

Out with SAS 70, in with SSAE 16 and ISAE 3402: **10 steps to a successful transition**

Since April 1992, the U.S. Statement on Auditing Standards No. 70 (SAS 70) has been the leading standard for guidance regarding assurance reports for service organisations. For almost 20 years, service organisations, user organisations and auditors have relied on SAS 70 reports to understand and gain assurance that proper controls relevant to user entities' internal control over financial reporting are in place at service organisations.



From mid-2011, new standards have taken effect. A number of factors have contributed to the need for these new standards:

- the globalisation of information technology and business process outsourcing generated the need for an international standard;
- a dynamic regulatory landscape helped create the need for additional information regarding internal control over financial reporting; and
- U.S. convergence with international standards.

The result is the recently released Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organisation (SSAE 16),¹ which is effective for periods dated on or after June 15, 2011.²

By design, SSAE 16 is closely aligned with the previously released global standard, International Auditing and Assurance Standards Board (IAASB) International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organisation (ISAE 3402).³

Key definitions

- service organisation: company providing outsourced service;
- subservice organisation: company providing service to the service organisation;
- service auditor: auditor performing SAS 70 review of the service organisation;
- user organisation: organisation receiving the outsourced service; and
- user auditors: external auditors of the organisation receiving the outsourced service.

ISAE 3402 was issued in December 2009 but shares with SSAE 16 the effective date of June 15, 2011. Both standards provide guidance for service auditors.⁴ The differences between SSAE 16 and ISAE 3402 are minimal as a result of efforts to converge the U.S. standard with the international one. The service organisation and the service auditor need to be aware of the differences when a service auditor is engaged to provide a report.⁵ Where differences do occur, the U.S. standard is generally more conservative. Key differences between SAS 70 and SSAE 16 are identified in the appendix.

¹ The full text of SSAE 16 is available for purchase at www.aicpa.org.

² The AICPA has indicated that this standard will be incorporated or codified into the attestation standards as AT 801. See AICPA FAQs — New Service Organisation Standards and Implementation Guidance at www.aicpa.org/InterestAreas/AccountingAndAuditing/Resources/AudAttest/AudAttestGuidance/DownloadableDocuments/Final%20Service%20Orgs%20FAQ.pdf.

³ The full text of ISAE 3402 is available at www.ifac.org/iaasb/Meeting-FileDL.php?FID=4998.

⁴ The U.S. guidance for user auditors is retained in AU Section 324, Service Organisations.

⁵ See Exhibit B: Comparison of Requirements of Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization*, With Requirements of International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*.

The new U.S. and international standards provide service organisations and professional firms with the guidance necessary to obtain or deliver reports for service organisations. Whether a service organisation has been receiving SAS 70 reports for several years or is just now evaluating the need for an assurance report, there are a number of steps management at service organisations can take to make a successful transition to — and be prepared for — the new assurance standards.

Although SSAE 16 focuses on internal control over financial reporting, it can be used as a guide for reporting on other types of controls, such as those related to compliance and operations objectives, under the AICPA's other attestation standards.

Stepping into the new standards

The new standards impose some additional responsibilities upon the service auditor and service organisation management. The impact of these responsibilities on the service organisation will differ from company to company, but it is anticipated that larger, more complex service organisations may need more time than smaller, single-location service providers to make any necessary process changes to transition to the new standards.

There are 10 steps management at service organisations can take to smooth the transition to the new standards. Management should begin this work immediately. The steps can be grouped into three action-oriented categories:

- establish a transition strategy with a service auditor;
- assemble assertions and suitable criteria; and
- initiate a communication plan.

Establish a transition strategy with a service auditor

To get started, service organisations should engage a service auditor to discuss the following three areas:

1. Work with an experienced and knowledgeable service auditor to better understand the implications of transitioning to SSAE 16 and ISAE 3402.

It is critical for a service organisation to meet with a service auditor that understands the implications associated with the new standards. Service auditors at accounting firms that are already familiar with the principles of suitable criteria and management assertions from other standards are likely to be better equipped to guide service organisations.

2. Work with the service auditor to determine whether multiple service auditor reports will be necessary.

Service auditors in most countries will be required to follow the local (country) audit standards. This means that U.S. certified public accounting firms will be required by the American Institute of Certified Public Accountants (AICPA) standards to follow SSAE 16. However, service auditors for organisations that have global operations or a global customer base may also wish to receive a service

auditor's report under ISAE 3402. A service organisation should discuss with its service auditor whether multiple reports under different standards will be beneficial to or required by its customer base. Although additional effort will be required to issue multiple reports, the effort can be minimised with proper planning and execution.

3. Assemble assertions and suitable criteria

Consistent with SAS 70, the new standards require the service auditor to obtain a written assertion from management of the service organisation. However, the new standards require that management's written assertion accompany the service auditor's report. Further, management's assertion must identify the suitable criteria on which it is based. The following additional steps should be taken with respect to developing management's assertion:



4. Review your company's existing monitoring and/or testing processes to determine if they are sufficient to support the written management assertion required by SSAE 16 and ISAE 3402.

Management of the service organisation will be required to provide a written assertion to accompany the service auditor's report, in which the service auditor will attest to the following:

- the fairness of the presentation of the description of the service organisation's system
- the suitability of the design of the controls to achieve the related control objectives stated in the description
- for a Type II report, the controls operated effectively throughout the specified period to achieve the stated control objectives

Management at service organisations with a formal or informal monitoring and testing process in place to support an assertion will likely be more comfortable with providing an assertion to customers in reports under the new standards. The standards do not provide guidance on how much work management of a service organisation should perform to make its assertion. It does, however, indicate that the service auditor should evaluate management's assertion as part of its procedures. Management will also need to be comfortable that it has developed and implemented suitable criteria on which to base the assertion.

The normal planning process is a good time for management to revisit the scope of the controls to be covered by the service auditor's report, formalise descriptions and criteria, and reassess the relevance of risks associated with services. If a service organisation has objectives that are stale and do not minimise risk in a meaningful way, it may be time to

scrap those control objectives in favour of new criteria that better benefit the company and its clients.

The amount of additional work necessary to transition to the new standards will be dependent upon how mature management's monitoring and testing processes are today. If management believes that existing monitoring and testing activities represent a robust process that supports its assertion, the only items likely to be necessary to move to the new standards may be the inclusion of additional disclosures in the report. For other organisations, a new approach will need to be taken regarding monitoring and testing activities.

5. Select and document the criteria that management would use to support its written management assertion.

Management assertion must be based on suitable criteria that are objective and relevant to financial reporting controls that would be applicable to user organisations. The new standards require that the criteria be fairly presented in the service organisation's description of its system. In preparing its assertion, management will need to review the description of its system to ensure that it includes sufficient information to support its belief that the assertion is based upon suitable criteria.

For example, management should take the opportunity to state control objectives more definitively. A control objective that focuses on data entry activities on behalf of the user organisations may be strengthened by including a reference to the completeness or accuracy of the data entry function.

Or the service organisation may specify the timeliness of entry as a component of the control objective to

ensure that a reader can objectively determine how this data entry function affects an assertion regarding revenue cutoff. The point is that service organisations should take this opportunity to evaluate their existing control objectives and activities and ensure that each is appropriately objective.

SSAE 16 also indicates that items related to presentation and disclosure could be relevant criteria that should be incorporated into the scope of the controls covered by the service auditor's report. Controls related to a service organisation's operations and compliance objectives may also be relevant to a user entity's internal control over financial reporting. Such controls may pertain to assertions about presentation and disclosure relating to account balances, classes of transactions or disclosures, or may pertain to evidence that the user's external auditor evaluates or uses in applying auditing procedures. For example, a payroll processing service organisation's controls related to the timely remittance of payroll deductions to government authorities may be relevant to a user entity because late remittances could incur interest and penalties that would result in a liability for the user entity.



7. Determine whether a written assertion from the subservice organisation is necessary.

If the service organisation relies on subservice organisations and the inclusive method is selected, a written assertion from the subservice provider will need to be included in the report. Subservice providers are likely to have their own approval process for signing off on an assertion for a publicly available document; this process could add to the lead time necessary to turn around a report under the new standards. Discuss timing with subservice organisations to meet your expected report issuance date.

8. Review the existing SAS 70 description of controls and make the necessary enhancements to include missing components to fully describe the system.

Management must provide a description of the service organisation's system throughout the period covered by the report. The description of the system will need to be more robust to cover the following, among other things:

- description of the services provided, including classes of transactions processed;
- description of the procedures by which services are provided, including transaction initiation, authorisation, recording, processing and reporting;
- description of the process used to prepare reports provided to customers;
- other aspects of the Committee of Sponsoring Organisations of the Treadway Commission (COSO) internal control framework relevant to user entities; and
- any changes that occur during the audit period.

Management must also review its description of controls that form the basis of an assertion to make sure those descriptions remain fair, suitable, accurate and complete. Reviewing — and rewriting — the description section to conform to the new standards' higher level of detail makes this one of the most labour-intensive steps in the transition. Organisations that already have detailed descriptions of the control systems in a format that follows the COSO framework may have minimal work to transition to the new standards. Others may have to spend time documenting in greater detail aspects of the criteria and the service organisation's system of processes and controls.

All service organisations should communicate with their service auditors to understand whether some gaps within the existing description of controls have been noted in the past and to determine the amount of work necessary to transition to the new standards in a timely manner.

9. Develop a communication plan regarding the new standards for customers and customer-facing employees such as sales and contract teams.

Until now, the assurance report for service organisations has been branded in the market as a SAS 70. There is a learning curve to overcome and rebrand the reports. Communicate internally to make sure salespeople know that an SSAE 16 report is the new SAS 70. Reach out to customers to make sure they understand both the transition to the new standards and the path management intends to take to get there. The degree of difficulty in communicating this message will differ based on the size and complexity of the service organisation and its customers.

Having a good communication plan demonstrates that the service organisation is serious about compliance and on the cutting edge of new developments. A good communication plan demonstrates that management understands and is prepared to implement the new standards. This type of communication speaks to a high level of organisational maturity — and may be a key differentiator for clients shopping for a new service provider.



10. Review existing customer contracts and contract templates to determine the revisions necessary to transition to the new standards.

In meeting its contractual obligations, management needs to consider whether existing customer contracts need to be updated to reference the new standards. Contract templates will also need to be amended.

Conclusion

How smooth the transition to new standards is, in part, dependent on what service organisations already have in place. Service organisations that have obtained SAS 70 reports in the past — and have detailed written descriptions of systems, services and controls — will transition to the new standards more easily than will organisations that have never obtained a SAS 70 report. We urge you to contact us to outline a transition strategy.

Business Risk Services

Cian Blackwell
Partner, Business Risk Services
T+353 (0)1 6805 710
E cian.blackwell@ie.gt.com

Sara McAllister
Director, Business Risk Services
T +353 (0) 6805 716
E sara.mcallister@ie.gt.com

www.grantthornton.ie

24-26 City Quay, Dublin 2

Offices also in Limerick, Kildare and Galway

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialist advice should be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing. Grant Thornton, Irish member of Grant Thornton International.
www.grantthornton.ie

Appendix: Key differences between SAS 70 and SSAE 16

SAS 70	SSAE 16
Auditors report need not be accompanied by management's written assertion.	<p>Management's written assertion is required to accompany auditor's report.</p> <p>Management's assertion must include the suitable criteria for its' assessment.</p>
Auditor's report need not be accompanied by a subservices organisation's written assertion (inclusive method used).	If a service organisation uses subservices organisation(s) and elects to use the inclusive method, the subservices organisation(s) assertion also accompanies the auditors report.
For Type II reports, the opinion on fair presentation of the system and suitability of design is as of a point in time.	For Type II reports, the opinion on fair presentation of the system and suitability of design is for the period covered by the report.



Grant Thornton

© 2011 Grant Thornton. All rights reserved.
Member of Grant Thornton International Limited