

30 May 2008

International Auditing and Assurance Standards Board (IAASB)
International Federation of Accountants
545 Fifth Avenue, 14th Floor
New York, NY 10017

Via e-mail to edcomments@ifac.org

RE: Proposed International Standard on Assurance Engagements (ISAE) 3402, “Assurance Reports on Controls at a Third Party Service Organization”

We very much appreciate the opportunity to provide comments and recommendations to the International Federation of Accountants (IFAC) for the proposed “Assurance Reports on Controls at a Third Party Service Organization.”

These comments and recommendations are offered on behalf of both ISACA and the IT Governance Institute (ITGI), international, independent thought leaders on IT governance, control, security and assurance. A brief description of the organizations is provided at the end of this letter.

General Comment

We are responding principally from an information technology (IT) perspective. We believe the proposed guidance will be useful to auditors and congratulate IFAC on its accomplishment.

Responses to IFAC Questions

Our response includes several suggestions that would add clarity to the document’s objectives. Based on our review of the proposed IFAC guidance, our responses to questions are as follows.

1. The proposal that the ISAE be written for application to assertion-based engagements. In particular, the IAASB would welcome any views on whether there are situations in which it would not be possible or practicable for management of the service organization to provide an assertion.

Page 13, Scope of this ISAE, paragraph 4, states that “...an assurance engagement may be either an ‘assertion-based’ engagement or a ‘direct reporting’ engagement.” We suggest adding to page 6 the definition of “direct reporting” from page 13: “A direct reporting engagement, under which all relevant information is included in the service auditor’s assurance report and there is no public assertion.” The standard should also identify any

situations in which “direct reporting” is appropriate and clearly indicate that in all other situations “assertion-based” is either required or strongly preferred.

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

On page 18, paragraph 15 (a), we suggest adding a bullet for “complementary user controls.” It also would be helpful to include the International Assurance Framework definition of “suitable criteria.”

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

We believe it is not necessary to disclose sample size, except in situations in which exceptions are found.

Other Comments

Consistent Use of the Term “Materiality”

The term “materiality” is not used consistently in the exposure drafts of ISA 402 and ISAE 3402. To avoid confusion, we suggest that the phrase “material with respect to financial statements being reported on” should be used consistently throughout ISA 402 and a phrase such as “material with respect to the system and controls being reported on” should be used consistently throughout ISAE 3402.

Reference to an IT Control Framework

It would be helpful for user auditors to be able to utilize a model set of control objectives or an IT control framework to assess whether the control objectives included in management’s assertion are relevant, appropriate and complete and whether user entity controls are required to address the risks identified. We suggest including an illustrative set of control objectives in an appendix or providing references to sources for such control objectives. One publication that might be helpful in this regard is the IT Governance Institute publication *IT Control Objectives for Sarbanes-Oxley, 2nd Edition* (www.isaca.org/sarbanes-oxley), which focuses on IT controls relevant to financial reporting and is available for download at no charge. Other useful information, including the comprehensive framework for IT governance and control called COBIT, is also available for download free of charge on the ISACA (www.isaca.org) and ITGI (www.itgi.org) web sites. These publications also might be beneficial in the audits of smaller companies and for practitioners, user entities and service organizations in developing nations. We suggest including such references as appropriate.

Internal Audit Function

Paragraph 9 (h) includes “others” (such as a compliance or risk department) in the definition of the internal audit function. These so-called “others” may lack the objectivity, training, experience and a set of professional standards that exist for professional auditors. Consequently, we do not believe they should be included as part of the definition of “internal audit function.” If the intent is to permit the service auditor to use/rely on the work of employees other than professional internal auditors, this should be dealt with as a separate definition and in paragraphs other than those dealing with “Using the Work of an Internal Audit Function.” However, we view such “others” as regular employees who would be performing important control and

monitoring functions, but whose work cannot be relied upon in the same manner as that of a professional internal audit function.

Shared Service Centers

Although proposed guidance ISAE 3402 could be applied to shared service centers, such guidance in its current form is not adequate for this purpose. Without such guidance, we suggest either deleting the reference to shared service centers or stating that it is *not intended to cover shared service centers*. Otherwise it requires significant additional clarification of how it would apply. Some troublesome areas include:

- Since the ISAE provides audit standards for external auditors, would ISAE 3402 require an enterprise to obtain and send a report on shared service center controls to its subsidiaries that use the shared service center?
- Where internal audits of the shared service center are regularly performed, is an external, third-party audit also required?
- How would different regulatory and statutory audit requirements in each country be addressed in a multinational company that uses a shared service center internationally?


* * *

With more than 75,000 members in more than 160 countries, ISACA (www.isaca.org) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor (CISA) designation, earned by more than 60,000 professionals since inception; the Certified Information Security Manager (CISM) designation, earned by 9,000 professionals since it was established in 2002; and the new Certified in the Governance of Enterprise IT (CGEIT) designation.

The IT Governance Institute (ITGI) was established by ISACA in 1998 to help ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly allocated, and IT performance is measured. ITGI developed *Control Objectives for Information and related Technology* (COBIT) and Val IT, and offers original research and case studies to assist enterprise leaders and boards of directors fulfill their IT governance responsibilities and help IT professionals deliver value-adding services.

Thank you for this opportunity to relay our comments regarding the IFAC guidance. ISACA and ITGI believe we are uniquely positioned to bring value to any future similar projects. Please feel free to call on us if we can be of assistance to IFAC in any way, including task forces, committees, work groups or just for reference purposes.

Respectfully submitted,



Everett C. Johnson, CPA
Chair, Professional Issues Working Group
Past International President, 2005-2007
ISACA (www.isaca.org)
IT Governance Institute (www.itgi.org)

Attachment—Additional Comments and Suggestions

General comment: It would seem ISAE 3402 would need to be adopted and in effect before the effective date of the redrafted ISA 402.

Page 5, Type of Report, second paragraph, second-to-last line states "...there is therefore no clear need for a report that covers a period of time." Without a stated rationale for this statement, it is confusing and should be either deleted or rephrased. Since it is unclear whether this background information will be included in the final standard, we suggest it be added, with the rationale, to an appropriate paragraph in the standard.

Page 8, Control Objectives. Please see our previous comment under *Reference to an IT Control Framework*.

Paragraph 2 indicates that this ISAE may be adapted for engagements to report on controls at a service organization other than those relevant to financial reporting. Suitable criteria have been published by the AICPA/CICA for Trust Services engagements to report on security, process integrity, confidentiality, privacy and availability. Since such criteria are relevant to these other types of reports and have been developed for international use, we suggest that they be referenced in a footnote.

Page 13, paragraph 3, indicates that a service auditor may be engaged to provide two additional types of reports on controls at a service organization. However, this list does not include—and, therefore, might be interpreted to preclude—other types of reports, such as a report under AICPA and CICA standards on one or more Trust Services principles (e.g., security, processing integrity or privacy). This paragraph should be reworded along the following lines: "... A service auditor may also be engaged to provide additional reports, which are not dealt with in this ISAE. Such reports *might include ...*"

Page 14-15, paragraph 9, should include a definition of "date of the report." Since standards and practices on this subject vary (e.g., last date of field work, date of final partner review of the work), a definition would be helpful. Without such a definition, paragraphs 47 and 48, dealing with subsequent events, might be inconsistently applied.

Page 15, paragraph 9 (a), defines the "carve-out method." The carve-out method is also referred to in paragraphs 56 (c) and A14. Additional guidance regarding the carve-out method should be included to avoid misinterpretation or misapplication. Guidance should be provided in areas such as:

- To what extent can processing and controls be performed by the subservice organization and still permit the service auditor to issue a meaningful report on the service organization? This is particularly significant for situations in which the service organization acts as an intermediary between the user and the subservice organization and performs few, if any, control functions affecting the user's internal controls.
- How would the existence of a subservice auditor's report affect the service auditor's decision whether to use the carve-out method? This response differs if the subservice auditor's report was qualified or noted significant exceptions.

Page 15, paragraph 9 (g), defines the “inclusive method.” The inclusive method is also referred to in paragraphs 56 (c) and A14. Additional guidance regarding the inclusive method should be included to avoid misinterpretation or misapplication. Guidance should be provided in areas such as:

- Does the service auditor need to obtain management representations from the subservice organization’s management?
- If the audit work on the subservice organization is performed by a different auditor (i.e., subservice auditor):
 - Does the service auditor need to take responsibility for the work of the subservice auditor or can the service auditor refer to the subservice auditor?
 - Should the testing performed and deviations identified by the subservice auditor be included in the service auditor’s report?
 - What are the considerations for a service auditor when all or a significant proportion of the processing and controls are at the subservice organization and covered by the subservice auditor’s report (i.e., has the service auditor done enough work to express an opinion)?
 - What should the service auditor do if he/she concludes that the work of the subservice auditor cannot be relied upon?

Page 15, paragraph 9 (i), (ii), (b), and paragraph 9 (j), (ii), (b). We suggest the following rewording for clarification: “The controls ... were suitably designed *to achieve the stated control objectives* ...”

Page 17, Acceptance and Continuance, paragraph 12 (b):

- (i) A frequent practice, particularly in first-time engagements, is for the service auditor to assist management in preparing the system description. We suggest adding clarification that the service auditor may assist management in preparing the system description as long as management takes ultimate responsibility for this description.
- (iii) This paragraph could benefit from clarification as it currently leaves the reader with questions, such as the following:
 - Where control objectives are specified by law or regulation or another party (the exception noted), is management no longer responsible for stating the control objectives?
 - Where control objectives are specified by another party (such as a user group), would one expect that the use of the service auditor’s report would be restricted only to members of the user group, thereby precluding its use by other customers of the service organization who are not user group members?
 - Shouldn’t management also acknowledge its responsibility for the completeness of the stated objectives? This would preclude management from omitting important control objectives that management expects would not be achieved.
 - What is meant by the “risks that threaten their achievement”? This appears to be a new concept. Are these referring to the inherent limitations of internal control, to the risks that the control is mitigating, or to other types of risk (e.g., competence of personnel, control environment, conditions at user entities)? If these include risks related to user entities, the service organization’s management is unlikely to be able to take responsibility for them. Examples and clarification would be helpful here.

Page 17, Acceptance and Continuance, paragraph 12. We suggest including other matters as follows:

- 12 (c) Management agrees to provide the service auditor with an appropriate written representation (as described in paragraphs 42 to 44).
- 12 (d) Management agrees to restrict the distribution and availability of the service auditor's report to only those parties described in the service auditor's assurance report section titled *Intended Users and Purpose*.

Page 18, paragraph 15 (a):

- Complementary user entity controls should be added to this list.
- Subparagraph (iv) could be clarified or examples provided. For example, do these "events and conditions" include establishing access permissions, limitations and conditions for use in applying automated control procedures, etc.?

Page 19, paragraphs 19 to 21. Please see our previous comment under *Reference to an Internal Audit Function*.

On page 20, paragraph 24, clarification is needed as to what types and how much internal audit work the service auditor can rely on. For example, should the service auditor perform all the tests of the most important controls (sometimes referred to as "key controls")? Also, it would be helpful to include a brief discussion about review and tests of internal audit work on which the service auditor relies.

Page 20, paragraph 25, requires the service auditor to identify and separately describe any tests performed by internal audit. This is inconsistent with paragraph 24, which requires the service auditor to take responsibility for the work of internal audit and make no reference to internal audit in the service auditor's assurance report. Paragraph 25 should be revised to require the service auditor to describe tests performed by internal audit as though they had been performed by the service auditor, thereby achieving consistency with paragraph 24.

Pages 20 and 21, Using the Work of a Service Auditor's Expert:

- Clarification is needed as to what types and how much of the work of an external expert can be used by the service auditor. For example, could an external expert perform substantially all of the work and the service auditor still issue an opinion?
- Clarification is also needed as to whether, and, if so, how, this guidance applies to contracted personnel who perform as members of the service auditor's engagement team.

Page 21, paragraph 31, requires the service auditor to identify and separately describe any tests performed by an external expert. This is inconsistent with paragraph 30, which requires the service auditor to take responsibility for the work of an external expert and make no reference to an external expert in the service auditor's assurance report. Paragraph 31 should be revised to require the service auditor to describe tests performed by an external expert as though they had been performed by the service auditor, thereby achieving consistency with paragraph 30.

Page 22, paragraph 35:

- We believe the determination of which controls at the service organization are necessary to achieve the stated control objectives is a responsibility of the service organization's management and not of the service auditor. The service auditor's responsibility is to assess

whether those controls identified by management are suitably designed to achieve the stated objective. This paragraph should be revised accordingly.

- Management also is responsible for identifying the risks that threaten the achievement of the stated control objectives. However, we are troubled with this concept and what is actually intended here. Please see our previous comment on paragraph 12 (b) (iii), last bullet. Subparagraph 35 (a) should be revised to clarify the meaning of such risks and the related responsibility of the service auditor.

Page 22, paragraph 36, should be revised to indicate that the "... service auditor shall test those controls that the *service organization's management* has determined are necessary ..." Please see our comment on paragraph 35 above.

Page 22, paragraph 38. We suggest including "relevant risks" as one of the matters to be considered by the service auditor when determining the extent of tests of controls.

Page 23, paragraph 42:

- We find the first sentence of this paragraph confusing and awkward. Please revise to clarify to whom "them" refers, who makes the "appropriate inquiries" and for what purpose, and that a written representation must be obtained, not just requested. We believe the intent is "The service auditor shall obtain written representations from senior management (or those charged with governance). Such representations should be based on senior management's knowledge and belief and on appropriate inquiries of and/or representations from lower levels of management sufficient to provide a basis for senior management's representations. Such representations: ..."
- Subparagraph (c)—We recommend that "any fraud or irregularities that have occurred" be added to the list of items to be disclosed to the service auditor.

Page 27, paragraph 57. We believe the service auditor should not have to report all deviations. Very minor deviations should not need to be reported.

Page 28, paragraph A3. This sentence is long, awkward and unclear. Please reword into shorter sentences and clarify.

Page 35, paragraph A22. We believe that the previous year's exceptions/deviations should be considered in establishing the nature and extent of testing. Further, there are situations in which the nature and extent of testing can be modified based on evidence from prior engagements. For example, a service auditor may have tested certain application controls without deviations in a prior engagement. In the absence of any changes in the system or controls in the current engagement, the service auditor may limit the tests of application controls and place additional reliance on general computer controls over system changes. We believe these concepts should be included in this paragraph.

Pages 41 to 44, Examples 1 and 2 of the Service Auditor's Assurance Reports, third paragraph. We do not understand why ethical requirements have been singled out here above and beyond other requirements and standards. Please clarify.