MORRISON | FOERSTER

Legal Updates & News

Legal Updates

A Guide to the Impact of SAS 70 on Outsourcing Projects

January 2008
by Alistair Maughan, Susan McLean

Related Practices:
- Sourcing

The worlds of outsourcing and U.S. financial regulation are beginning to coincide. In particular, a number of large (and not-so-large) companies are increasingly insisting on comprehensive regulatory-driven audit requirements as part of their outsourcing arrangements. This can be a contentious area, with the parties arguing over the scope of the audit and who will pick up the costs, which can be substantial.

The issue is not just confined to U.S. companies or even to the outsourcing of financial services. The relevant laws and standards – the Sarbanes-Oxley Act of 2002 (SOX) and the Statement on Auditing Standards No. 70: Service Organisations (SAS 70) – potentially affect not just U.S. companies and foreign subsidiaries of U.S. companies, but also any company based outside the U.S. that is subject to U.S. Securities and Exchange Commission (SEC) regulation or that uses U.S. accounting rules.

In order to negotiate these issues effectively, it is vital to understand why a so-called SAS 70 audit is required and what it entails. In this article, we give the background to SAS 70 and its application to outsourcing agreements and aim to answer some of the queries typically raised in respect of SAS 70. We also detail some of the issues that companies need to consider when outsourcing processes that are subject to SAS 70, and likewise some of the issues that service providers need to know when a customer insists on having SAS 70 audit rights.

What are SOX and SAS 70?

In its short life, SOX has become almost a household name. It is a U.S. federal law that was passed in July 2002 in response to high-profile business accounting scandals, such as Enron and WorldCom, in order to reinforce investment confidence and protect investors by improving the accuracy and reliability of corporate disclosure. Amongst other things, SOX establishes standards with which public companies and public accounting firms must comply, and addresses key issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure.

Less well-known than SOX, SAS 70 is shorthand for the Statement on Auditing Standards No. 70: Service Organisations, which is an auditing standard issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 defines the professional standards that govern the way in which an external auditor should assess and report on the internal controls of an external service provider, and is required for all audits conducted under Generally Accepted Auditing Standards in the U.S. (GAAS). SAS 70 is not new; it was adopted as a standard in 1992. However, increased outsourcing and the visibility of control requirements introduced in Section 404 of SOX have increased the attention required to be given to SAS 70 audits.

What is the Link between SAS 70 and SOX?

Section 404 of SOX and the relevant rules [2] promulgated by the SEC require each SEC-listed

company to produce a report on the company's internal controls as part of the annual report which the company files with the SEC. [3]

This report must contain, amongst other things, an assessment of the effectiveness of the company's internal control structure and procedures for financial reporting. This means that the company has to (i) evaluate the effectiveness of the company's internal control over financial reporting; and (ii) have the public accounting firm that conducted the audit attest to and report on the assessment made by the company's management. The way in which a company's internal control over financial reporting is assessed is governed by Auditing Standard No. 2 (AS2), set by the U.S. Public Company Accounting Oversight Board (PCAOB). [4]

If a company does not use any external service providers to carry out its business, there is no additional SAS 70 requirement over and above this SOX Section 404 obligation. But, of course, companies that do not use any outsourcing or other external services providers to perform business functions are very rare. So any company with outsourcing arrangements which affect the company's internal control over financial reporting must also test the effectiveness of the internal controls of its outsourcing services provider as part of its SOX Section 404 assessment – and the procedures set out in SAS 70 [5] are the means by which such assessment must be carried out.

In practice, this means that the company should obtain an SAS 70 Report on the external services provider from an independent auditor.

Does SAS 70 Apply to All Outsourcing Arrangements?

In deciding whether SAS 70 applies to a particular outsourcing arrangement, a company has to consider two things: the requirements of the SEC rules and the requirements of SAS 70 itself. The basic test is whether outsourcing affects the company's internal control over financial reporting.

According to the SEC rules, [6] an internal control over financial reporting means a process which is designed by, or under the supervision of, the company's management to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. Therefore, where any services received from an outsourcing service provider impact on a process that could affect the way in which the financial affairs of a company are recorded and reported, it is likely that the company will be required to test the effectiveness of the outsourcing service provider's internal controls. Such services include those that form part of the company's information system. [7] According to SAS 70, a service organisation's services are part of an entity's information system if they affect any of the following:

- The classes of transactions in the entity's operations that are significant to the entity's financial statements;
- The procedures, both automated and manual, by which the entity's transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements;
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the entity's financial statements involved in initiating, recording, processing and reporting the entity's transactions;
- How the entity's information system captures other events and conditions that are significant to the financial statements; and
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.

Typical service providers affected by SAS 70 include application service providers, managed security providers, trust departments, claims processors, clearing houses, credit processing companies, application service providers, and data hosting providers. Note, however, that there is specific guidance that SAS 70 is not intended to apply to: [8]

- "Situations in which the services provided are limited to executing client organisation transactions that are specifically authorised by the client, such as the processing of checking account transactions by a bank or the execution of securities transactions by a broker," and
- "The audit of transactions arising from financial interests in partnerships, corporations and joint ventures."

As there is no definitive test, each outsourced service will need to be judged on its own particular facts and circumstances.

Does SAS 70 Apply to Business Process Outsourcing?

The nature of the business process that is to be outsourced will determine whether or not SAS 70 applies. As mentioned above, the question to ask is, whether or not the business process affects the company's internal control over financial reporting. Since a wide variety of business processes will affect the processing of financial and related information of a company, it is likely that SAS 70 will apply to a wide variety of business process outsourcing (BPO) arrangements, including the outsourcing of finance and accounting related functions (e.g., payroll and credit processing). Accordingly, SAS 70 is as, if not more, likely to affect BPO arrangements than IT outsourcing arrangements.

Are There Any De Minimis Levels?

The position that many large companies now take is that all material outsourcings are covered by SAS 70, and so there is a requirement for an SAS 70 audit in respect of all key relevant outsourcings.

There are no *de minimis*levels in determining whether an SAS 70 audit ought to be carried out; a company cannot rely on any quantitative threshold to circumvent the need to obtain an SAS 70 report from its outsourcing service providers. The only relevant question is whether or not the outsourced function affects the company's internal control over financial reporting.

If the function has no material impact on a company's financial reporting and cannot result in a material error in the financials of the customer, then it is unlikely that an SAS 70 audit will be required. It is also possible to argue (although not often with much success) that no SAS 70 audit will be required where an error at the outsourced level would be picked up by the company's own internal control system. However, it is worth noting that, in our experience, companies' accounting and audit firms advocate conducting an SAS 70 audit in any event.

Does SAS 70 Apply to Sub-Contractors?

In outsourcing transactions, it is common for a service provider to sub-contract certain elements of the services. In such circumstances, does the sub-contractor also need to be subject to an SAS 70 audit? In general, the answer is yes – as long as the part sub-contracted passes the key test of affecting the company's internal control over financial reporting. A company that uses an outsourcing service provider must be assured that it has adequate control over any outsourced functions relevant to financial reporting. So, if A outsources a function to B, and B in turn sub-contracts to C, either:

- B must take responsibility for C; or
- A must consider whether it needs a separate review of C, based on whether or not the functions that have been sub-contracted to C will have a material impact on A's financial reporting.

In fact, in the above example, B has a choice of having two types of SAS 70 audits done, resulting in two types of SAS 70 reports. One would be termed a carve out report, and the other would be termed an inclusive report. In the case of a carve out report, only B's controls would be reviewed and the auditors' report would say that it had not looked at the controls in place at C. On the other hand, in the case of an inclusive report, the auditors would also review the controls at C, and therefore the resulting SAS 70 report would address the controls in place at both B and C.

Does SAS 70 Affect Non–U.S. Companies or Non–U.S. Outsourcing Deals?

SAS 70 can affect non-U.S. companies and it applies even where none of the outsourced services are being carried out in the U.S. The test is not whether a company is SEC-regulated or U.S.-listed. Any company that is audited in accordance with U.S. GAAS, regardless of whether or not it is a public company or a private company and regardless of whether or not it is a U.S. company or a non-U.S. company, will be subject to the SAS 70 requirements in respect of any applicable outsourced functions.

What Does an SAS 70 Audit Involve?

SAS 70 requires a company's outsourcing services providers to be subject to an annual audit, performed either by the service provider's own independent auditor or by the auditors of the company itself. Auditors who conduct SAS 70 audits are required to follow the AICPA's standards for field work, quality control, and reporting. However, an SAS 70 audit is not a checklist audit; there is no predetermined set of control objectives or control activities that a service provider has to achieve.

There are two types of SAS 70 audits: (i) a Type I audit and (ii) a Type II audit. [9]

In a Type I SAS 70 audit, the auditor examines and comments on whether the service provider's description of controls is presented fairly; controls are designed effectively, and controls are placed in operation as of a specified date.

In a Type II SAS 70 audit, in addition to what is done in a Type I audit, the auditor also examines and comments on whether or not the service provider's controls are operating effectively over a specified period of time. Type II audits are proportionately more time-consuming and expensive; therefore in a Type II audit, the auditor should, amongst other things:

- Gather information through discussions with appropriate service organisation personnel and through reference to various forms of documentation, such as system flowcharts and narratives to ascertain the controls that a service provider has in place;
- Determine whether the description of controls that the service provider has in place is sufficient to ascertain how the service provider's control may affect the service user's own internal control, for example through the review of:
    - Hiring practice and key areas of authority and responsibility;
    - Risks associated with processing specific transactions;
    - Policies and procedures over the modification of computer programs;
    - Information and communication about ways in which user transactions are initiated and processed; and
    - The involvement of internal auditors;
- Obtain evidence of whether controls have actually been placed in operation, for example, through procedures such as inquiry of appropriate management, supervisory, and staff personnel; inspection of service organisation documents and records; and observation of service organisation activities and operations; and
- Conduct tests of controls to determine whether specific controls are operating with sufficient effectiveness to achieve specific control objectives in accordance with the applicable AICPA Professional Standards.

For the purposes of compliance with SOX, it is generally considered that only a Type II SAS 70 audit will be acceptable. This is because the PCAOB states that as evidence of internal control over financial reporting operating effectively, a company to which SAS 70 applies should obtain a *report with the service auditor's opinion on the service organisation's description of the design of its controls, the tests of controls, and the results of those tests performed by the service auditor, and the service auditor's opinion on whether the controls tested were operating effectively during the specified period.* [10]

How Much Does an SAS 70 Audit Cost?

The costs of an SAS 70 audit will vary depending of the type of audit (*i.e.*, Type I or Type II), the size of the company being audited, the state of the control environment, and whether or not the audit should be an *inclusive*one that probes the sub-contractors of the service provider. However, since an SAS 70 audit is a comprehensive examination of controls (with the auditor spending time reviewing documentation, interviewing personnel and observing and testing controls), the costs can be substantial.

Because of the expense and time involved in a Type II audit, in addition to the issue of whether an SAS 70 audit is required in the first place outsourcing parties often end up negotiating over what type of audit is required, and, obviously, who will pick up the cost of it. In a major outsourcing situation, a company may take the position that a potential service provider having or funding its own current Type II audit is simply another cost of doing business – and one that can be spread amongst all of its outsourcing clients.

What are the Implications of an SAS 70 Report?

If a company is able to obtain a satisfactory SAS 70 Report, there will generally be no problem regarding the evaluation of the company's outsourced activities. However, if a company is unable to obtain a satisfactory SAS 70 Report (or any SAS 70 Report at all), it may be necessary for the company to disclose this fact in its annual report as a material weakness in its internal control arising from its inability to obtain evidence of effective internal control of its external outsourcing services provider. The company's management will be required to determine whether the inability to assess the internal controls over a particular outsourced activity is significant enough to cause management to conclude in its report that the company's own internal control over financial reporting is ineffective. [11] In addition to the management's determination, the company's auditor must also determine whether management's inability to assess certain controls warrants a determination that management has not fulfilled its responsibility to evaluate the effectiveness of the company's internal control over financial reporting and support its evaluation with sufficient evidence.

Is an SAS 70 Audit Sufficient?

Any company that is outsourcing services which will be subject to SOX should be aware that there is a growing consensus that even a Type II SAS 70 audit may not be sufficient to demonstrate SOX compliance. As the SAS 70 standard was developed long before SOX, it was not designed to address the controls that SOX addresses. Accordingly, when outsourcing a service, companies should consider if there are any additional controls and tests that they need to impose upon the service provider.

Issues to Consider in the Context of Outsourcing Arrangements

For Companies Considering Outsourcing:
Where you are outsourcing processes which you believe will be subject to SAS 70, you should consider the following issues:

- General obligation. You should consider including a general obligation on the service provider to institute all appropriate controls in performing the services (in its systems and all other processes and tools used to perform the services) to the extent reasonably necessary to satisfy your (and any other service recipients') obligations under SOX.
- Recipient of audit rights. You will need to consider who needs SAS 70 audit rights – is it just the direct customer or, where there are other service recipients (whether group companies or external customers); do you also need to secure SAS 70 audit rights for these other recipients of the services?
- Frequency of audit. Your right to an annual SAS 70 audit should be documented.
- Appointment of auditors. You will need to consider who is going to appoint the auditors. Do you expect this to be done by the service provider, or do you want to appoint the auditors (for example, because you have already appointed auditors to carry out an SAS 70 audit on other, connected, parts of your business)?
- Audit Type. You will need to decide whether you need a Type I or Type II audit, or specify in the contract that either may be required.
- Scoping, timing and form of report. Ideally, you should agree up-front on the exact scoping, timing and form of each report. If this is not possible, you should include in the contract a process for agreeing on this at the appropriate time.
- Sub-Contractors. Where the service provider is sub-contracting any elements of the services, you should ensure that the SAS 70 audit covers the sub-contracted services (i.e., you should insist on an inclusive, rather than a carve-out SAS 70 report).
- Costs.
    - Who will pay for the independent auditor to carry out the SAS 70 audit? If the service provider does not undergo SAS 70 audits currently (either for its own internal purposes, or to meet other customer requirements), it is likely that this will be a cost that you will be expected to bear. However, where this is a shared requirement across many customers, you should argue that the costs be shared on a pro-rata basis.
    - Who will bear the internal costs of the service provider in connection with the audit? You should consider whether it is reasonable for you to cover any reasonable, demonstrable, incremental costs incurred by the service provider in cooperating with, and supporting, the SAS 70 audit. The service provider should, of course, obtain approval in advance to any such costs.
- What happens following the completion of the audit? Depending on who engages the auditors (whether you or the service provider), a copy of the audit report should be provided

to the other party. The contract should then detail the remediation process in respect of any deficiencies identified in a report.

- Use of audit report. You should make clear that although the report must be considered the confidential information of both parties, you may provide copies, where necessary, to your group companies and any external auditors or professional advisers, and that you may use the report as a contribution to your attestations under SOX.

Footnotes:

[1] With thanks to Eric Roberts, Director of Forensic Accounting, Morrison & Foerster LLP.

[2] See Exchange Act Rules 13a-15 and 15d-15.

[3] Note that registered investment companies, issuers of assetbacked securities, and non-public companies are not subject to the reporting requirements mandated by Section 404 of SOX.

[4] The Public Company Accounting Oversight Board is a private sector, non-profit corporation created by SOX to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair and independent audit reports.

[5] See paragraph B21 of AS2.

[6] See Exchange Act Rules 13a-15 and 15d-15./p>

[7] See AU Section 324.03 of the AICPA Professional Standards.

[8] See AU Section 324.03 of the AICPA Professional Standards.

[9] See AU Section 324.24 of the AICPA Professional Standards.

[10] See paragraph B21c of AS2.

[11] See Answer 28 of PCAOB Staff Questions and Answers, dated 23 June 2004 (revised 27 June 2004).