

Internal Auditing & Business Risk magazine

New gold standard to change third party assurance

From 15 June 2011 outsourcers will be required to use a new standard to provide assurance to their users that will impact on their processes and internal controls, which is likely to mean more work for internal auditors at a time when they are already stretched.

Mark Russell, a senior manager in Ernst & Young's Advisory practice, looks at the real impact ISAE 3402 will have on organisations, and what internal auditors of service providers, as well as those at organisations using service providers, need to do to prepare and respond to the change.

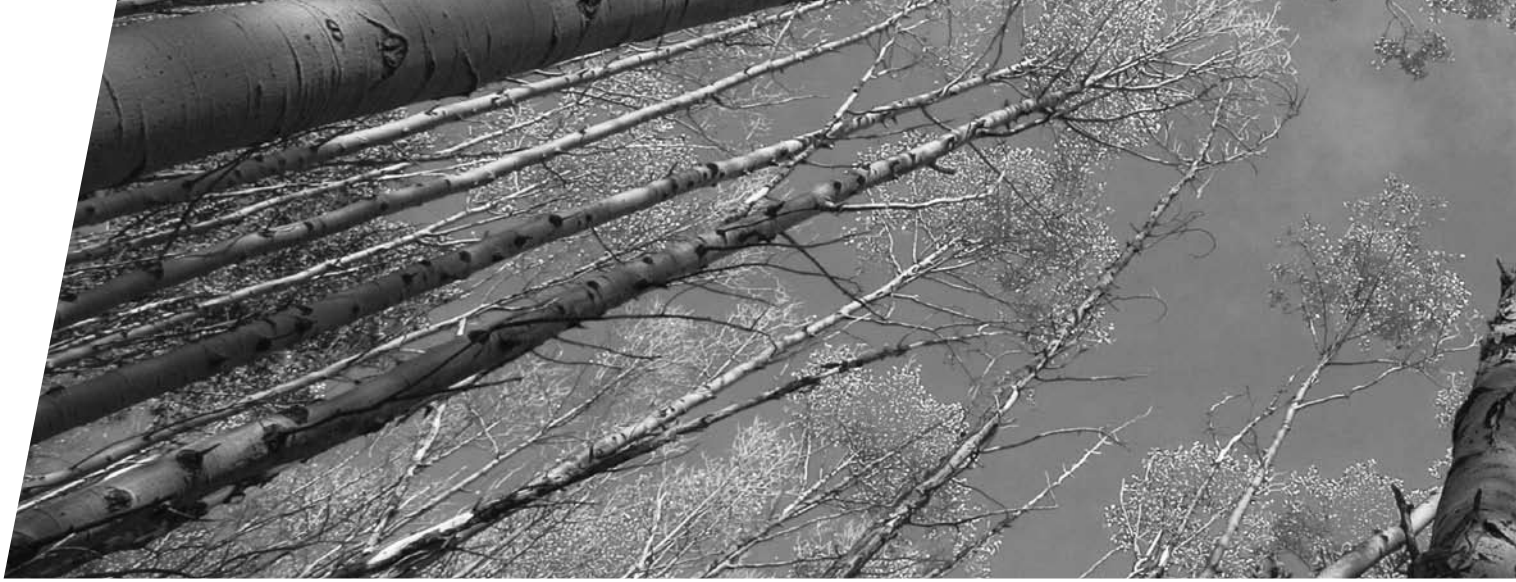
For many years outsourcers (or service organisations, per the standards) have had a mechanism for providing independent assurance to their user organisations and their user organisations' auditors. The most globally recognised or 'gold' standard has been SAS 70, issued by the American Institute of Certified Public Accountants, although there are also UK standards such as AAF 01/06 and ITF 01/07.

On 18 December 2009, the International Auditing and Assurance Standards Board issued ISAE 3402, 'Assurance Reports on Controls at a Service Organization'. This new standard can be adopted from now and replaces SAS 70 for periods ending on or after 15 June 2011. The Institute of Chartered Accountants in England and Wales is now looking at how ISAE 3402 will impact AAF 01/06 and ITF 01/07. It is therefore important that service organisations and user organisations and their auditors understand the changes that ISAE 3402 will bring and what this will mean as to how assurance is provided.

What do service organisations need to do?

The new standard presents service organisation management with two challenges:

1. Communicating with users.
2. Changes to existing SAS 70 projects, dealing with an increased workload which may mean more work for internal audit to help management meet the new requirements of ISAE 3402.



Communicating with users

Service organisations should communicate as soon as possible with user organisations to explain that ISAE 3402 will provide the same level of independent assurance, and to ask user organisations if they still require the assurance provided by the SAS 70 report. The SAS 70 report may no longer be required, or cover areas that are no longer of concern – in which case ISAE 3402 may be a chance to reduce the scope, with savings in costs.

Internal audit, as the in-house controls professionals, often support SAS 70 projects, and we would expect them to be involved in the transition to ISAE 3402. This involvement is likely to be greater in the transition year, both as they help with the specific areas outlined below and also because the transition will need project management. Because these reports are controls projects, internal audit may be asked to manage the transition.

What changes does ISAE 3402 bring?

The biggest change requires service organisation management to publicly sign-off that controls have been operating effectively for the period covered by the report.

ISAE 3402 considers that this sign-off requires additional activities by the service organisation, including:

- 1.** A fuller description of the processes and controls they operate for users.
- 2.** A risk analysis of those processes, so management can attest that the controls address these risks sufficiently.
- 3.** Management has undertaken sufficient work to assess whether controls have operated effectively.

The requirement for a fuller description of processes and controls

This may not require more work; the description in many SAS 70s already meets the ISAE 3402 requirements. However, some only include a brief description of the controls, and ISAE 3402 is clear that this will be insufficient. Under ISAE 3402 management should provide enough detail to allow a user to understand the in-scope processes and to then do their own risk assessment. Therefore, management needs to discuss with the service auditor whether or not the existing description is sufficiently detailed and if not, how it can be enhanced to provide the expected level of information.

Our experience is that writing this description is best left to controls professionals who know what a user auditor will need. Often this task is undertaken by internal auditors, as they have a good understanding of the organisation and its processes and controls. If the descriptions need to be improved, internal audit should be well placed to do this, if time can be found in the plan.



Risk analysis

Because service organisation management has to attest that the controls are designed appropriately, it needs to do a risk analysis. For most service organisations, this should be relatively straightforward, since they can use the existing SAS 70 control objectives and assess whether the current SAS 70 controls are adequately designed to support these control objectives.

A service organisation that is starting an ISAE 3402 project from scratch would not have this head start, but the mapping of controls to assess whether they support the control objectives adequately should be relatively straightforward. This should play to internal audit's core skills and understanding of the business and we would expect internal audit to be involved in this risk analysis. For example, it could document the risk analysis, mapping the controls to the risks and the control objectives so it can be shown that the controls address the risks inherent in meeting the control objectives. Specifying relevant control objectives will need more thought and is likely to involve internal audit as well as the service auditor. As with SAS 70, ISAE 3402 does not contain prescribed control objectives (unlike some other standards in this area, such as AAF 01/06).

Management's work to assess the effectiveness of the controls

ISAE 3402 says, "This assertion may be based on the service organisation's monitoring controls". On this basis, management may be able to show that controls have operated effectively by documenting how existing activities (both within the standard processes and separate evaluation processes, such as quality audits, internal audits or reviews of customer complaints), can be combined to provide assurance that controls have operated effectively over the period. This is an area that internal audit may be asked to assess or perform to provide management's assessment of operating effectiveness.

If the current sources of assurance are insufficient, for example, because existing monitoring controls do not cover all key in-scope controls, internal audit may be asked to extend their work to address this and hence support management's assertion, if this is considered a valuable use of internal audit resources.

It is worth noting that the quality of management's assessment process is not part of the scope of the service auditor's opinion.

What do user organisations need to do?

User organisations should focus on ensuring the introduction of ISAE 3402 does not reduce the level of assurance they receive from their service organisations. Often internal audit at user organisations uses a SAS 70, rather than their own work, as the source of assurance over controls at the service organisation. Internal audit should ensure that the ISAE 3402 report will continue to provide the necessary assurance, which may also be part of SOx assurance. Also, internal audit should continue to look at the controls identified in the ISAE 3402 report as needing to be operated by user organisations, and consider these are being tested appropriately.

Assuming internal audit lead assurance discussions with service organisations, it should:

1. Review contracts and, if necessary, request changes so that the service organisation is required to provide a 'SAS 70 or equivalent' report, rather than just a SAS 70 report. Contracts should include a right of audit access so internal audit can audit areas not covered by the ISAE 3402 report if necessary.
2. Ask service organisations when they will switch to ISAE 3402.
3. Challenge if the service organisation says the ISAE 3402 report will cost more - as noted above, the transition costs from SAS 70 to ISAE 3402 should be minimal for a service organisation that is already delivering a good SAS 70.
4. Use this change as an opportunity to discuss their assurance needs with the service organisation, to look at whether the current approach can be improved.

Conclusion

The transition from SAS 70 to ISAE 3402 will require both service and user organisations to understand the timetable for the change and what it means to them. For service organisations that already provide assurance via SAS 70, the changes will centre on pulling together existing information in most cases, and working with their user organisations to make sure they are comfortable with the change. These changes may well see increased work for internal audit to support the additional requirements of ISAE 3402. User organisations should make sure that the new ISAE 3402 report will continue to provide them with the assurance they need, and to drive discussions around this with their service organisations if necessary. This is also likely to require more input from internal audit, if they have led such discussions historically.

For further information please contact
Paul Durkin +44 (0)20 7951 3692, pdurkin@uk.ey.com or
Mark Russell +44 (0)1179 812 204, mrussell@uk.ey.com.

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 144,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

For more information, please visit www.ey.com/uk.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

The Ernst & Young organization is divided into five geographic areas and firms may be members of the following entities: Ernst & Young Americas LLC, Ernst & Young EMEA Limited, Ernst & Young Far East Area Limited and Ernst & Young Oceania Limited. These entities do not provide services to clients.

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

© Ernst & Young LLP 2010. Published in the UK. All Rights Reserved.



In line with Ernst & Young's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

Copyright IIA - UK and Ireland. Reproduced with the permission of the IIA - UK and Ireland.