



LEADING THE IT GOVERNANCE COMMUNITY

3701 Algonquin Road, Suite 1010 Telephone: 847.253.1545
Rolling Meadows, Illinois 60008, USA Facsimile: 847.253.1443 Web Sites: www.isaca.org and www.itgi.org

25 April 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: International Standard on Auditing (ISA) 402 (Revised and Redrafted), “Audit Considerations Relating to an Entity Using a Third Party Service Organization”

Gentlemen:

We very much appreciate the opportunity to provide comments and recommendations to the International Federation of Accountants (IFAC) for the proposed “Audit Considerations Relating to an Entity Using 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

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

More Important Comments

Paragraphs 12 and A17

On page 12, paragraph 12, Assessing the Risks of Material Misstatement, we believe that a user auditor could misinterpret what we believe to be the intent of this paragraph. We suggest adding a second condition to the description of the situation for which assurance of control at a service organization is needed. We suggest rewording the paragraph as follows.

12. When the user auditor's risk assessment includes an expectation that controls at the service organization are operating effectively for certain assertions for which controls are applied only at the service organization or controls at the user entity depend on the effectiveness of controls at the service organization, the user auditor shall obtain audit evidence about the operating effectiveness of those controls at the service organization from one or more ...

In addition, examples of such controls should be included in paragraph A17. One such example of a control might be an important exception report used by the user entity, but produced by processing at the service organization based on criteria provided by the user entity.

Further, either paragraph 12 or paragraph A17 should clarify:

- (a) To what extent a user auditor can rely on other types of assurance reports on controls at service organizations, such as a report issued under AICPA attestation or CICA assurance standards on one or more Trust Services principles, such as processing integrity or security
- (b) Whether a service-organization report based on a "direct-reporting engagement" would continue to be satisfactory

Consistent Use of the Term "Materiality"

The term "materiality" is not used consistently in 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, particularly from small and medium-sized practices, to be able to reference an IT control framework to assess whether the combination of user entity and service-organization controls are appropriate to address the risks identified. One publication that might be helpful in this regard is the IT Governance Institute publication *IT Controls for Sarbanes-Oxley, 2nd Edition* (www.isaca.org/sarbanes-oxley), which focuses on IT controls relevant to financial reporting and is available at no charge. Other useful information, including the comprehensive framework for IT governance and control called COBIT, is also available 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.

Responses to IFAC Questions

Our response includes several suggestions that would add clarity to the document's objectives. (*Italicized words indicate modifications.*) Based on our review of the proposed IFAC guidance, our response to question 1 (a) is as follows.

1. Paragraph 4 of proposed ISA 402 (Revised and Redrafted) allows for the ISA to be adapted, as necessary in the circumstances, to situations where an entity uses a shared service center which provides services to a group of related entities. In particular, the IAASB would welcome views as to whether: (a) The ISA is capable of being adapted for these circumstances.

On page 3, paragraph 5, Shared Service Centers, the second sentence states, “While the focus of proposed ISA 402 (Revised and Redrafted) is on an entity’s use of a third party service organization, the IAASB is of the view that it may also be applicable, adapted as necessary in the circumstances, to situations where an entity uses a shared service center that provides services to a group of related entities.”

Although the proposed guidance ISA 402 could be applied to shared service centers, such guidance in its current form is not adequate for this purpose. We suggest either deleting it 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 ISA provides audit standards for external auditors, would ISA 402 require an organization 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?

Other Comments

We have included additional, more detailed, comments and suggestions in the attachment, which we believe will help clarify the guidance.

* * *

With more than 65,000 members in more than 140 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 55,000 professionals since inception; the Certified Information Security Manager (CISM) designation, earned by 7,000 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 advance international thinking and standards in directing and controlling an enterprise’s information technology. ITGI developed *Control Objectives for Information and related Technology* (COBIT®), now in its fourth edition, and offers original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

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,

A handwritten signature in black ink, appearing to read "Everett C. Johnson". The signature is fluid and cursive, with the first name "Everett" and last name "Johnson" clearly distinguishable.

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 before the effective date of the redrafted ISA 402.

Page 13, paragraph 15 states: “In determining the sufficiency and appropriateness of the audit evidence provided by a Type A or Type B report in support of the user auditor’s opinion, the user auditor shall be satisfied as to the service auditor’s professional reputation, competence and independence. (Ref: Para. A29)” Because there are consulting firms and others issuing reports similar to those set forth in the proposed ISAE 3402, it is important to clarify in paragraphs 15 and A29 that the user auditor should consider reports only from firms of professional accountants.

Page 14, paragraph A4, the last sentence states, “In these circumstances, the user entity may be unable to, or may elect not to, implement effective controls over these transactions.” We are unsure what this sentence means or is intended to communicate. If the user entity elects not to implement control over these transactions, what does this mean? Please clarify whether this means the user entity needs to rely solely on controls at the service organization or whether no reliance on any controls is intended.

We believe that user auditor requests relating to the service organization or service auditor *always* should be made through the user entity. A direct relationship between the user auditor and either the service organization or the service auditor is inappropriate. The following comments relate to such user auditor requests:

- Page 15, paragraph A6, the last sentence before items (a) and (b) states, “A user auditor, for example, may request a service auditor to perform procedures on the user auditor’s behalf, such as:” We suggest that this be reworded to indicate that the user auditor’s request may be made through the user entity or directly to the service auditor and to indicate the type of report or review of the service auditor’s work that would be appropriate in these circumstances.
- Page 21, paragraph A32: “The user auditor may also request the service auditor, on the user auditor’s behalf, to gain access to the user entity’s records maintained by the service organization.” We suggest that this sentence be reworded as follows: “The user auditor also may request, through the user entity and the service organization, the service auditor ...”

Page 17, paragraph A13, the first sentence states, “Knowledge obtained through the user auditor’s experience with the service organization may also be helpful in obtaining an understanding of the nature of the services provided by the service organization.” It would be helpful to clarify the type of experience the user auditor would be obtaining about the service organization. Does it relate to experience from other clients? Normally a user auditor would not have much interaction with a service organization.

Page 18, paragraph A19, cites examples where an auditor “may perform procedures to update the information in a Type A report.” Consider adding another option, namely obtaining a letter from the service organization describing any changes that have occurred.

Page 18, paragraph A20, we suggest changing the second line from “therefore specific tests of controls...” to “therefore *certain* tests of controls.”

Page 21, paragraph A29, the third line adds a consideration of “whether the service auditor is subject to regulatory oversight.” What if the service auditor is not? In other words, a service auditor could be providing service organization reports and never have its work reviewed. See also our comments for Page 13, paragraph 15.

Page 21, paragraph A31, the last sentence states, “In such circumstances, the user auditor may need the consent of the service auditor before making such a reference.” Would this allow an auditor, when issuing a qualified audit opinion, to indicate that the service auditor’s report of XYZ service organization led to the qualified opinion? It could be a challenge to obtain the consent of the service auditor before making such a reference.