

SAS70: A practitioner's view

Sarbox – brief summary

Few topics have provoked as much debate amongst those responsible for corporate governance in the US and globally as the enactment of the Sarbanes Oxley Act in July 2002. Why globally, you might ask? Well, in short, if you are a publicly registered company under the jurisdiction of the Securities and Exchange Commission or if you are a service provider of any significance to such a company, under Section 404 of the act you must provide an annual assertion that internal controls over financial reporting are effective. Additionally, an independent auditor of the organisation is currently required to provide an opinion on management's assertion over internal control in addition to the auditor's opinion on the presentation of the financial statements.

Important Sarbox changes

Those who have gone through the external audit process on their internal controls will know that getting this letter of opinion can be a long and costly process. But this may be about to change.

As a consequence of calls made in the US Senate for a relaxation of the provisions of the Act on the grounds that it places an onerous burden on business, the Securities and Exchange Commission made an important announcement on December 13th 2006. In their statement the SEC announced that in future companies subject to the 2002 corporate reform law would be allowed to design their internal controls to address the areas in which they face the biggest risks. Companies will essentially be able to "tailor" their controls to their own needs, which should significantly reduce the time and money smaller firms spend on compliance. Most significantly the SEC announced that it will recommend dropping the requirement that external auditors must attest to management's evaluation of a company's internal controls.

For smaller businesses this will undoubtedly reduce the cost and effort involved in asserting Sarbox compliancy. For larger companies acting as service providers to SEC regulated companies of any substance it is difficult to imagine them getting away without having the internal controls independently audited. This would be particularly true of service providers operating in sensitive areas such as transaction processing and host data management.

One thing is sure – external audit or no external audit; the need for effective internal controls and corporate governance is still there to ensure the financial scandals which gave rise to Sarbox are not to be repeated.

SOX and SAS70

There is frequent confusion about the relationship between the provisions of the Sarbanes Oxley Act (and more specifically section 404 of it) and the SAS70 auditing standard. Under the Sarbanes Oxley Act there was a provision for the setting up of a Public Company Accounting Oversight Board (PCAOB). This board was given responsibility for providing guidance which auditors must follow when examining management's assertion on the effectiveness of controls over financial reporting. On March 9 2004 the board issued the official auditing standard (Auditing Standard No.2). Appendix b of the file rule contains information regarding service organisations and confirms that a SAS70 service auditor's report is an acceptable format to allow management to assess the operating effectiveness of controls at the service organisation.

Since then, the SAS70 report has become the principle standard means of assessing a company compliancy with the provisions of Section 404 of the Sarbanes Oxley Act 2002.

What does a SAS70 report contain

SAS 70 reports (Service Auditor's Reports) are generally divided into three or four sections depending on the type of engagement performed. There are two types of Service Auditor's Reports: Type I and Type II.

A Type I report describes the service organization's description of controls at a specific point in time (e.g. June 30, 2006). The audit opinion expressed in the case of a Type I is confined to whether the controls as described were functioning at that point of time. It does not express an opinion as to the appropriateness of the controls. A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period (e.g. January 1, 2006 to June 30, 2006) The contents of each type of report is described in the following table:

Section Contents	Type I Report	Type II Report
1. Independent Service Auditor's Report (i.e. audit opinion)	Included	Included
2. Service organization's description of controls	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4. Other company information	Optional	Optional

How to prepare for a SAS70

The following is a list of the key actions required in preparation for a SAS70 audit:

1. **Inventorise and understand all the various business and IT operational processes** within your organisation and understand the risk profile of each of them should one or more of the processes fail in whole or in part.
2. **Define clear and concise Control Objectives** for each discrete area of your IT and business functions. Achievement of these control objectives will be the key metric by which success or failure can be objectively measured.
3. **Define one or more controls in support of each control objective.** The control should be designed to guarantee (in so far as reasonably possible) the achievement of the control objective. This is a critically important part of ensuring an effective control environment and an unqualified letter of opinion following the completion of the SAS70 audit.
4. **Assign ownership and accountability for each control objective** to an individual and make it part of his/her personal objectives.
5. **Policing** – if the controls as documented are comprehensive and congruent with the business and IT environment enforcement should come naturally as managers and team leaders go about their daily work.
6. **Review** – control objectives and controls need to be reviewed to take account of changes within the organisation, the market in which it operates and most importantly the regulatory environment

Conclusion

If there is a view within an organisation that the SAS70 control environment is burdensome and overly bureaucratic then one or more of the following problems prevail:

1. **It is possible that the control mechanisms as designed are inefficient and or inappropriate. If this is the case review them and change them so that they become a useful part of your business processes**
2. **It may be that a lot of manual compensating controls are in place to ensure achievement of the control objective. These may exist because of deficiencies in systems. If this is the case address the root cause of these deficiencies which are giving rise to compensating controls.**

3. **Frequently line managers complain that the level of review and oversight required to provide signoff in a control area takes up an inordinate amount of their time.**
Well, the answer to this is that as managers this is part of their job and they need to ensure that information provided to them to support signoff is concise and appropriate. This may necessitate change to IT systems to improve the quality of supporting data available to them. If staff consistently complain that the application of the control places an “overhead” on them the control needs to be reviewed to harmonise it with the execution of the function.
4. **If there is a widespread attitude that maintenance of a SAS70 control environment is just a box ticking exercise to keep on the right side of the law then the whole benefit of embracing a standard has been completely missed. In such an organisation, it is quite likely that there is a general lack of regard for process and control from executive management down. Unless that mind set can be changed such an organisation if it manages to achieve an unqualified opinion once, is unlikely to be capable of repeating it.**

How can O-C Group help ?

Through applying our years of experience in implementing and maintaining SAS70 in Service Organisations processing 100 of millions of transactions for SEC Controlled companies O-C Group can help your organisation implement and maintain a robust control environment which supports efficiency and unlocks the opportunity to provide services to large US corporates.