

SAS 70

**More than just an Auditing Standard
for Outsourcing Arrangements**

Contents

- 1 Foreword
- 2 Introduction to SAS 70
- 3 Benefits of SAS 70
- 4 SAS 70 versus other
Certifications
- 5 Leveraging on SAS 70



Foreword

Traditionally, outsourcing was a tactical decision driven primarily by the need to cut costs or remove relatively unprofitable, cost-ineffective processes. However, it has now become boardroom agenda for most organizations as a business strategy to access best-in-class processes, cost predictability as well as business value creation, in the long term.

Outsourcing has transformed into a mature industry by overcoming typical barriers of language, culture and time zones. With many organizations realizing its value, the outsourcing industry has seen a significant increase in the number of service providers or service organizations. As a result, companies now have the luxury of choice in selecting their service providers. A checklist based approach that is generally used in vendor selection specifically inquires, amongst other aspects, about the number of relevant certifications and quality control processes in place. Consequently, service organizations undergo numerous certifications and quality initiatives to demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

Apart from certifications such as CMM and ISO, customers are increasingly demanding the SAS 70 ('Statement on Auditing Standards No. 70' or 'the Standard') attestation from service organizations for assurance on their internal controls. This is largely due to the current regulatory environment which presents new challenges for outsourcing arrangements, specifically with regard to the Sarbanes-Oxley Act of 2002 ('SOX'). If third-party services impact financial reporting or the internal control environment, either directly or indirectly, the company's management is now responsible for evaluating the design and effectiveness of the control structure in place, both within the service provider and between the two organizations.

The Standard aims at assisting auditors of companies in developing an audit strategy for outsourced processes that have a direct or indirect bearing on financial reporting. Post the advent of SOX, the demand for SAS 70 has multiplied several folds. It is now also being used as a control assessment tool, for outsourced processes, from a SOX compliance perspective.

'Following the Sarbanes-Oxley Act of 2002, the Auditing Standard No. 70 governing internal controls for service organizations is getting serious attention – more than a decade after it was issued'

Further, one also comes across instances where service providers are undergoing SAS 70 audits on their own will to demonstrate robust internal controls over their service delivery.

Accordingly, it would not be incorrect to say that SAS 70 has also become as much a quality tool as a financial audit tool. Such is the demand for SAS 70 reports, that inability to meet the demands for a SAS 70 attestation, may lead to competitors gaining an edge over the service provider. Of late SAS 70 reports are also being used by prospective customers to gain an understanding and comfort on the internal controls framework prior to making 'that important decision'.

This paper touches upon some of the key aspects related to the SAS 70 framework and also attempts to highlight some of the ways to get more value out of the SAS 70 attestation exercise. Hope you find it useful.

Gaurav Sahu
Business Risk Services, Grant Thornton
Gaurav.Sahu@wcgt.in

Introduction to SAS 70

The Statement on **Auditing Standards No. 70, *Service Organizations***, is a widely recognized Auditing Standard issued by the American Institute of Certified Public Accountants (AICPA) in April 1992.

A service auditor's examination performed in accordance with SAS 70 is widely recognized, since it represents that a service organization has been through an in-depth audit of their control activities, which includes general computer controls and outsourced processes. The SAS report also provides useful information on the entity level controls of the service organization.

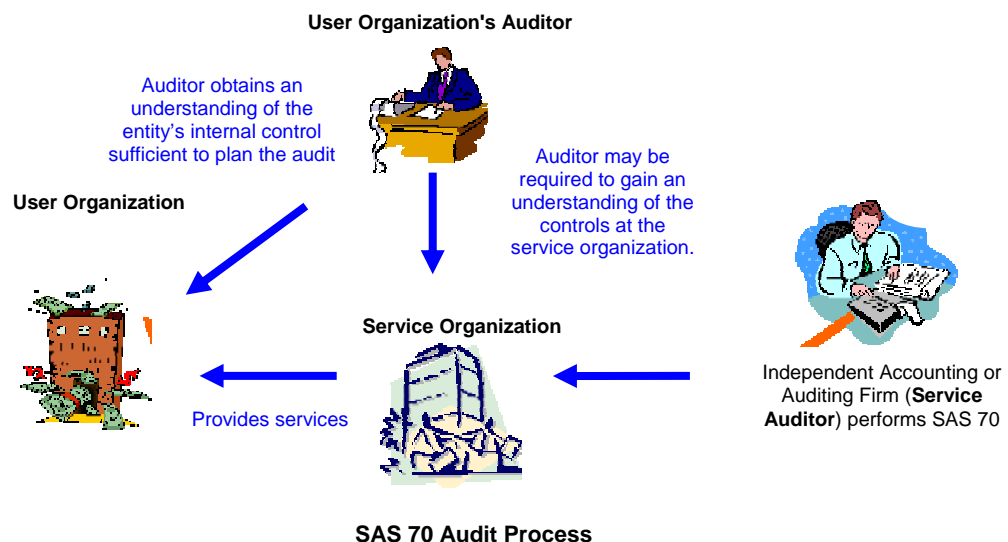
SAS 70's ability to assess effectiveness of internal control over financial reporting has facilitated its integration into the requirements of SOX.

There are two types of SAS 70 reports - *Type I and Type II*. As part of a SAS 70 Type I attestation, the service auditor reports whether the controls have been designed effectively and placed in operation as on a particular date. The

Type II reports go one step further where the service auditor also tests the operating effectiveness of the controls over the reporting period. It generally covers a minimum period of 6 months. Considering that a Type I report only covers the controls placed in operation by the service organization on a particular date, it may not provide adequate comfort on whether the controls were operating as designed over a specified period.

A SAS 70 report is primarily an *auditor-to-auditor communication* and is designed to provide information to the auditors of user organizations on the robustness of the service organization's internal controls.

A SAS 70 report highlights the controls covered, test procedures performed and the exceptions noted. Business organizations can benefit from this report as it is a useful tool for company management to assess how effectively outsourced processes are being managed by the service organization.



Benefits of SAS 70

Typically, a SAS No. 70 report contains:

- an auditor's opinion, on the design, implementation and effectiveness of controls at a service organization for a specific audit period
- a description of the service organization's control environment, its control objectives and controls that are in place to achieve those control objectives
- details of the tests performed by the auditor to assess operating effectiveness and the results of these tests
- information intended for use by the user organizations and user organizations' independent accountants

Benefits of a SAS 70 to user organizations:

- User organizations that obtain a service auditor's report from their service organization receive valuable information regarding the service organization's control environment
- The user organization receives an independent assessment of whether controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report)

Benefits of SAS 70 to service organizations:

- An unqualified opinion that is issued by an independent accounting firm differentiates the service organization from its peers by demonstrating the functioning of an effectively designed control environment
- A service auditor's report helps the service organization build trust with its user organizations (i.e. customers)
- A current service auditor's report minimizes the requirement for incremental audit requests from its customers and their respective auditors
- SAS 70 engagements are performed by control-oriented professionals who have experience in accounting, auditing, and information security, therefore allowing the service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party.
- Very often this process results in the identification of opportunities for improvements in many operational areas.



SAS 70 versus other Certifications

Fundamentally, SAS 70 is an examination/audit based on agreed control objectives and controls that are relevant to the functional environment of the outsourced process/project. While CMM, ISO 27001, COPC, GLBA, HIPAA etc. are standards, the compliance to which can be demonstrated through certification, SAS 70 involves formulation of control objectives and controls based on the risks related to the outsourcing

arrangement, that can impact the financial statements of user organizations.

Hence, the control framework for a SAS 70 is definable per engagement and the examination scope is decided by the service organization in consultation with the user organization/ user auditor.

A comparison between SAS 70 and other certifications

	CMMI	ISO 9001	ISO 27001	SAS 70
Focus	Project management	Consistency and quality	Information security	Internal controls related to the service or application provided by a company to its clients. Also includes general computer and infrastructural controls
Intended Audience	Company management and clients	Company management and clients	Company management and clients	Clients' management, clients and clients' external auditors
Testing Procedures	Minimal testing	Minimal testing	Minimal testing	Detailed and stringent sampling and testing procedures
Intended Purpose	To provide company management with a 'best practice' review of the project management practice	Defining and ensuring adherence to pre-defined processes	To provide the company's management with a 'best practice' review of Information Security	Designed to provide clients and their auditors with information about the controls at the service provider that may affect the clients' financial statements
Nature of Report	Certification - does not provide listing of controls and testing results of auditor	Certification - does not provide listing of controls and testing results of auditor	Certification - does not provide listing of controls and testing results of auditor	Assurance report on whether <ul style="list-style-type: none"> ▪ Description of service provider's controls placed in operation is fairly stated ▪ Controls are suitably designed ▪ Controls are operating effectively over the specified period
Control objectives and activities	Yes, requirements defined by SEI-CMM	Yes, requirements defined by ISO	Yes, requirements defined by ISO	Defined by the user organization, its auditor and service organization

Leveraging on SAS 70



The SAS 70 attestation process can help bring an independent and objective view to the way controls are exercised in a service organization. Most often, it not only helps in enhancing the control structure of the outsourcing arrangement, but also in clarifying the roles and responsibilities between the user organization and its service providers. An experienced SAS 70 auditor can add value to organizations by sharing leading practices relating to various aspects of the outsourcing arrangement. Service organizations should keep the following in mind to ensure that maximum value is derived out of a SAS 70 attestation exercise:

Scope Setting

The SAS 70 scope should ideally be determined through a process of communication with the user organizations and their auditors. In some cases, the SAS 70 requirement may not be limited exclusively to address SOX related requirements. In such cases where other regulatory requirements need to be addressed, a careful analysis of the scope of work is an essential first step for ensuring that the appropriate sets of controls and IT systems that impact the regulated or sensitive information are identified.

Readiness Assessment

Service organizations that are new to the SAS 70 review process should carry out a SAS 70 pre-readiness review. The review facilitates identification and quick assessment of controls that should be implemented or improved prior to the actual audit. The pre-readiness review identifies potential problem areas and provides sufficient time to service organizations to remediate such control gaps, if any. In addition, this review also highlights the expectations, including time commitments that may be necessary from control owners and other service organization personnel. In many cases, service organizations that do not have a pre-readiness review performed, receive

a 'qualified opinion' on their SAS 70 report. A qualified opinion indicates a significant control weakness(es) was noted and a certain number of control objectives were not met for the period under review.

Planning

To ensure that the SAS 70 audit process is smooth, it is important to provide adequate prior intimation about the SAS 70 audit to all the relevant process owners. Ensure that the directive has been communicated from the top.

Get the auditors to hold a SAS 70 workshop where process owners are present, prior to the commencement of the exercise. Provide process owners with the information on communication and other protocols, including aspects such as the kind of evidences to be maintained for the audit.

Encourage service auditors to talk about the areas they feel can be improved upon

The service organizations should not take the SAS 70 attestation as a 'get over with it' exercise. They should encourage the auditors to discuss areas where they feel that other organizations are doing better.

Change in Controls

Service organizations may periodically make changes to its service delivery related processes to correct deficiencies or to enhance capabilities. Such changes should be assessed from a control impact standpoint and communicated to the respective control owners to avoid any surprises at the time of the SAS 70 audit.

Finalizing the SAS 70 auditors

Service organizations should give adequate weightage to the prior experience of service auditors before hiring them. Relevant domain experience will surely help in getting more value from the audit process.

About Grant Thornton India

Grant Thornton India is a member firm within Grant Thornton International. The Firm in India was established in 1935 and is one of the oldest and most reputed accountancy firms in India. Grant Thornton India is also the leading firm in India advising business owners and entrepreneurs with international ambitions.

About Grant Thornton International Ltd

Grant Thornton International is one of the world's leading organisations of independently owned and managed accounting and consulting firms. These firms provide assurance, tax and specialist advisory services to privately held businesses and public interest entities. Clients of member and correspondent firms can access the knowledge and experience of more than 2,400 partners in over 120 countries and consistently receive a distinctive, high quality and personalized service wherever they choose to do business. Grant Thornton International strives to speak out on issues that matter to business and which are in the wider public interest and to be a bold and positive leader in its chosen markets and within the global accounting profession.

For any queries please contact:

Gaurav Sahu

E: Gaurav.Sahu@wcgt.in

M +91 98119 69933

D +91 11 4278 7036

Rohan Abraham

E: Rohan.Abraham@wcgt.in

M +91 98867 70070

D +91 80 4243 0770

Our offices in India:

BANGALORE

3274 / A, 11th Main
HAL 2nd Stage
Indiranagar
Bangalore 560 008
T +91 80 4243 0700

CHENNAI

Unit nos. 13, 14 & 16
11, Thiru-vi-ka Road
Royapettah
Chennai 600 014
T +91 44 45510002

GURGAON

Centre Point
A block,
Sushant Lok, Phase I
Gurgaon 122 022
T +91 124 4628000

HYDERABAD

53 A, Sagar Society
Road No. 2
Banjara Hills
Hyderabad 500 034
T +91 40 64528666

MUMBAI

Engineering Centre
9, Matthew Road
Opera House
Mumbai 400 004
T +91 22 66262655

NEW DELHI

National Office
L 41 Connaught Circus
Outer Circle
New Delhi 110 001
T +91 11 42787070

PUNE

401 Century Arcade
Narangji Baug Road
Off Boat Club Road
Pune 411 001
T +91 20 30224461

Disclaimer:

The information and opinions contained in this document have been compiled or arrived at from published sources believed to be reliable, but no representation or warranty is made to their accuracy, completeness or correctness. This document is for information purposes only. The information contained in this document is published for the assistance of the recipient but is not to be relied upon as authoritative or taken in substitution for the exercise of judgment by any recipient. This document is not intended to be a substitute for professional, technical or legal advice. All opinions expressed in this document are subject to change without notice.

Whilst due care has been taken in the preparation of this document and information contained herein, Grant Thornton, does not accept any liability whatsoever, for any direct or consequential loss howsoever arising from any use of this document or its contents or otherwise arising in connection herewith.



Grant Thornton

© 2008 Walker Chandio Grant Thornton. All rights reserved.

www.wcgt.in