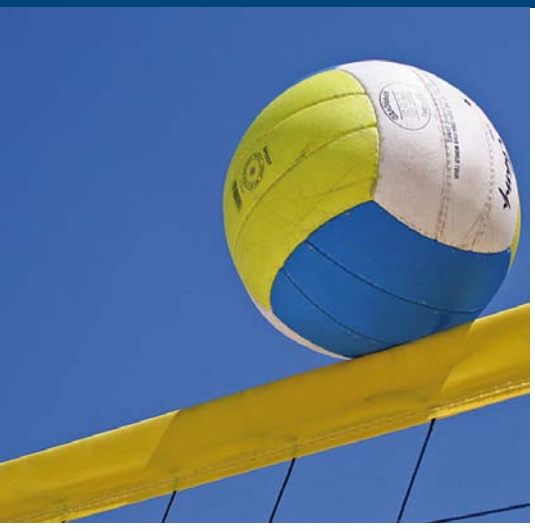

SAS 70 revised

ISAE 3402 will focus on financial reporting control procedures

Jaap van Beek and Marco Francken

Many people now know that the current SAS 70 standard is going to be fundamentally changed. Expectations are that it will become possible to provide third parties with other (and greater) assurance concerning various responsibilities in the areas of internal control. This new standard, the ISAE 3402 "Assurance Reports on Controls at a Service Organization" was accepted by regulators in September 2009, but it remains to be seen if the changes are, in fact, so great. The differences and the impact of this new standard practice will be further discussed in this article.

Introduction

Beginning in mid-2011, service providers currently using SAS 70 reports will change to a new standard for reporting internal controls to third parties. Based on the recently ratified ISAE 3402 standard, this new standard will in practice replace current standard SAS 70 and, as a result, establish an international basis for practice, supported by the IFAC (International Federation of Accountants) and the ASB (US Auditing Standards Board). In the Netherlands, this standard will be included in the COS standards. The US version is not expected to differ much from the IFAC standard. There is also some question about the extent to which this new standard materially differs from the SAS 70 and what this means for service providers. Are adjustments needed, and what are the constraints and challenges of the new standard? What are the alternatives if parts of ISAE 3402 do not meet the needs of users?

Timetable for implementing the new standard
The proposed effective date for the new standard will affect reporting periods ending after mid 2011 (the final date is yet to be decided). Since service auditor reports cover periods of between six and twelve months, service auditors may use the new standard from the second quarter of 2010. The IAASB and the ASB will allow early adoption of the new standard, so that reports under the new standard can be expected in the second half of 2010.

J.J. van Beek
is a partner at KPMG IT Advisory. He has over twenty-years of experience in all areas of IT auditing, with an emphasis on evaluating and advising on the automated information provision of financial institutions and insurers. He is the leader of the IT attestation service line in the Netherlands (SAS 70).

vanbeek.jaap@kmpg.nl

M.A. Francken
is a director at KPMG IT Advisory. He is working on various internal control procedures from an audit and advisory perspective. In this respect, he focuses on IT controls in relation to the financial statements. He is also actively involved in IT Attestation (SAS 70) and External Audit support services at KPMG IT Advisory the Netherlands.

francken.marco @ kpmg.nl

The authors would like to thank Han Boer and Ronald van Langen of KPMG for their comments on an earlier version of this article.

Background of the international standard

Country-specific	Worldwide
• Canadian Institute of Chartered Accountants (CICA) Handbook section 5970 • US Statement on Auditing Standards (SAS) No. 70 • UK Audit and Assurance Faculty Standard (AAF) • AU Guidance Statement (GS) 007 • JP Audit Standards Committee Report No. 18 • Germany IDW PS 951	• ISAE 3402 as default standard for countries without existing standard *or* • ISAE 3402 as basis for updates of current local standard

Table 1: **Country-specific and global standards for internal control reports**

Many service providers use an SAS 70 report (Statement on Auditing Standards No. 70) to provide insight into their methods of managing internal control procedures. SAS 70, which has been the standard for reporting on the internal control framework of a service organization, is now being replaced.[1] Although the new standard is specifically intended for the reporting of the internal control procedures in a service organization insofar as they relate to the annual audit of a user organization, it is being implemented more widely in practice and actually exceeds the possibilities offered by SAS 70.

Due to the lack of a global standard, several countries are already using standard practices that, in effect, underlie the ISAE 3000 standard, in order to develop their own national standards (see Table 1) ([Bello9]).

The International Auditing and Assurance Standards Board (IAASB) has been eager to establish a global standard for the reporting of control procedures related to outsourced processes. They developed the International Standard on Assurance Engagements (ISAE) 3402. Interested parties were able to provide feedback on the first draft of the text until May 2008,[2] and the IAASB subsequently published a second draft in June 2009, with final approval coming in September 2009. According to current expectations, ISAE 3402 will become the standard for reporting on control procedures in cases involving the outsourcing of activities relating to financial statements around mid-2011, but may also be used even before that time (early adoption). Strictly speaking, an international template already exists and may be adopted by national organizations with or without adjustment. The replacement of US standard SAS 70 was implemented in the US early in 2010. In the Netherlands, NIVRA and NOREA have also begun preparations to adopt ISAE 3402. In the case of NIVRA, this involves COS 3402, and for NOREA, it concerns Directive 3402.

1 SAS 70 has not officially existed for some time now: the really relevant standard (now actually the regulations) is AU 324 (Professional Standards, vol. I, AU SEC 324). Yet no one speaks about AU 324, because the term SAS 70 has been widely established.

2 The responses can be found at: http://www.ifac.org/IAASB/Exposure-Drafts.php.

ISAE 3402: main changes

After many years of discussion, one international standard has been established as a basis for national practice. Yet this innovation has somewhat disappointed service report users. For instance, ISAE 3402 is reserved for controls relating to (a part of) the user's financial accounting. For reporting on other processes, reference has to be made to ISAE 3000, since the new standard does not allow the reporting of control procedures for non-financial processes, not even when financial and non-financial processes are combined. The framework and guidance based on the standard can, of course, be useful for reporting on control procedures outside the scope of financial statements, but in using it in this way, the service organization and the auditor must be aware of the possible (significant) differences in applying criteria for materiality concept, use, *etc.* In effect, the form and content of the report will change little and the scope not at all, despite the likely name change (SAS 70 disappearing and being replaced by the international SAR, the Service Auditor's Report). We will return later in the article to the applicability of ISAE 3000 to other (non-financial) processes.

The main differences between SAS 70 and the ISAE 3402 standard are:

- SAS 70 is an auditing standard. The new standard is an "assurance" standard (an "attestation" standard in the United States). The main changes here involve management being required to include a statement on the operation of the control procedures in the report. This underlines management's responsibility for establishing a system of controls, but it does not mean that, under the new standard, management establishes a separate function to document and evaluate controls. Of course, the service auditor must be able conclude that management has a reasonable basis with which to support its statement. The auditor's report will be "direct reporting" and not derived from the management statement.

Furthermore, the audit criteria (suitable criteria) on which management and the auditor assess internal controls have been included in the ISAE 3402 standard, which was not the case for SAS 70. In this context, suitable criteria (fairness of presenta-

tion, suitability of design and operating effectiveness) are to be explained in detail. The standard therefore gives a minimum set of criteria, which the control framework of the service organization must meet. The service auditor shall also assess the adequacy of the criteria and measures taken. The effect of this change will show up in practice, as it is to be expected that the criteria shall receive more explicit attention and the degree of freedom in formulating controls shall decline slightly, since the criteria have to be clearly identified in the audit objectives. The authors expect that connections between the controls and criteria shall remain complex and, therefore, a matter of professional judgment.

- Viewed somewhat superficially, the auditor's opinion will seemingly change in the manner explained below. In fact, substantive differences between the old and new standards remain small, with two notable exceptions. First, the auditor shall issue one opinion covering three elements in the assessment criteria. Second, a Type II report shall also involve an opinion covering all three elements throughout the entire period. In a SAS 70 Type II, only the performance of the control activities (Chapter III) is reviewed, while the new standard will test all relevant COSO elements such as monitoring, information & communication, *etc.* (hence current Chapter II as well). In practice, this could mean more work, depending on the relevance of Chapter II in relation to the control procedures under Chapter III.

Suitable criteria

Fairness of presentation. The auditor shall determine if the description is faithful. Does the description clearly and transparently indicate the elements that are within the report's scope and/or have to be implemented by the user? Does the description contain sufficient detail and accurate information to enable an assessment about the control procedures? Are the control procedures in the description actually implemented?

Suitability of design. The auditor shall verify if a control procedure is appropriately designed so that the control objectives can be achieved with a reasonable degree of certainty. Even if an individual control procedure is insufficient, the objectives may still be achieved with a reasonable degree of certainty due to the effectiveness of other control procedures.

Operating effectiveness. The auditor shall ascertain if the control procedure is effective. Before a control procedure may be re-used, various pieces of evidence must be considered and tested to determine if it functions as described.

Furthermore, there remain two possible types of reports (Type I for design and implementation of control procedures, and Type II for operation). A report must cover at least six months. The testing activities must be described in the report, while indicating the "sample sizes" used, in case of any relevant exceptions. The current SAS 70 standard has limited the distribution circle for the reports. The new standard 3402 requires the auditor's opinion to explicitly indicate the users and the intended use. The auditor may consider using additional terminology in relation to limiting the distribution circle.

Audit criteria are included in the ISAE 3402 standard

Alternative for non-financial processes: ISAE 3000

A number of practical objections regarding the existing SAS 70 remain valid. For this reason, the ISAE 3402 only applies to processes related to financial statements, therefore matching the scope of SAS 70. However, current practice reveals that service providers would like to have a broader scope. They wish to have independent assurance about the outsourcing of *non-financial* components, including:

- Continuity of the service provider
- Compliance with SLA agreements
- Accuracy of the information flows between (for example) pension administration and the Board
- Communications to stakeholders (governance)

In practice, this extension of the SAS-70 scope is usually included in Section IV of the report and is therefore not included in the opinion contained in the service auditor's report.

ISAE 3402 is not intended to provide such extension, but there is a good alternative: namely ISAE 3000. This standard already exists and is included by NIVRA in COS 3000, while NOREA has NOREA guideline 3000 for it. Unlike ISAE 3402, the standard is more "free form," only requiring a number of mandatory elements to be covered. These include the definition of the audit object, the control measures implemented at a particular moment or over time, and qualitative factors, such as reliability, continuity and exclusivity. Where appropriate, the auditor will have to assess the applicability of quality criteria in order to prevent – figuratively speaking – an irrational task from being accepted. Assurance reports can be prepared in a manner virtually identical to the SAS 70 reports. It is also possible to opt for a "short" variant just covering the mandatory SAS-70 components, in which audit objectives and control procedures

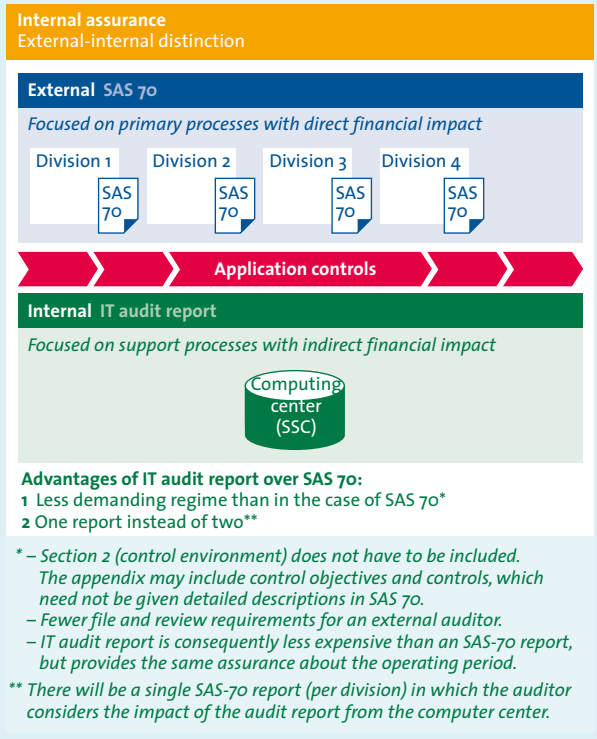

Figure 1: **Internal assurance: internal and external**

are indicated in an appendix as supplements to the opinion. In this case, the report actually consists of a statement referring to the relevant control objectives and control procedures in the appendix. The procedures are similar to TPAs (Third Party Announcements), which have been used in the past.

Such a "short" variant is also an alternative for those cases where an internal service center provides assurance to the internal users of its services. Such situations are prevalent in cases where an IT service center provides various departments with infrastructural IT services, as illustrated in Figure 1. The auditors of the data center provide an IT audit report (without assurance) to the divisions for the SAS 70 reports that the divisions provide to their customers.

Strictly speaking, an SAS 70 is not used internally, nor is an ISAE 3000. An IT audit report is therefore also illustrated in Figure 1.

An SAS 70 is generally larger and can therefore be more expensive than an ISAE 3000 report. In the case of the ISAE 3000 report providing the same assurance, the appendix to the declaration can be limited to the audit objectives and control procedures, and Section II (of the SAS 70) may be omitted, if desired. The testing by the auditor can still be the same, but this need not be indicated in the assurance report. As mentioned, the ISAE 3000 is free form.

Besides the previously mentioned examples of the use of ISAE 3000, consideration can also be given in this structure to new/other areas about which assurance is to be provided, such as statements regarding confidentiality, privacy, governance and soft controls. In practice, there is an increasing need for assurance in these areas.

In fact, the development of the new ISAE 3402 standard again demonstrates the value of ISAE 3000 as an alternative. An acceptable standard is therefore already available for (IT) service organizations desiring more than the current (SAS 70) and new (ISAE 3402) standards allow.

Review of similarities and differences with the current SAS 70 standard

Differences:

- The new standard is an assurance standard and no longer an audit standard, which means, among other things, that management is made explicitly accountable. The opinion of the service auditor will look slightly different because a single opinion is given about a variety of elements.
- In Type II, the main changes are that management is required to include a statement on the operation of the control procedures in the report.
- In a Type II report, all elements in the report are evaluated in terms of all three criteria throughout the entire reporting period, resulting in one opinion.

Similarities:

- The anticipated control effort required from management and the service auditor is expected to remain materially the same.
- There are still two types of reports (Type I and II).
- Type II reports should cover a minimum period of six months.
- Restrictions in use remain substantially the same.
- Testing by the service auditor will remain part of the report.
- Sample sizes are only mentioned when exceptions are identified.

Sensible choices for the service organization

Service organizations may now choose which standard best meets their needs, based on the ways in which ISAE 3402 or 3000 are incorporated in national guidelines. If the report predominantly concerns financial processes relevant to the annual audit, a standard derived from ISAE 3402 will be the most appropriate. In all other cases, the use of the ISAE 3000 standard will be preferred, in which it is still possible to employ the same structure and degree as in the case of ISAE 3402.

If the decision is made to adopt the new standard, the most important activities for the service organization are:

- *Understanding the changes.* In particular, this concerns the need for a management statement to be included in the report.
- *Consultation with service auditor.* This especially relates to the expected impact on the service auditor's report, his or her duties and the impact on any sub-service organizations. The new 3402 standard states that an inclusive report not only has to describe and test the controls used by the sub-service organization, but the organization-wide control procedures as well (Chapter II). This eliminates all the advantages of an inclusive report, and it would be more practical if a sub-service organization prepared its own report. For the sake of report users, it would be beneficial to hold timely discussions on the needs and consequences of early adoption.
- *Transition plans.* These should include organizing internal training programs, coordination with the legal department (if any), developing a communications plan and reviewing existing reports and processes to determine how the new criteria will be met. In any event, attention should be given to whether there is an adequate basis for the new management to become assertion based. Unlike SOx 404, not all management controls must be first tested by management before being tested by the auditor.

Conclusion

ISAE 3402 is the new standard for reporting on the management of outsourced processes that relate to the financial reporting of the outsourcing party. This new standard will hardly differ from the SAS 70 standard, so it will not require the service organization to implement any material adjustments. If a service organization wishes to provide insight and assurance about non-financial processes, it is better to choose the ISAE 3000 standard. Moreover, this alternative already exists! In the opinion of the authors, this decision represents the main challenge involved in providing service organizations with more options in demonstrating the accountability of their services with the desired degree of assurance.

References

[Bello9] Sander van Bellen, Marco Francken and Joyce Grotencleas, *De pensioenwereld*, 2009.

[Houto9] Dennis Houtekamer and Remco de Graaf, *ISAE 3402: einde van de SAS 70 in zicht?*, January 2009.

[ISEA09] *Proposed New International Standard and Amendments on Assurance Engagements ISAE 3402, Assurance Reports on Controls at a Third Party Service Organisation*, IAASB, July 2009.