken by the service auditor. One respondent expressed concern that some of the proposals in ED-ISAE 3402 may not be practicable, particularly those relating to “suitable criteria” for making assertions (see further discussion below). That respondent recommended that the ISAE not be finalized without the support of representatives of management confirming that the proposals are practicable, which may require pilot testing to establish whether this is the case.
 - (ii) Some service organizations currently rely on their service auditor to assist in preparing the description of the service organization’s system. The ISAE should provide guidance on the implications, including independence implications, of this practice under an assertion-based approach.
 - (iii) The ISAE should make it clear whether direct reporting engagements: (a) should not be undertaken at all; (b) should only be undertaken in certain circumstances (e.g., when required by law or regulation); or (c) may be undertaken at the auditor’s discretion (and if undertaken, what Standard applies).
- (b) Five respondents did not support the proposal.
 - (i) Two were IFAC member bodies whose main reason was for opposing the proposal was that it may discourage use of ISAE 3402 in certain jurisdictions where assertion-based engagements are not prevalent. The primary jurisdiction where assertion-based engagements for service organizations are not prevalent is the USA. The applicable standard in the USA is SAS 70.³ An Exposure Draft of a revised SAS 70 (ED-SAS 70), based on ED-ISAE 3402, was approved by the AICPA’s Auditing Standards Board (ASB) in July this year. One significant change from the current SAS 70 requirements is the proposal to limit reports on controls at service organizations to assertion-based engagements. In fact, ED-SAS

³ Statement on Auditing Standards (SAS) 70, “Service Organizations,” as amended.

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

70 goes further than ED-ISAE 3402 by requiring the service auditor to withdraw from the engagement (or disclaim an opinion if withdrawal is not possible) if management does not provide a written assertion to be distributed to user entities. A comparison, prepared by ASB staff, of ED-ISAE 3402 with the version of ED-SAS 70 was tabled at the ASB's July meeting and is available for information (see table of reference papers at the end of this memorandum).

- (ii) The other three respondents who did not support the proposal were service organizations. The ED was sent to 37 service organizations identified by IAASB members, firms and member bodies around the world, 5 of which responded. One of the 5 supported the proposal, one did not comment on it, and 3 did not support the proposal. Of those 3, two are very large global IT service organizations (Hewlett Packard and IBM), and one is a mid-sized European financial services organization. The reasons provided were:

- *“The level of assurance provided by an assertion based assurance report in comparison with the direct report based assurance report is comparable. Therefore we are of the opinion that explicit statement by management of the service organisation ... does not add substantial value, specifically given the fact that the service auditor will provide assurance based upon the same criteria. Given the fact that SAS 70 - as a broadly used and accepted standard - is based on direct reporting we believe that the acceptance of the proposed standard in the marketplace will benefit from a direct reporting approach.”*
- The proposed requirement would require public release of the name and title of the signatory, which may violate internal policies and privacy legislation.
- If the nature, timing and extent of the service auditor's procedures would not significantly change (as indicated in the explanatory memorandum), then the proposed requirement *“would appear to be only a transfer of liability from the auditors to management in the event that the testing failed to reveal a significant breakdown in controls. Therefore, service organizations would need to perform our own detailed testing to verify those assertions prior to engaging the auditors. While there would be some intrinsic value to such pre-assessment activities, it would substantially increase the overall cost of producing such a report (i.e., staff effort to conduct internal “pre-assessments,” risk assessments and mitigation activities for potential liability, plus the amount paid to the auditors). As such, the audit fees from the firms would need to decrease accordingly or the cost of these reports would greatly exceed the benefits, and we would seek less costly alternatives. Lastly, if the provision of such a statement could potentially result in a liability, our Legal department would demand the right to review and revise wording before granting approval for signature — and I doubt that this would be an option.”*
- *“The example in the draft requires the signature of someone in “management”*

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

or responsible for “governance.” This requirement seems different from the required signatory for the representation letter to the auditors. For example, in our organization, the signatory for the representation letter is a management representative, but at a level that still has direct knowledge and comfort of the existence of the controls being described. In fact, we have included multiple signatures in cases where controls have extended across different domains. However, with the greater visibility and liability potential of this assertion, such management levels would not be permitted to sign such a document. Given my organization’s signatory requirements and the fact that our international footprint would spread certain responsibilities across multiple individuals, it would likely end up being someone in the C-suite, who would have the ability to bind the corporation to such a situation, but who realistically wouldn’t have the same level of direct knowledge. In order for such a signature to occur, we would require sufficient internal testing as mentioned in the previous “Liability” bullet. This requirement may be more feasible with smaller organizations that have sole individuals responsible for the controls from end to end, but the viability for large organizations (which most service organizations typically are) would be questionable.”

- *“... there are control-related assertions that in many cases it is not practical or appropriate for a service organization to make. In particular, the Exposure Draft suggests that a service provider should make assertions as to the design and execution effectiveness of controls. Service providers often operate controls designed or selected by, or under the specific instruction of, customers; in these cases, the applicable customer, not the service provider, typically has contractual and other responsibilities for the design of the controls and their effectiveness.*

... these contractual and other allocations of responsibility should continue to govern the parties’ relationships and ... service providers should not be requested to provide assertions inconsistent with these allocations. Accordingly, ... the ISAE standards should not require service providers to make assertions concerning controls and their effectiveness where contractual or other circumstances warrant. ... (instead) ... any assertions that a service provider makes regarding controls or their effectiveness should be those agreed upon between the service provider and its external auditors consistent with the responsibility allocation for controls that is appropriate to the specific circumstances of the engagement.

... for the reasons stated above, ... assertions made by a service provider to its clients should not be inconsistent with the allocation of responsibility imposed by contracts, applicable laws, or other circumstances and ... the assertions should not implicitly or explicitly change the contractual or other legal relationships between service providers and their customers.

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

... (we therefore propose) that any assertions relating to the adequacy of control design or the effectiveness of controls made by a service organization be made to external auditors pursuant to contractual or other arrangements with those auditors only.”

Suitable Criteria

11. For an assurance engagement to report on controls at a service organization, suitable criteria are required for evaluating whether the description of the system is fairly presented, whether the controls are suitably designed and, in the case of a Type B report, whether the controls have operated effectively. To ensure consistent application of the requirements regarding the suitability of criteria, ED-ISAE 3402 specified the minimum elements of suitable criteria. The IAASB requested views on the appropriateness of these minimum elements.
12. Thirty-five respondents commented on this matter. The preliminary staff analysis indicates that:
 - (a) Twenty-seven respondents supported the minimum elements; either as stated, or with some changes to improve the wording, including:
 - Four respondents who thought that the criteria for evaluating whether the description of the system is fairly presented should be more explicit about the completeness of the control objectives identified in the description, or about the boundaries of the system being described.
 - Two respondents who suggested the minimum elements should be more directly tied back to the characteristics of suitable criteria noted in the International Framework for Assurance Engagements.
 - (b) The remaining seven respondents offered a range of comments and suggestions for improvement, including that the minimum elements:
 - Are too vague, boilerplate, theoretical or transaction-oriented.
 - Do not adequately cover user-designed controls.
 - Should focus more on control objectives, and be clearer regarding the link between control objectives and risks.
 - Should require discrete descriptions of services that are not homogeneous.
 - Should be more directly tied back to the characteristics of suitable criteria noted in the International Framework for Assurance Engagements.
 - Should, with respect to the criteria for evaluating whether the description of the system is fairly presented,:
 - Be more explicit about the completeness of the control objectives identified in the description.
 - Clearly address: the services covered, the period to which the description relates,

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

the control objectives, and related controls; not the entire system (which includes, e.g., the control environment, risk assessment, and the information system).

Disclosure of Sample Sizes

13. The IAASB requested views on whether the description of tests of controls included in a Type B report should include the disclosure of sample sizes only when a deviation from controls is found.
14. Thirty-four respondents commented on this proposal. The preliminary staff analysis indicates that:
 - (a) Twenty-three respondents supported disclosure of sample sizes only when a deviation from controls is found.
 - (b) Three respondents queried the IAASB's rationale for differentiating between cases when deviations are found and cases when they are not.
 - (c) Seven respondents disagreed with the rationale for differentiating between cases when deviations are found and cases when they are not, as articulated in the explanatory memorandum. Three of these respondents suggested details of the factors the service auditor used to determine the sample size (e.g., tolerable error) should be included in the service auditor's report.
 - (d) One respondent believes that a Type B report need not describe the tests of controls undertaken by the service auditor, and therefore need not include disclosure of sample sizes whether or not deviations are found.

Requirements Based on ISAs

15. The IAASB requested views on the inclusion in the proposed ISAE of a number of requirements based on the requirements of ISAs dealing with matters such as using the work of the internal audit function, sampling, documentation, and using the work of a service auditor's expert. In particular, the IAASB requested views on whether all such matters as are relevant had been identified, and whether these matters should be dealt with in proposed ISAE 3402 or in ISAE 3000.⁴
16. Thirty-eight respondents commented on this proposal. The preliminary staff analysis indicates that:
 - Nearly all respondents believe the requirements included are generally appropriate, albeit that there are some topics that one or more respondents think should be dealt with that aren't currently, or should be dealt with in more detail than they currently are. These include: fraud; compliance with laws and regulations; modified opinions; sampling;

⁴ ISAE 3000, "Assurance Engagements Other than Audits or Reviews of Historical."

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

communication of weaknesses in internal control with management and those charged with governance; and agreeing the terms of engagement.

- Most respondents seemed to be of the view that relevant topics should be dealt with in ISAE 3402 for the time being, but that topics with generic application to assurance engagements should be moved to ISAE 3000 when it is next revised.
- Four respondents believe that the requirements of ISAs could be included in the requirements of the ISAE by reference only (e.g. “apply, adapted as necessary in the circumstances”); another 2 respondents thought a far greater number of requirements adapted from the ISAs, and their associated application material, should be included in the ISAE; and one other respondent thought that service auditors who are familiar with ISAs should recognise their utility as guidance without the need for the ISAE to cover the same topics to the same extent as in the ISAs.

Objectivity of External Experts

17. The IAASB requested views on whether ISAE 3000 should include a requirement, similar to that proposed in ED-ISAE 3402, to evaluate whether an external expert whose work is to be used in an assurance engagement, has the necessary objectivity for the purposes of that engagement. This request arose from a likely change to the Code to specifically exclude external experts from the definition of engagement team⁵. If this were to happen, external experts would not be subject to the Code, including its independence requirements.
18. The preliminary staff analysis indicates that most respondents that commented on this proposal agreed that if the definition in the Code were to be changed, ISAE 3000 should be revised to include a requirement to evaluate the objectivity of external experts.

Comments Received on Other Issuers

19. Significant comments received on other issues, based on the preliminary staff analysis, on which Representatives’ views are sought are summarized below.

Non-Financial Controls, and Shared Service Centers

20. Paragraph 2 of ED-ISAE 3402 states:

The focus of this ISAE is on controls at third party service organizations relevant to financial reporting by user entities. It may also be applied, adapted as necessary in the circumstances of the engagement, for engagements to report on:

- (a) Controls at a service organization other than those that are likely to be part of user entities’ information systems relevant to financial reporting (for example, controls that affect user entities’ regulatory compliance, production or quality control).

⁵ The International Federation of Accountants’ Code of Ethics for Professional Accountants.

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

- (b) Controls at a shared service center, which provides services to a group of related entities.

21. Nine respondents made substantive comments on this paragraph. Each called on the IAASB to develop further guidance, either in this ISAE or in a separate ISAE, for broader application with respect to non-financial controls or shared service centers. For example:

- *“Paragraph 2 should not state that the ISAE may also be applied, adapted as necessary in the circumstances of the engagement, to report on engagements other than those relevant to financial reporting by user entities; this will create an expectation that auditors will adapt the standard to the circumstances described, but without providing practitioners with the necessary means to do so. The ISAE as currently drafted cannot serve all such needs.”*
- *“We believe it is unwise to promote opening the door to using ISAE 3402 to a wider range of engagements to which it might not be well suited. We agree that there is a need for assurance standards beyond ISAE 3402 to support a broader range of assurance engagements related to reporting on controls, including those at service organizations and shared service centers, and we encourage IAASB to develop such standards.”*
- *“We support the inclusion of Paragraph 2 in proposed ISAE 3402. However, we do not believe it is quite as simple from a standards perspective as indicating the standard “...may also be applied, adapted as necessary in the circumstances...” This opens the door to various types of reporting with very little guidance. As a result, we are concerned that proposed ISAE 3402 may become a general reporting standard used for different purposes that extend beyond auditor-to-auditor communication on matters of relevance to a user entity’s financial statements, without appropriate guidance. Although we would welcome broader use of proposed ISAE 3402, we believe that additional guidance would be helpful, describing the types of engagements that would be appropriate and how these engagements ought to be conducted”.*

Restrictions on Use or Distribution of the Service Auditor’s Report

22. ED-ISAE 3402 includes a proposed reporting requirement to identify “the purpose(s) and intended users of the service auditor’s assurance report” (paragraph 56(f)). The Application Material in relation to this requirement states:

ISAE 3000 requires that when the criteria used to evaluate or measure the subject matter are available only to specific intended users, or are relevant only to a specific purpose, the assurance report includes a statement restricting the use of the assurance report to those intended users or that purpose. The criteria used for engagements to report on controls at a service organization are relevant only for the purposes of providing information about the service organization’s system, including controls, to those who have an understanding of how the system is used for financial reporting by user entities, and accordingly the service auditor’s assurance report states that it is intended only for use by existing users and their

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

financial statement auditors. (paragraph A28)

23. Seven respondents commented on this matter. One respondent *“strongly encouraged the IAASB to at least acknowledge in the ISAE that it is a wide-spread reporting practice in jurisdictions where allowed by relevant law or regulation ... to insert additional wording (in the service auditor’s report) 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.”* This respondent noted that this is *“clearly in the public interest as (such wording) guards against the possibility of unwarranted reliance on the report by prospective users of it.”*
24. Some respondents recommend that the ISAE *“be tightened to not only identify the purpose and intended user of the report, but to also require that the report state that it is intended **only** for use by existing users and their financial statement auditors (i.e. clearly restrict the use).”*
25. Other respondents argued for a more flexible, principles-based approach, noting that it is not always appropriate to restrict the service auditor’s report. For example, *“In some jurisdictions, assurance reports on controls at third party service organizations are issued on a ‘to whom it may concern basis’. For such jurisdictions, it is important that the conditional nature of paragraph A28 is emphasised; only where criteria are restricted to intended users, or are relevant only to a specific purpose, should the use of the assurance report be restricted.”*
26. A service organization noted: *“The issue arises with potential clients of a service organization. As part of their due diligence activities (prior to signing a contract), such potential clients often require evidence of controls. The evidence typically requested is a current 3rd party assurance report (SAS 70, Section 5970, etc.) covering the site / service of interest. Caveats are typically issued during such sharing such that the potential client is aware that the report would be for “information purposes only”, would offer no guarantees to future compliance, and could not be used for audit or controls reliance. If this standard, in conjunction with ISAE 3000, absolutely prohibits the sharing of reports with potential clients, what mechanism would be available to provide such assurance? Workarounds would end up arising, such as requests to firms to issue confirmation letters, which could end up defeating the purpose of these restrictions.”*

Specimen Control Objectives

27. The explanatory memorandum noted that the IAASB had discussed whether to include specimen control objectives in an appendix to the proposed ISAE. The IAASB took the view that any benefit of providing specimen objectives would be outweighed by the risk that they may be inappropriately used on engagements when objectives specific to the services provided by the service organization should be used.
28. Five respondents noted that it may be helpful for the ISAE to include specimen control objectives (as do certain national publications on service organization engagements); to refer

IAASB CAG PAPER

IAASB CAG Agenda (September 2008)

Agenda Item H.2

Service Organizations – Proposed ISAE 3402

to externally developed objectives such as IT Governance Institute's publication *IT Control Objectives for Sarbanes-Oxley*; or to establish a mechanism for national bodies who develop specimen objectives to share them. These respondents believe that accessible specimen control objectives could be an important step in helping to ensure consistent application of ISAE 3402 in practice.

Matters for Consideration by CAG:

Q1. What are Representatives' views regarding respondents' comments on the matters noted above, in particular:

- Assertion-based engagements?
- Non-financial controls, and shared service centers?
- Restrictions on use or distribution of the service auditor's report? and
- Specimen control objectives?

Q2. Are there any other comments that Representatives may wish to raise?

Material Presented – IAASB CAG REFERENCE PAPERS

Exposure Draft of Proposed ISAE 3402 (including the explanatory memorandum), and all responses received to date.

<http://www.ifac.org/Guidance/EXD-Details.php?EDID=0099>

A comparison, prepared by ASB staff, of ED-ISAE 3402 with the version of ED-SAS 70 tabled at the ASB's July meeting. This comparison was prepared by ASB staff. It should be noted that the final version approved by the ASB, which has not yet been published, may contain changes from the version used in this comparison.

http://www.aicpa.org/download/auditstd/20080728_Agenda_Materials/1B.pdf