Client Alert.

4 January 2011

Changes to SAS 70: Are you Ready?

By Sue McLean and Chris Ford

Compliance audits of outsourcing service provider arrangements have become increasingly common over the past few years, especially for service scope affecting public companies' financial reporting. In 2011, changes will take effect that may cause outsourcing customers to amend their approaches to auditing of service provision arrangements.

Over the last 20 years, organisations that outsource functions ("user organisations") have become comfortable using the AICPA Statement on Auditing Standards No. 70 ("SAS 70") as a means to audit a service provider's controls that affect the internal controls of the user organisation. One effect of the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley") was that companies which publicly traded their securities in the U.S. markets were required to comply with significantly more stringent audit requirements. As a result, reliance by user organisations on SAS 70 reports provided by service providers was of even greater importance and, over the past 8 years, user organisations and service providers worked out reasonable methods of allocating risks associated with internal controls.

However, just as the outsourcing industry has become familiar with SAS 70, the audit regime is changing.

In an effort to clarify standards and converge with international standards, the SAS 70 requirements for conducting an audit on a service organisation are being replaced with two new standards that will become effective in 2011 and 2012, respectively. While at first blush the changes may not seem significant, the practical impact which they may have on service providers may shift the aforementioned allocation of risk associated with the appropriateness of service providers' controls as they affect the internal controls of the user organisation.

In our Client Alert published on 23 January 2008, we explained the impact of SAS 70 on outsourcing projects. In this Alert, we will outline the key changes introduced by the new regime and what service providers and user organisations need to know.

NEW REGIME

As we set out in our previous Client Alert, SAS 70 contains guidance for "user auditors" (i.e., auditors who audit the financial statements of user organisations) and auditors reporting on a service provider's controls ("service auditors"). Under the new regime, the requirements for user and service auditors are being split.

Statement on Standards for Attestation Engagements ("SSAE") 16 "Guidance for Service Auditors Reporting on the Service Organization Controls" will act as guidance for service auditors. SSAE 16 has been designed to mirror and comply with the new international reporting standard (International Standard on Assurance Engagements ("ISAE") 3402 "Assurance Reports on Controls at a Service Organisation"). SSAE 16 will become effective for reporting periods ending on or after 15 June 2011.

In addition, a new SAS, "Audit Considerations Relating to an Entity Using a Service Organization", has been introduced for user auditors. The new SAS will become effective for reporting periods ending on or after 15 September 2012. (During the period between 15 June 2011 and 15 September 2012, auditors will continue to follow the guidance set out in the existing SAS 70 rules.)

SIGNIFICANT CHANGES

As SSAE 16 is largely based on SAS 70, the audit process and reports will be very familiar to those who have previously conducted a SAS 70 audit.

However, there is a material change in that, under the new regime, the management of a service organisation will now be required to provide a written assertion attesting to the fair presentation and design of controls (in a Type 1 report), and with respect to a Type 2 report, the operating effectiveness of controls. Previously, auditors reported directly on controls and a service provider's management was not required to provide a written assertion of this nature.

As a service provider's management will need to have a reasonable basis for making the assertion, they may need to develop their own processes to support the assertion if such processes are not already in place. SSAE 16 provides specific requirements that must be met by management in order to provide an assertion such as: (i) identifying criteria that will be used to prepare the description of its system and to evaluate whether controls are suitably designed (Type 1 report), and with respect to a Type 2 report, are operating effectively, and (ii) identifying any risks that threaten the achievement of the control objectives.

If the service provider relies on controls at a "subservice" organisation (whether a subcontractor or affiliate), it may decide to include or exclude within the scope of the SAS 70 report the controls used by such subservice organisation. If it elects the inclusive method (i.e., its system controls will include controls at the subservice organisation), the service provider will also need to determine whether the subservice organisation's controls are suitably designed (Type 1 report) or (Type 2 report) operating effectively. In order to do this, it will need to obtain a written assertion from the management of the subservice organisation.

PRACTICAL EFFECTS

These two developments may have practical impacts on the ways in which service providers and user organisations allocate risk and responsibilities associated with the control environment. In a typical arrangement, service providers will agree to provide generic SAS 70 reports to user organisations that cover the control environment to all of the service provider's customers within that control environment, and not specifically tailored to any specific user organisation. While user organisations have attempted to obtain specific certifications from service providers regarding their controls, service providers have often been unwilling to do so. Now, under SSAE 16, management of service providers will be required to give an assertion as part of the audit process.

As was the case with Sarbanes-Oxley, where management is required to give an attestation of its internal controls over financial reporting, which potentially increased the risk profile to the company and to the individual members of management, management of service providers may be wary of the increased risks that they could incur from making the assertion required by SSAE 16. Service providers may attempt to mitigate additional risk by changing the historical contractual risk allocation found in today's outsourcing agreements.

User organisations, of course, will attempt to use a breach of that assertion as a means to recover damages against service providers. Thus, while service providers will attempt to reduce (or at least neutralize) their exposure to internal control-related risks, user organisations will likely attempt to increase that exposure, armed with a new piece of evidence, i.e., management's assertion under SSAE 16. This may result in hard-fought negotiations that will be required to create a new paradigm.

Another issue that may change the risk allocation picture is how the assertion requirement will impact service providers' willingness to make statement about their subcontractors. As stated above, SSAE 16 allows service providers to exclude subservice organisations from their controls but, if subservice organisations are included, management of those organisations must make an assertion of their own. To include the subservice organisation in the service provider's controls may increase the cost of subcontracting due to the increased risk to which the subcontractors would be exposed.

Generally, user organisations attempt to require service providers to make contractual representations about the effectiveness of their subcontractors' internal controls. SSAE 16 may have a chilling effect on service providers' willingness to make such representations; they may opt to take the subcontractors out of the equation altogether or, at a minimum, attempt to pass along to the user organisations the increased cost of subcontracting resulting from the increased risk to the subcontractor. Unfortunately, the impact of the new rule could therefore have a negative impact on a fundamental tenet in outsourcing deals – that the service provider is always responsible for the acts or omissions of its subcontractors.

OTHER KEY CHANGES

- More detail is required in terms of the documenting of processes and controls.
- In a Type 2 report, the description of the service provider's system and opinion on the system will cover the applicable reporting period (rather than for a specified date, as was the case before).
- In a Type 2 report, if internal audit work has been used, the service auditor will need to detail such work in its description of tests and in its procedures with respect to such work.
- The auditor will be required to investigate the nature and cause of any deviations. If they result from deliberate acts by personnel, the auditor must assess the risk that the organisation is not fairly presented and that the controls are not suitably designed or operating effectively.
- When assessing controls, auditors cannot rely on evidence contained in previous engagements. Assessments must be based wholly on evidence obtained during the relevant reporting period.

IMPLICATIONS FOR SERVICE PROVIDERS

Service providers should consider:

- whether they should select SSAE 16 or ISAE 3402 to meet the needs of their customers. If a service provider is located in the U.S., it will need to follow SSAE 16. However, where the service provider has operations and/or customers outside the U.S., it may not be so clear-cut. In fact, where a service provider has a wide customer base, there may be benefits in carrying out an examination under both sets of standards;

- how the new rules will affect their organisations and auditing practices. Do existing processes and controls have the necessary level of detail required by the new rules? What additional processes or process changes will need to be implemented so that assertions can be supported?;
- who in management will provide the assertion (e.g., CIO, COO, CFO, etc.), and who else needs to be involved in order to support that assertion?;
- how to engage with subservice organisations and whether to select the carve-out method or inclusive method of reporting; and
- which of their contracts with user organisations require an SAS 70 report and whether any amendments need to be made to those contracts to take account of the rule changes.

Service providers should also consider the potential benefits of early adoption of new standards. It would help to give them time to assess whether the correct processes are in place to ensure compliance with the new standards. They could also use early adoption to give them a competitive advantage and help demonstrate to customers that they have a stronger control environment than their rivals. However, they will have to gauge, of course, whether their customers will accept early adoption.

IMPLICATIONS FOR USER ORGANISATIONS

User organisations that receive or require SAS 70 reports from service providers should:

- review the changes to the rules and discuss with the relevant service providers the potential impact of the changes;
- consider whether they require a service provider to issue a report under SSAE 16 and/or ISAE 3402;
- consider whether any amendments need to be made to their contracts with a service provider;
- where a service provider uses subcontractors to provide the services, check with the service provider whether it intends to take an inclusive or carve-out approach to subservice controls and what impact this may have on the user organisation's reliance on controls.

CONCLUSION

Although the new auditing standards do not involve a great volume of changes, a few of them may present some challenges and could result in changes to well-understood risk allocation methodologies. Service providers will need to make strategic decisions as to what additional processes or process changes need to be implemented in order to comply with the new standards, and user organisations will need to consider how the new standards impact what reporting provisions they require from service providers. Service providers and user organisations should start planning now in advance of the rule changes to help ensure a smooth transition to the new regime.

Contact:

Sue McLean
+44 20 7920 4045
smclean@mofo.com

Chris Ford
(202) 887-1512
cford@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.