Assurance Reports on Controls at a Service Organization— IAASB Task Force Recommendations dated June 2009 in Response to IAASB's Consideration of Significant Comments on Exposure

A. Assertion-Based Engagements

A1. As communicated at the December 2008 IAASB meeting, forty-two respondents commented on the proposal that ISAE 3402[1] be written for application to assertion-based engagements, of which, thirty-six supported the proposal.[2] A number of those respondents made additional suggestions or comments, which the Task Force has considered and, in some cases, has addressed through proposed changes, for example, making it more explicit in the ISAE that the service organization should have a sound basis for its assertion (see new paragraphs[3] 12(a)(iv) and 12(b)(i.1) of Agenda Item 2-B.

A2. Of the six respondents who did not support the proposal, three[4] were IFAC member bodies. One respondent (FSR) thought the ISAE should allow either assertion-based or direct reporting engagements. The main reason offered by the other two respondents for opposing the proposal was that it may discourage the use of ISAE 3402 in certain jurisdictions where assertion-based engagements are not prevalent.

A3. The other three respondents[5] who did not support the proposal were service organizations. The ED was sent to thirty-seven service organizations identified by IAASB members, firms and member bodies around the world, five of which responded. One of the five supported the proposal, one did not comment on it, and three did not support the proposal. Of those three, two are very large global service organizations (Hewlett Packard and IBM). The reasons they provided were discussed at the December 2008 meeting. Generally, it appeared that some service organizations may have been under the impression that their responsibilities under the assertion-based model would be far broader than under a direct reporting model, which is not the case. Further consideration of responses also has led the Task Force to refine its recommended wording with respect to one-to-one engagements.

A4. In the Issues Paper discussed at the December 2008 IAASB meeting, the Task Force noted that some comments from service organizations about the assertion-based requirements appeared to be focused primarily on one-to-one situations where the user

[1] International Standard on Assurance Engagements (ISAE) 3402, "Assurance Reports on Controls at a Service Organization."

[2] AICPA, AIA, CSCPA, CICA, CIPFA, CNCC-CSOEC, DnR, FEE, FICPA, HKICPA, IdW, ICPAS, ICAEW, ICAIre, ICAP, JICPA, NIVRA, SAICA, AUASB, APB, IRBA, Mn Serv, AGA, ACAG, OAGC, GAO, NAO, PA Sask, BDO, DTT, EYG, GTI, KPMG, PwC, ISACA, VanRanst.

[3] Subsequent references to paragraph numbers are to the draft of proposed ISAE 3402 at Agenda Item 2-B unless otherwise noted.

[4] ACCA, FSR, NZICA.

[5] HP, IBM, Robeco.

entity designs the system, which is operated for it by the service organization. ISAE 3402, on the other hand, is aimed at one-to-many situations, where the service organization is responsible for both the design and operation of the system. The Task Force considers that the primary issue is not whether services are provided on a one-to-one or a one-to-many basis, but rather whether the service organization is responsible for the design of the system. In some cases, 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. Paragraph 2(b) now scopes out such cases.

A5. At the December 2008 meeting, some members of the IAASB expressed a concern about the wording of the assertions used in the examples appended to ISAE 3402. The concern is perhaps best reflected in the following comment from the UK Auditing Practices Board's comment letter on the exposure draft: "*It is not clear to us that management will be able to describe the criteria as suggested by paragraphs 15-17 and A5; we observe that in the illustrative reports there is just a 'boiler plate' repetition of the wording of those paragraphs. Further, it is not clear to us how the statement of the criteria, in the form suggested, will actually be of benefit to users. Our discussions suggest that users take assurance from the opinion of the auditor or reporting accountant that the assertions are fair and reasonable, and are less interested in the basis on which management makes its assertions.*"

A6. The Task Force has reconsidered the wording of paragraphs 15-17 and of the illustrative reports. While some minor changes have been made to the wording, the Task Force is not proposing that any substantial changes be made to overcome a perception of "boiler plate" disclosures.

A7. The Task Force considers that explicitly stating the criteria in the service organization's assertion is beneficial to users – it helps users' understanding to know that the service organization is expressly of the view that, for example, relevant information has not been omitted or distorted in preparing the description, and that the risks that threatened achievement of the control objectives stated in the description have been identified and dealt with. It is also beneficial that service organizations are aware of their responsibility to consider such things, which it seems some of them may not have been previously, even though they had been signing representation letters addressed to their auditors.

A8. Further, while users may take assurance from the opinion of the service auditor that the assertions are fair and reasonable and are less interested in the basis on which management makes its assertions, the opinion of the service auditor is without any context and liable to misunderstanding unless the users are made aware of the basis upon which that opinion is formed, which is the role of the criteria. As the International Framework for Assurance Engagements (Assurance Framework) notes: "without the frame of reference provided by suitable criteria, any conclusion is open to individual interpretation and misunderstanding."[6]

A9. The Task Force has, nonetheless, considered whether the criteria can be referred to in the

[6] Assurance Framework, paragraph 35.

service organization's assertion and in the assurance report in a meaningful "shorthand" way, similar to how financial statements refer to an acceptable financial reporting framework as the criteria. IAASB staff is exploring the possibility, albeit relatively remote at this stage, of a representative association of service organizations in Europe undertaking a due process that may see criteria along the lines of those in paragraphs 15-17 being promulgated as generally accepted criteria which could be incorporated into assertions and assurance reports by reference.

A10. A number of respondents suggested that the ISAE should include an expectation that the service organization has a reasonable basis for the assertion it makes. A number of respondents also suggested that the IAASB should provide guidance for use by service organizations on the nature and extent of the work they should undertake to support the assertion (or should initiate discussions with other bodies that may provide such guidance). Related to this is the question of whether the service organization, when making its assertion, is entitled to rely on the work undertaken by the service auditor, and the misunderstanding expressed by one service organization that "*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).*"

A11. To address these matters, the Task Force has added paragraph A3.1 to make it clear that the service organization needs a reasonable basis for its assertion, that the basis need not involve separate evaluations, and that the service auditor's work is not a substitute for the service organization's own processes.

A12. Some respondents also noted that some service organizations currently rely on their service auditor to assist in preparing the description of the system, and asked for the ISAE to provide guidance on the implications, including independence implications, of this practice under an assertion-based approach. As paragraph A2 notes: "the service auditor is subject to independence requirements of the IFAC Code." The Task Force considers the current principles and guidance in the IFAC Code to be adequate and is not proposing to add further application material on this matter. The Task Force notes, however, that requiring that service organization engagements must be assertion-based will also help clarify the relative responsibilities of the service organization and the service auditor, and highlight the self-review threat that would occur if the service auditor were to be involved with preparing the description.

B. Suitable Criteria

B1. At the December 2008 meeting, the IAASB asked the Task Force to consider whether the ISAE could more clearly articulate the relationship between risks, control objectives and suitable criteria. The Task Force was also asked to consider whether the approach adopted on this matter could be reconciled with that adopted in the U.S. Public Company

Accounting Oversight Board's (PCAOB) Auditing Standard No. 5.[7]

B2. The Task Force's view on the relationship between risks, control objectives and suitable criteria is as follows:

(a) *Relationship between risks and control objectives:* As noted in paragraph 9(c), "control objectives relate to risks that controls seek to mitigate." Control objectives typically are stated in terms of what they aim to achieve, for example, that "controls provide reasonable assurance that physically held securities are protected from loss, misappropriation, and unauthorized use." Typically, there would be more than one control in place for each control objective.

(b) *Relationship between control objectives and suitable criteria:* The control objectives (and the related controls) are part of the description of the service organization's system. In order for the service organization to provide a written assertion that the controls related to the control objectives in the description of its system are suitably designed, the service organization uses criteria consistent with paragraph 16:

- The service organization has identified the risks that threaten achievement of the control objectives stated in the description of its system; and
- The controls identified in that description would, if operated as described, provide reasonable assurance that those risks do not prevent the stated control objectives from being achieved.

B3. Paragraph 12(b)(iv) has been revised and paragraph A3.2 has been added to clarify these relationships.

B4. In the Task Force's view, this approach is consistent with that in AS 5.

C. Restricting the Assurance Report

C1. At its December 2008 meeting, the IAASB discussed whether the ISAE should include a requirement to restrict the use of the service auditor's report. The IAASB agreed to adopt a principles-based approach to identifying in the report the intended users of the assurance report and the intended purpose for which that report is provided, recognizing that it is not always appropriate to restrict the use of a service auditor's report.

C2. The IAASB also discussed at the December 2008 IAASB meeting the following wording extracted from ISAE 3000,[8] which was included in paragraph A28: "*When the criteria used 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*,". In this context, the Task Force was asked to consider the implications of whether it is the criteria or the assurance report itself that is publicly available.

[7] AS No. 5, "An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements."

[8] ISAE 3000," Assurance Engagements Other than Audits or Reviews of Historical Financial Information."

C3. In the context of an engagement to report on the controls at a service organization, the Task Force is of the view that the assurance report will only be useful to those who have a sound understanding of the *subject matter*, i.e., the service organization's system, and how it has been used. This is consistent with the suggested paragraph under the heading "Intended Users and Purpose" in the example assurance report at Appendix 2, which states "*This report and the description of tests of controls on pages [yy-zz] are intended only for customers who have used XYZ Service Organization's [type or name of] system, and their auditors, and have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, assessing the risks for material misstatements of customer's financial statements*."

C4. A further issue is what it means to "restrict" the assurance report. In particular, does including a statement of "Intended Users and Purpose," such as that in the paragraph above, constitute a restriction? Or is it necessary for the assurance report to go further than this and specifically state that it is not to be distributed to or used by anyone other than the intended users or used for any other purpose? The Task Force considers it to be unnecessary in the case of ISAE 3402 to require the assurance report to specifically state that it is not to be distributed to or used by others or used for other purposes. However, the Task Force is of the view that the requirement in paragraph 56(f) should be amended to more closely relate to the example reports, so that there is no misunderstanding as to the nature and purpose of that communication.

D. Controls other than Those Related to Services that Are Likely to Be Relevant to User Entities' Internal Control as It Relates to Financial Reporting

D1. At the December 2008 meeting, the IAASB agreed that ISAE 3402 should not state that it can be adapted as necessary for engagements to report on controls other than those related to services that are likely to be relevant to under entities' internal control as it relates to financial reporting, but rather that such engagements should be conducted under ISAE 3000 and that ISAE 3402 may provide guidance in those circumstances. This is now stated in paragraph 2(a).

D2. The Task Force was asked to consider:

(a) Whether this decision should be reflected in the title of the ISAE? The Task Force does not think it is necessary to change the title.

(b) Whether additional guidance on, e.g., understanding the scope of the subject matter and the criteria in such engagements, should be added? The Task Force does not think additional guidance on this matter should be added since the focus of this ISAE is on financial controls, and any guidance in relation to other controls that is brief enough to be incorporated in this ISAE is likely to be so generic as to be of limited or no practical use.

E. Materiality

E1. It was noted at the December 2008 meeting that the conclusion in the sample Type B service auditor's reports (Appendix 2) contains three separate opinions, and that the lead-in wording includes the phrase "in all material respects" to cover all three. The Task Force was asked to consider whether this phrase should apply only to the opinion about the fair presentation of the description of the system.

E2. The Task Force considers that the placement of the phrase "in all material respect" is appropriate, i.e., materiality applies to all three components of the service auditor's conclusion. This is consistent with paragraph 18, which requires the service auditor to consider materiality with respect to the fair presentation of the description, the suitability of the design of controls and, in the case of a type 2 report, the operating effectiveness of controls.

E3. If materiality were excluded from the opinion with respect to design and operating effectiveness of controls, this would give the misleading impression that the assessment of design effectiveness is more "black and white" than it is in fact; and that any, even trivial, deviation observed by the auditor when testing the operating effectiveness of controls would result in a qualified opinion.

F. Experts and Internal Auditors

F1. Paragraph 31, which required the service auditor to refer to the work done by experts when describing tests performed, has been deleted because the service auditor directs the expert and is fully responsible for that expert's work. Mention of that work in the auditor's report would, therefore, suggest a division of responsibility when none is intended.

F2. Paragraph 25, which requires the service auditor to refer to the work done by internal auditors when describing tests of controls performed, has been retained because internal auditors are not under the direct supervision of the service auditor, and therefore this information is likely to be relevant to user auditors in determining the reliance they will place on the service auditor's report.

G. Other Matters

G1. *Preconditions for an assurance engagement*: Paragraph 12 does not adopt the new language from clarified ISAs 210[9] and 200[10] on "preconditions for an audit (assurance engagement)" and "the premise on which an audit (assurance engagement) is conducted." The Task Force considers the current construction to be adequate for this ISAE. New terminology considered during the revision of ISAE 3000 likely will be incorporated in ISAE 3402 by consequential amendment if considered appropriate.

G2. *Inclusive method and subservice organizations:* Paragraph A1.2 has been added to clarify that when the inclusive method is used, the service auditor is fully responsible for opining on all information about the subservice organization that is included in the description. The service auditor, therefore, will ordinarily require full access to the subservice organization, written representations from the subservice organization management etc.

[9] ISA 210, "Agreeing the Terms of Audit Engagements."

[10] ISA 200, "Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing."

For this reason, the inclusive method is hardly, if ever, used unless the service auditor is also the auditor of the subservice organization. Addition of this paragraph is responsive to several comments calling for more guidance on this matter.[11]

H. US ASB's Revision of Statement of Auditing Standards (SAS) 70

H1. As mentioned at the December 2008 IAASB meeting, the US Auditing Standards Board (ASB) approved a proposed Statement on Standards for Attestation Engagements (SSAE), *Reporting on Controls at a Service Organization* (ED-SSAE) in late 2008.[12] The ASB's intention is that the new SSAE will replace SAS 70,[13] which had been accepted in many jurisdictions, in the absence of an ISAE, as the de facto international standard for assurance reports on controls at a service organization. The comment deadline for ED-SSAE was February 2009. The IAASB Task Force and the US ASB Task Force held a joint meeting in March 2009.

H2. The joint meeting was constructive and positive. The Task Forces covered a range of issues, most of which were resolved satisfactorily through discussion. There are, however, four issues that may (subject to decisions made by the IAASB and US ASB) result in substantive differences between ISAE 3402 and the SSAE. These issues are discussed below:

Intentional Acts

H3. The SSAE includes a requirement that, if the service auditor believes that any identified deviations have resulted from intentional acts by the service organization personnel, the service auditor should assesses the risk that the description is not fairly presented, the controls are not suitably designed, and in a type 2 engagement, controls are not operating effectively. ISAE 3402 does not have such a requirement.

H4. The SSAE also includes a requirement to obtain a written representation as to whether management of the service organization has any knowledge of any actual, suspected, or alleged intentional acts by the service organization's management or employees, that could adversely affect the fairness of the presentation of the description of the service organization's system or the completeness or achievement of the control objectives stated in the description.

H5. ISAE 3402 does not include the concept of "intentional acts". In the context of a service organization, intentional acts are likely to be (i) management of the service organization overriding one or more controls to achieve a desired outcome (e.g., control overridden in order to achieve performance objectives), or (ii) personnel of the service organization not performing one or more controls that are needed to achieve a control objective. The Task Force believes that as part of the work effort required under ISAE 3402, such acts would

[11] AICPA, DTT, EYG, PwC 3

[12] Available at: www.aicpa.org/Professional+Resources/Accounting+and+Auditing/Audit+and+Attest+Standards/

[13] 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.

be covered and that it is not necessary to include a reference to “intentional acts” as it may suggest that the service auditor is assuming responsibility for fraud in the context of a financial statement audit, which is covered under ISA 240.[14]

Subsequent Events

H6. The SSAE requires the service auditor to inquire whether management is aware of any events subsequent to the period covered by the description of the system up to the date of the service auditor’s report that could have a significant effect on the controls at the service organization or on the service auditor’s report. If so, and information about that event is not disclosed by the service organization in its description, the service auditor is required to disclose it in the service auditor’s report.

H7. Events that could have a significant effect on the service auditor’s report are the equivalent of what accounting standards are known as “Type 1” events and these are covered in ISAE 3402 (paragraph 47). Events that could have a significant effect on the controls at the service organization subsequent to the period covered by the description are “Type 2” events. These events are not covered in ISAE 3402 because, typically, the service organization would have, under contract with the user entities, an obligation to reach out to them and disclose such events.

Restriction on Use of the Service Auditor’s Report and Description of Tests of Controls and Results Thereof

H8. The SSAE requires the service auditor to restrict the use of the service auditor’s report and description of tests of controls and results thereof to management of the service organization, user entities of the service organization’s system during some or all of the period covered by the service auditor’s report and user auditors. The suggested wording in the example reports is as follows:

> This report and the description of tests of controls and results thereof on pages [yy-zz] are intended solely for the information and use of management of XYZ Service Organization, user entities of XYZ Service Organization’s [type or name of] system during some or all of the period [date] to [date], and their user auditors, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities’ financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

H9. The requirement and suggested wording in ED ISAE 3402 does not include the last sentence of the paragraph above, which was a decision made by the IAASB at the time the exposure draft was issued.

[14] ISA 240, “The Auditor’s Responsibilities Relating to Fraud in an Audit of Financial Statements. “

Description of the Tests of Controls

H10. Paragraph 57 of ISAE 3402 includes a requirement to disclose the period to which the items tested relate. The SSAE has a similar requirement, but we understand that the US Task Force is considering deleting it.

H11. Other differences between ISAE 3402 and the SSAE that are likely to remain, but which the Task Force does not consider to be significant, include:

- Differences in wording, for example, where the ISAE 3402 wording has been aligned, adapted as appropriate, with clarity changes to the requirements of a corresponding ISA.
- The SSAE refers directly to Auditing Standards. For example: *"AU section 350, Audit Sampling" (AICPA, Professional Standards, vol.1) addresses planning, performing, and evaluating audit samples. If the service auditor determines that sampling is appropriate, the service auditor should apply the requirements in paragraphs .31–.43 of AU section 350, which address sampling in tests of controls.*" The IAASB has discussed on a number of occasions whether it is appropriate in the IAASB context for an ISAE to reference an ISA, and has decided against this practice.
- The SSAE has specific requirements for a type 2 engagement with respect to changes in the service organization's controls during the period that are similar to the requirement currently in SAS 70.[15] When developing ED-ISAE 3402, the IAASB agreed not to include such requirements because the description in a type 2 engagement covers an entire period, and so the auditor's procedures will necessarily cover changes during that period without it being specifically required. Nonetheless, paragraph 15(b) has been added to ensure the criteria used to prepare the description are clear that changes during the period need to be described.
- The SSAE makes a specific reference to situations when the service auditor uses members of the service organization's internal audit function to provide direct assistance to the service auditor. Such a reference is not included in ISAE 3402 as ISA 610[16] does not cover such situations.
- The written representations required in the SSAE are at same date as the date of the service auditor's report, whereas the date of the written representations in ISAE

[15] A recent draft of the SSAE has the following wording: "When performing a type 2 engagement, the service auditor should inquire about changes in the service organization's controls that were implemented during the period covered by the service auditor's report. If the service auditor believes the changes would be considered significant by user entities and their auditors, the service auditor should determine whether those changes are included in the description of the service organization's system. If such changes are not included in the description, the service auditor should describe the changes in his or her report and modify his or her opinion on the fairness of the presentation of the description. If the superseded controls are relevant to the achievement of the control objectives stated in the description, the service auditor should determine from management whether it is possible for the service auditor to test the controls before and after the change, and if it is not possible, the service auditor should determine the effect on the service auditor's report."

[16] ISA 610, "Using the Work of Internal Auditors."

3402 has been changed to be a date as near as practicable to, but not after, the date of the service auditor’s assurance report, to be consistent with ISA 580.[17]

[17] ISA 580, “Written Representations. “