Service Organizations – ISAE 3402
Significant issues

Overview

Respondents were generally supportive of proposed new ISAE 3402, "Assurance Reports on Controls at a Third Party Service Organization" (ED-ISAE 3402). While numerous suggestions for improvements were made, only a relatively small number of major issues were raised in addition to the issues upon which the explanatory memorandum accompanying ED-ISAE 3402 sought specific comment.

Issues upon which the Explanatory Memorandum Sought Comment

A. *Assertion-Based Engagements*: Whether the ISAE should be written for application to assertion-based engagements only.

B. *Suitable Criteria:* Whether the minimum elements of suitable criteria specified in ED-ISAE 3402 are appropriate.

C. *Disclosure of Sample Sizes*: 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.

D. *Requirements Based on ISAs:* Whether, and if so to what extent, the ISAE should include requirements based on those in ISAs dealing with such matters as: using the work of the internal audit function; sampling; documentation; and using the work of a service auditor's expert.

E. *Objectivity of External Experts:* Whether ISAE 3000[1] 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 the engagement.

Other Major Issues

F. *Non-Financial Controls, and Shared Service Centers:* Whether, and if so how, the ISAE should deal with non-financial controls, and controls at shared service centers.

G. *Restrictions on the Service Auditor's Report:* Whether the ISAE should include a requirement to restrict the use or distribution service auditors' reports.

H. *Specimen Control Objectives:* Whether to include specimen control objectives in an appendix to the proposed ISAE.

Each of these issues is discussed in more detail below, with the Task Force's comments and recommendations following in boxed text.

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

A. Assertion-Based Engagements

1. 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 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.

2. Forty-two respondents commented on this proposal:

   (a) Thirty-six[2] 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 (APB) 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 felt strongly that the ISAE should not be finalized without the support of representatives of management confirming that the proposals are practicable, which may require testing to establish whether this is the case.

Management's basis for its assertion: Paragraph 25 of ED-3402 notes that "The written representations reconfirming the service organization's assertion about the effective operation of controls may be based on ongoing monitoring activities, separate evaluations, or a combination of the two." It also provides guidance about the nature of ongoing monitoring activities.

The Task Force recommends that paragraph 25 be amended as follows and repositioned to provide guidance on the assertion in paragraph 9(j)(ii):
~~The written representations reconfirming the service organization's assertion about the effective operation of controls~~ In the case of a Type B engagement, the assertion includes that the controls related to the control objectives stated in the service organization's description of its system operated effectively throughout the specified period. This may be based on ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of a service organization and include

[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.

regular management and supervisory activities. Internal auditors or personnel performing similar functions may contribute to the monitoring of a service organization's activities. Monitoring activities may also include using information from communications from external parties, such as customer complaints and regulator comments, that may indicate problems or highlight areas in need of improvement. The fact that the service auditor will report on the operating effectiveness of controls is not a substitute for the service organization's own processes to provide a sound basis for its assertion.

(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.

ED-ISAE 3402 paragraph A2 notes that "the service auditor is subject to independence requirements of the Code." The Task Force considers the current principles and guidance in the Code to be adequate and is not proposing to add further application material on the matter.

(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).

See Task Force recommendation following (b)(i) below.

(b) Six respondents did not support the proposal.

(i) Three respondents[3] were IFAC member bodies. One (FSR) thought the ISAE should allow either assertion-based or direct reporting engagements. The main reason offered by the other two 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.[4] The US ASB Exposure Draft (November 2008) includes a proposal to limit reports on controls at service organizations to assertion-based engagements. In fact, the US exposure draft 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 provided to user entities.

Although this was the intent of ED-ISAE 3402, the Task Force recommends that

[3] ACCA, FSR, NZICA.

[4] Statement on Auditing Standards (SAS) 70, "Service Organizations," as amended.

ISAE 3402 clarifies that it requires 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 provided to user entities.

(ii) The other three respondents[5] 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 service organizations (Hewlett Packard and IBM). 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.

The Task Force notes that ED-ISAE 3402 does not require the service organization's assertion to include an individual's name and title.

- 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.*"

[5] HP, IBM, Robeco.

With respect to any transfer of liability, the Task Force considers it unlikely that a service organization's liability would increase as the service organization is the responsible party for the preparation of the system description and is associated with its publication (and may even often actively promote it in marketing materials). Further, the Task Force is of the view that a service organization, as the responsible party in terms of the International Framework for Assurance Engagements, and having provided a representation letter to the auditor, should be capable in a *one-to-many* situation of asserting its responsibility for the description of the system, the design of the system, and, in a Type B engagement, the operating effectiveness of controls. (See next boxed comment for *one-to-one* situations.)

As noted in the Task Force’s response to paragraph 2(a)(i) above, the intention is to make it clearer in ISAE 3402 that the service organization’s assertion may be based on ongoing monitoring activities, separate evaluations, or a combination of the two, rather than the extensive process envisaged by the respondent. This would not require undue additional expense.

- “*… 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.

  … (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."

These comments are focused primarily on *one-to-one* situations in which the user 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, in which the service organization is responsible for the design and operation of the system. The Task Force considers that this distinction should be more clearly articulated in the ISAE, which could provide additional guidance for adaptation to *one-to-one* situations, including noting that, where the user entity designs the system, there would be no assertion or service auditor's opinion about the whether the system is suitably designed. *One-to-one* situations in which the user entity designs the system often occur when an entity decides to outsource an existing function and few, if any, changes are made to the manner in which that function operates (at least in the short term) even though it is operated by a service organization. In some such cases, the user entity also retains responsibility for the effective operation of controls, perhaps within a control environment established by the service organization. The Task Force will explore the different *one-to-one* scenarios further, and draft guidance as appropriate.

- "*The example in the draft requires the signature of someone in "management" 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.*"

The procedures adopted for signing the representation letter should, generally, be sufficient for signing the assertion. See also the Task Force's comments on the third bullet point above. The Task Force will give further consideration to this matter.

B. Suitable Criteria

3. Thirty-eight respondents commented on this matter:

   (a) Twenty-nine respondents[6] supported the minimum elements; either as stated, or with some changes to improve the wording, including:

   - Four respondents[7] 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[8] 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.

Completeness: The question of completeness of control objectives was discussed extensively prior to exposure. In essence, the concept of completeness is only meaningful when it is tied to a specific circumstance. As neither the service organization nor the service auditor can be sure of the exact circumstances in which the description of the system will be used by any particular user entity or user auditor in a one-to-many situation (e.g., they will know what controls are in place at the user entity), the criteria cannot be absolute about the completeness of control objectives. The application material at paragraph A13 states that the following may assist the service auditor in the required evaluation of whether the stated control objectives are reasonable in the circumstances: "*Where the stated control objectives have been specified by management, are they complete? 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.*" This builds upon the following text in paragraph 16 "*the description is presented to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the service organization's system that each individual user entity and its auditor may consider important in its particular environment.*" The Task Force will consider whether further guidance regarding the internal consistency of the description and control objectives is warranted (e.g, to guard against the description purporting to cover certain topics but omitting control objectives relevant to them).

Boundaries: The Task Force will consider changes to the criteria for matters noted by respondents such as more clearly identifying the boundaries of the system being described.

Characteristics: The intention of the guidance is to elaborate on how the characteristics

[6] AICPA, ACCA, AIA, CICA, CIPFA, CNCC-CSOEC, DnR, FICPA, FSR, HKICPA, IdW, ICPAS, ICAP, JICPA, NIVRA, KICPA, NZICA, AGA, ACAG, OAGC, NAO, PA Sask, BDO, EYG, GTI, ISACA, VanRanst.

[7] CICA, IdW, BDO, VanRanst.

[8] GAO, SAICA.

of suitable criteria noted in the International Framework for Assurance Engagements can be applied in the context of service organization engagement. The Task Force does not consider it necessary to repeat those characteristics in the requirements of the ISAE, but will consider whether it would be helpful to refer to them in the application material.

(b) The remaining nine respondents[9] offered a range of comments and suggestions for major changes, 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, with respect to the criteria for evaluating whether the description of the system is fairly presented, clearly address each of the following elements separately: the services covered, the period to which the description relates, the control objectives, and related controls; and should exclude the control environment, risk assessment, and the information system.

The Task Force will further consider specific suggestions for improvements included in responses, but at present does not plan on recommending major changes.

C. Disclosure of Sample Sizes

4. 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. This is the approach followed in ED-ISAE 3402, and is consistent with current practice in most jurisdictions. The rationale for this approach, as noted in the explanatory memorandum accompanying ED-ISAE 3402, is as follows:

The IAASB concluded that disclosure of sample sizes may not provide, on its own, sufficient information to the intended users to understand the judgments made by the service auditor in their determination; therefore, there might be a risk that intended users may misinterpret the significance of different sample sizes as they relate to user entities. The IAASB concluded, on the other hand, that disclosure of sample size when a deviation from controls is found provides intended users with relevant information as to the rate of deviation encountered in the sample. This information assists user auditors in the performance of their risk assessments.

[9] ICAEW, FEE, HP, AUASB, APB, IRBA, DTT, KPMG, PwC.

5. Thirty-seven respondents commented on this proposal:

   (a) Twenty-six respondents[10] supported disclosure of sample sizes only when a deviation from controls is found.

   (b) Ten respondents[11] queried or disagreed with the IAASB's 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[12] suggested it may be helpful to include in the service auditor's report details of the factors the service auditor used to determine the sample size, for example:

   "We agree that the disclosure of sample sizes on its own may not provide sufficient information to the intended users to understand the judgments made by the service auditor in their determination and that therefore there might be a risk that intended users may misinterpret the significance of different sample sizes as they relate to user entities. However, in our view, this is an argument for the disclosure by the service auditor of not only the samples sizes, but also of the factors and significant judgments made in their determination, rather than an argument for not disclosing sample sizes.

   It appears to us to be rather inconsistent to have service auditors, on the one hand, include a description of tests of controls because it is important for the user auditor to obtain an understanding of the work that has been undertaken by the service auditor to reach his or her conclusion on the operating effectiveness of controls so that the user auditor can form a view as to whether the work is sufficient in the context of the user entity under audit (see the wording of the last two sentences of the Description of Tests of Controls Subsection in the Explanatory Memorandum), but on the other hand, not have service auditors dis-close sample sizes (for those tests) and the factors and significant judgments made in their determination. The fact that not disclosing sample sizes reflects current practice in most jurisdictions does not mean that this practice is a good practice.

   We believe that if ISAE 3402 reports are to be useful to user entities, and in particular, to user auditors, then sample sizes and the factors and significant judgments made in their determination ought to be disclosed in these reports. However, we agree that it is even more important to disclose sample sizes when deviations from controls are detected."

   (c) One respondent[13] 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.

[10] AICPA, CICA, CIPFA, CNCC-CSOEC, FEE, FSR, HKICPA, ICPAS, ICAEW, ICAIre, JICPA, AUASB, IRBA, AGA, ACAG, OAGC, GAO, NAO, PA Sask, Basel, DTT, EYG, GTI, PwC, ISACA, VanRanst.

[11] DnR, FICPA,ICAP, IdW, KICPA, SAICA, KPMG, NIVRA, NZICA, APB.

[12] IdW, SAICA, NIVRA.

[13] ACCA.

The Task Force considers that user auditors need to have information about the nature of the tests of controls the service auditor has performed to be able to make appropriate linkages with their own work at the user entity and thus have sufficient confidence that that tests performed fulfill their own responsibilities under ISA 402 (Revised and Redrafted). However, user auditors do not need to be informed of either the sample size or the details of all the factors the service auditor considered in determining the extent of testing. In part, detailing such factors in a meaningful way that avoids boilerplate disclosures would be unnecessarily burdensome (not only for the service auditor as author, but also for user entities and user auditors as readers). Also, determining the extent of testing is rightly a matter of professional judgment by the service auditor upon which the user auditor is entitled to rely. Information about the extent of testing is needed however when deviations are found, because knowledge of the sample size provides user auditors with relevant information as to the rate of deviation, which assists them in performing their risk assessments under ISA 402 (Revised and Redrafted).

D. Requirements Based on ISAs

6. 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.

7. Forty-one respondents[14] commented on this proposal:

    - Nearly all respondents believe the requirements included are generally appropriate, although one or more respondents identified particular requirements that are not currently covered in proposed ISAE 3402 which they thought should be, or which they thought should be dealt with in more detail than they currently are. These include: fraud; compliance with laws and regulations; modified opinions; sampling; communication of weaknesses in internal control with management and those charged with governance; and agreeing the terms of engagement.
    - Most respondents mentioned 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[15] believe that the requirements of ISAs could be included in the requirements of the ISAE by reference only (e.g., "the service auditor should apply ISA XXX, adapted as necessary in the circumstances of the engagement"); two respondents[16]

[14] AICPA, ACCA, AIA, CICA, CIPFA, CNCC-CSOEC, DnR, FEE, FICPA, FSR, HKICPA, ICPAS, ICAEW, ICAIre, ICAP, JICPA, NIVRA, KICPA, NZICA, SAICA, AUASB, APB, IRBA, Mn Serv, AGA, ACAG, OAGC, GAO, NAO, PA Sask, Basel, IOSCO, BDO, DTT, EYG, GTI, KPMG, PwC, VanRanst.

[15] NZICA, SAICA, OAGC, GAO.

[16] IOSCO, IdW.

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[17] thought that service auditors who are familiar with ISAs should recognize their utility as guidance without the need for the ISAE to cover the same topics to the same extent as in the ISAs.

The Task Force continues to believe that it is not appropriate to include the requirements of ISAs in the requirements of the ISAE by reference only, because to do so would not result in sufficient clarity as to which requirements of the ISAs should be applied or how they ought to be adapted. The Task Force will review individual suggestions for inclusion of specific requirements and application material from additional ISAs. It should be noted that the IAASB's Strategic Plan calls for a project proposal to review ISAE 3000 to be considered in early 2009. Additional work to determine which aspects of particular ISAs should be included in ISAE 3402 will inform the project to review ISAE 3000 should the IAASB decide to go ahead with that project.

E. Objectivity of External Experts

8. 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 team.[18] If this were to happen, external experts would not be subject to the Code, including its independence requirements.

9. 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.

As noted above, the IAASB's Strategic Plan calls for a project proposal to review ISAE 3000 to be considered in early 2009. Feedback on this proposal will inform the project to review ISAE 3000 should the IAASB decide to go ahead with that project.

F. Non-Financial Controls, and Shared Service Centers

10. 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).

[17] ACCA.

[18] The International Federation of Accountants' Code of Ethics for Professional Accountants.

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

11. Nine respondents[19] 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."*

Non-financial controls: For the reasons stated by respondents, the Task Force agrees that ISAE 3402 should not state that it can be adapted as necessary for engagements to report on non-financial controls, but rather that ISAE 3402 should state that such engagements should be conducted under ISAE 3000 and that ISAE 3402 may provide guidance in those circumstances.

Shared service centers: The Task Force is conscious of the fact that ISA 402 (Revised and Redrafted) is scheduled for approval at the December IAASB meeting, and that a similar issue is under consideration with respect to that ISA. The Task Force's preliminary conclusion is that shared service centers should not be covered by ISAE 3402 although the standard may provide guidance where the component auditor specifically reports on controls. The Task Force will consider this issue again in light of the IAASB's discussion of ISA 402 (Revised and Redrafted) at its December meeting.

[19] CICA, CNCC-CSOEC, FEE, ICAEW, IdW, NIVRA, EYG, PwC, ISACA.

The Task Force's recommendation for amendment to paragraph 2 is as follows:

2. ~~The focus of t~~This ISAE applies where the services provided by a third party service organization~~s~~ that are covered by the service auditor's assurance report are likely to be relevant to user entities' internal control as it relates to financial reporting ~~by user entities~~. It may also provide guidance ~~be applied~~, adapted as necessary in the circumstances of the engagement, for engagements under ISAE 3000 to report on controls~~:~~

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

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

G. Restrictions on Use or Distribution of the Service Auditor's Report

12. 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)). Paragraph A28 of the Application Material states in relation to this requirement:

> 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 financial statement auditors.

13. Seven respondents commented on this matter.

14. Three respondents[20] recommended that the ISAE explicitly require restriction of the assurance report, for example, *"paragraph 56 (f) (should) 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).*"

15. Two respondents[21] 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*

[20] NAO, NZICA, KPMG.

[21] FEE, NIVRA.

relevant only to a specific purpose, should the use of the assurance report be restricted." Another respondent (PwC) *"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."*

16. A service organization (HP) 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.*"

The Task Force does not consider that there should be a requirement to restrict in all cases the users of the assurance report or the purpose for which that report may be used. It does, however, agree that it is appropriate to adopt a flexible approach, recognizing that in some jurisdictions it is common to restrict the report. It therefore recommends revision of paragraphs 56(f) and A28 as follows:

56(f) Identification of the intended purpose(s) and ~~intended~~ users of the service auditor's assurance report. 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.

A28. ~~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.~~ In some cases, t~~T~~he criteria used for engagements to report on controls at a service organization are relevant only for the purposes of preparing and auditing the financial statements of existing user entities. ~~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.~~ In such cases, the service auditor's assurance report states that it is restricted ~~intended~~ ~~only~~ for use only by existing (and past) users and their financial statement auditors because only they have a sufficient understanding of how the system has been used for financial reporting.

H. Specimen Control Objectives

17. 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.

18. Seven respondents[22] noted that it would be helpful for the ISAE to: include specimen control objectives like those in certain national publications on service organization engagements (APB, GTI, ISACA); refer to externally developed objectives such as the IT Governance Institute's publication *IT Control Objectives for Sarbanes-Oxley* (FSR, KPMG, APB, ISACA); or establish a mechanism for national bodies who develop specimen objectives to share them (ICAEW). These respondents believe that accessible specimen control objectives could be an important step in helping to ensure consistent application of ISAE 3402 in practice.

The Task Force considers that the ISAE stands apart from the specific control objectives used by service organizations, and that it is not the role of the IAASB to prepare, refer to, or endorse any specific objectives. It acknowledges, however, that some IFAC member bodies, national standard setters (NSS) and others, such as ISACA, develop specimen control objectives, the use of which could lead to more consistent application of ISAE 3402 in practice. The Task Force therefore suggests that this topic be raised at the next IAASB / NSS meeting to determine whether there is potential for collaboration between NSS and others to develop international implementation guidance that includes specimen control objectives.

[22] FEE, FSR, GTI, ICAEW, APB, KPMG, ISACA.

[BLANK PAGE]