

SERVICE ORGANIZATIONS – ISA 402**SIGNIFICANT ISSUES****1. Existing ISA Risk Assessment Requirements**

- 1.1 The ISA 402 project proposal stated that one of the objectives to be achieved in this project is to “align the standards and guidance with the audit risk standards.” The key provisions in the audit risk standards related to an entity’s use of a service organization are summarized below.
- 1.2 ISA 315.02 requires the auditor to “...obtain an understanding of the entity and its environment, including its internal control, sufficient to identify and assess the risks of material misstatement of the financial statements whether due to fraud or error, and sufficient to design and perform further audit procedures.” ISA 315 builds on this by requiring the auditor’s understanding to include “the nature of the entity” (ISA 315.25), “business risks that may result in material misstatement of the financial statements” (ISA 315.30) and, in particular, “internal control relevant to the audit” (315.41), which includes the information system. The required understanding of the information system is described in ISA 315.81, which states:

The auditor should obtain an understanding of the information system, including the related business processes, relevant to financial reporting, including the following areas:

- The classes of transactions in the entity’s operations that are significant to the financial statements.
 - The procedures, within both IT and manual systems, by which those transactions are initiated, recorded, processed and reported in the financial statements.
 - The related accounting records, whether electronic or manual, supporting information, and specific accounts in the financial statements, in respect of initiating, recording, processing and reporting transactions.
 - How the information system captures events and conditions, other than classes of transactions that are significant to the financial statements.
 - The financial reporting process used to prepare the entity’s financial statements, including significant accounting estimates and disclosures.
- 1.3 The auditor is then required to “...identify and assess the risks of material misstatement at the financial statement level, and at the assertion level for classes of transactions, account balances and disclosures” (ISA 315.100).
- 1.4 Based on this understanding and risk assessment, ISA 330.07 requires the auditor to “...design and perform further audit procedures whose nature, timing, and extent are responsive to the assessed risks of material misstatement at the assertion level.” These further audit procedures include tests of controls, as described in ISA 330.23:

When the auditor’s assessment of risks of material misstatement at the assertion level includes an expectation that controls are operating effectively, the auditor should

perform tests of controls to obtain sufficient appropriate audit evidence that the controls were operating effectively at relevant times during the period under audit.

- 1.5 Finally, ISA 330.25 also requires the auditor to perform tests of relevant controls to obtain audit evidence about their operating effectiveness when “...the auditor has determined that it is not possible or practicable to reduce the risks of material misstatement at the assertion level to an acceptably low level with audit evidence obtained only from substantive procedures...”

1.6 *Issues*

- (a) *Based on the definition of internal control, including the information system, and the requirements for understanding internal control and performing risk assessments in ISA 315, the task force believes that if a service organization performs activities that are part of the entity’s information system relevant to financial reporting then the service organization is performing activities that are part of the entity’s internal control relevant to the audit. Does the IAASB agree?*
- (b) *Accordingly, if a user organization is performing activities that are part of the entity’s internal control relevant to the audit, the user auditor performing an ISA audit should understand the activities performed by the service organization that affect the entity’s information system relevant to financial reporting, and should consider those activities in identifying and assessing the risks of material misstatement. Does the IAASB agree?*
- (c) *If the user auditor’s risk assessments are based on the expectation that controls at a service organization are effective, or if it is not possible or practicable to reduce the risks of material misstatement at the assertion level to a an acceptably low level with audit evidence obtained only from substantive procedures because of the activities performed by the service organization that are part of the user organization’s internal control, the auditor should perform (or otherwise obtain evidence of) tests of controls at the service organization? Does the IAASB agree?*

2. Types of Service Organizations to be Encompassed by ISA 402

2.1 As is evident from the Appendix to Agenda Item 4, there are many different types of service organizations used today, whose services span a number of dimensions, e.g., from:

- Traditional activities (such as payroll), to newer frontiers (such as application service provision over the internet);
- Routine activities (such as call centres), to complex arrangements where the service organization exercises considerable discretion (such as the controllership function);
- Peripheral activities (such as building maintenance), to core activities (such as investment management for a retirement benefit plan); and
- Activities that clearly have a direct effect on the user organization’s internal control as it relates to the preparation of the financial statements (such as payroll processing), to broader activities that are not directly related to finance and accounting (such as waste disposal).

- 2.2 With respect to this last dimension (financial statement effect), requests for reports about broader controls appear to be increasing. For example, in some jurisdictions where managed funds are highly regulated, requests for reports on controls over prudential compliance are becoming more common. Other requests are also starting to emerge, e.g., controls over: money laundering, and compliance with privacy legislation and environmental legislation regarding waste disposal outsourcing, which may be seen as having some relationship to the audit of the financial statements with respect to the entity's compliance with laws and regulations (ISA 250). Still broader requests may be likely in future, e.g., controls over research methodologies with respect to clinical drug trials, which in some cases could affect the going concern assumption (ISA 570). While such activities may be of interest to user auditors in some cases, current practice for service auditors' reports does not ordinarily encompass them because service auditors' reports address only service organization activities that directly affect a user organization's information system relevant to financial reporting. It could be argued that the appropriate principle for coverage in ISA 402 is that the auditor should consider the activities of a service organization and related controls when, had those activities been conducted "in house," the auditor would have had a responsibility under ISA 315 and ISA 330 to consider them. This would exclude broader activities in most cases.

2.3 Issue

- (a) *As described in Issue 1 above, the task force believes the auditor should consider the activities of a service organization when they directly affect the user organization's internal control as it relates to the preparation of the financial statements, and consequently, the auditor's risk assessment procedures and responses to risks. Should the auditor also consider the activities of other types of service organizations where those activities do not directly affect the user organization's internal control as it relates to the preparation of the financial statements? If so, what is the rationale for requiring the auditor to do so, what boundaries should be specified within the context of current ISAs, and should ISA 402 provide guidance on such situations?*

- 2.4 In some cases, a shared service centre that provides services "internally" to a group of companies may be considered a service organization from the perspective of the auditor of a component of the group. This may be particularly relevant to the auditor of the component when the service provided is, e.g. the internal audit function, or indeed the controllership function¹. The task force is still considering the implications of this and the appropriate cut-off between ISA 402 and ISA 600 with respect to shared service centres.

3 Procedures to Obtain Information and Evidence

- 3.1 In some cases, a user organization may use a service organization that performs very limited activities, and the user organization may have designed and implemented controls over the activities performed by the service organization. In other cases, the service organization's activities may be more significant and the user organization may not have implemented such

¹ Where a third party provides such services, ISA 402 would apply.

controls, but instead may be relying on the controls at the service organization. Based on the answers to the questions in Issues 1 and 2 above, the user auditor may determine that information is needed about the design and implementation of the activities and relevant controls at the service organization in order to perform the risk assessment. The user auditor may also determine that evidence is needed about the operating effectiveness of the controls at the service organization as part of the audit of the financial statements of the user organization.

- 3.2 The task force believes that the user auditor may obtain information about the design and implementation of relevant controls at the service organization by directly performing procedures at the service organization, engaging another auditor to perform procedures at the service organization, obtaining information from manuals, internal audit reports, or other documents, or obtaining information from a report on the controls at a service organization issued by a service auditor.
- 3.3 Similarly, the task force believes the user auditor could obtain evidence about the operating effectiveness of controls at the service organization by directly performing tests of the controls at the service organization, engaging another auditor to perform tests of controls at the service organization, or by obtaining a report on tests of controls performed by a service auditor.

3.4 *Issues*

- (a) *Does IAASB agree? Are there any other ways for the user auditor to obtain information about the design and implementation of relevant controls at a service organization, or to obtain evidence about their operating effectiveness?*
- (b) *Whilst ISA 402 would acknowledge that the user auditor may specifically engage another auditor to perform procedures at the service organization, the task force believes that ISA 402 need not further address this situation because such other auditor is under the direction of the user auditor. Does the IAASB agree?*
- (c) *The task force is yet to consider in detail the factors that a user auditor will need to consider in evaluating the sufficiency and appropriateness for the user auditor's purposes of the information provided by a report on the controls at a service organization. National standards identify matters such as the following (some of which are discussed elsewhere in this Agenda Item), and the task force would welcome any views the IAASB may have on these, or related matters at this stage:*
- Whether the report is Type A or B (see Issue B.4 (a) in Agenda Item 4-B);*
 - The level of detail in the description of tests performed (see Issue B.4 (b) – (d) in Agenda Item 4-B);*
 - The level of assurance obtained by the service auditor (see Issues C.3 (a) and (b) in Agenda Item 4-B);*
 - The level of detail in the description of controls;*
 - How sample sizes are determined and whether they should be disclosed;*

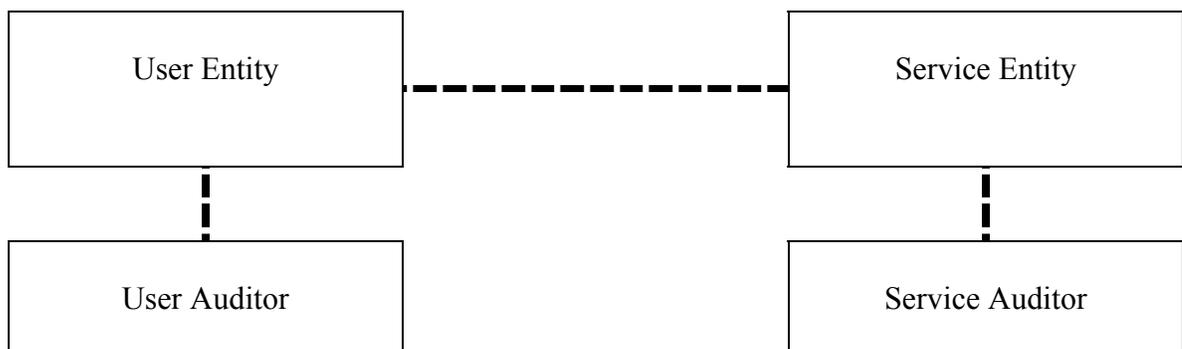
- *Whether samples tested included items from the particular user organization (or from a particular category, e.g., in a multinational service organization, the country in which the user organization operates);*
- *The terms of the service auditor’s engagement (in some jurisdictions it is common for the service auditor’s engagement letter to be included with their report);*
- *The date of the report vis-à-vis the user organization’s balance sheet date;*
- *The reputation, experience etc. of the service auditor;*
- *The effect of identified control weaknesses; and*
- *Whether the user auditor was consulted in determining the nature, timing and extent of the procedures carried out by the service auditor.*

4. Definitions and Relationships

4.1 The task force discussed the definitions of user organization, service organization, user auditor, and service auditor, and the relationships between these parties. The task force believes it is important to recognize the following relationships:

- The *user organization* has a direct relationship with its auditor and with its service organization(s).
- The *user auditor* has a direct relationship only with its client (the user auditor) whose financial statements it is auditing.
- The *service organization* has a direct relationship with its customers (the user organizations) and its own service auditor.
- The *service auditor* has a direct relationship only with its client (the service organization).

4.2 This set of relationships is depicted on the following chart.



4.3 In most jurisdictions, there is no direct relationship between the service auditor and user auditor. Communications between service auditors and user auditors are conducted through their respective clients who have entered into the servicing relationship. For example, it is common for service auditor reports to be distributed by service organizations to their user

organizations who in turn distribute the report to their user auditors, rather than being distributed from the service auditor directly to user auditors. Similarly, a user auditor’s questions, requests for additional information or other communications about a service auditor report are often communicated by the user auditor to the user organization who then communicates them to the service organization for communication to the service auditor.

- 4.4 In some jurisdictions, however, there may occasionally be a direct relationship between the user auditor and the service auditor if the user auditor directly contracts with a service auditor to perform specific work on behalf of the user auditor. This is the case particularly in those situations where the role of the service organization is evolving from a transaction processing model towards a controllership model, and the level of communication and the relationship between user auditor and service auditor is changing, e.g. where specified substantive procedures are performed by the service auditor on behalf of the user auditor. The task force is still considering a number of questions regarding such situations, including whether the auditor being engaged is part of the engagement team, "an other auditor" under ISA 600, "Using the Work of Another Auditor" or a "service auditor." While ISA 402/ISAE 3402 will likely need to address such situations, they are expected to be dealt with as a special case rather than the norm.
- 4.5 However, a service auditor has an indirect relationship with user organizations and user auditors, in that the report issued by a service auditor to its client is expected to be used by user organizations and user auditors. Some standard setters have reflected the relationship between a service auditor and users of a service auditor’s report by requiring a paragraph in a service auditor’s report that identifies intended users, e.g.: the sample report in SAS 70² says:

This report is intended solely for use by management of XYZ Service Organization, its customers, and the independent auditors of its customers.

- 4.6 In other jurisdictions, guidance specifically addresses the legal issues relevant to the relationship between the service auditor and the user auditor, e.g., AAF 01/06³ says:

Reporting accountants disclaim responsibility and liability to customers’ auditors, having regard to the responsibility of customers’ auditors for their own audit reports and for determining to what extent (if any) the assurance report amounts to sufficient appropriate audit evidence for the purposes of their audit of a relevant customer’s financial statements.

- 4.7 ISAE 3000.49 (f)⁴ addresses this matter to some extent, in a generic sense, by saying:

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

² Statement on Auditing Standards (SAS) No. 70, *Service Organization*, as amended, issued by the AICPA’s Auditing Standards Board.

³ Technical Release AAF 01/06 “Assurance reports on internal controls of service organizations made available to third parties,” issued by the Audit and Assurance Faculty of the ICAEW.

⁴ International Standard on Assurance Engagements (ISAE) 3000, “Assurance Engagements Other than Audits or Reviews of Historical Financial Information.”

assurance report should include] a statement restricting the use of the assurance report to those intended users or that purpose: in addition, whenever the assurance report is intended only for specific intended users or a specific purpose, the practitioner considers stating this fact in the assurance report.[#] This provides a caution to readers that the assurance report is restricted to specific users or for specific purposes.

[#] While an assurance report may be restricted whenever it is intended only for specified intended users or for a specific purpose, the absence of a restriction regarding a particular reader or purpose does not itself indicate that a legal responsibility is owed by the practitioner in relation to that reader or for that purpose. Whether a legal responsibility is owed will depend on the legal circumstances of each case and the relevant jurisdiction.

4.8 *Issues*

- (a) *Should ISA 402 (and ISAE 3402) be written primarily on the assumption of no direct relationship between the service auditor and the user auditor?*
- (b) *In addition to defining the terms noted in paragraph 4.1 above, should ISA 402 and/or ISAE 3402 address the relationships between these parties?*
- (c) *Should ISA 402 and/or ISAE 3402 provide guidance that reinforces this relationship through such matters as the degree to which a user auditor may rely on the work of a service auditor based on e.g., the distribution of the report, the addressee of the report, and the engagement letter?*

[Blank Page]