Weighing in on the Benefits of a SAS 70 Audit for Software as a Service providers

With increasing oversight and growing demands for industry regulations, third party assurance has never been under a keener eye than we live in today. From insider scandals to outside threats, the protection of corporate and personal information is the corner stone of information security compliance. Obtaining a current SAS 70 audit report can be a significant differentiator within your industry and provide value to new and current customers.

Statement of Auditing Standards No. 70 (SAS 70) audits have become the global de facto standard in third party information security assurance. The passage of laws like Sarbanes-Oxley (SOX) has sparked other countries to re-evaluate their own forms of SOX regulations; driving companies to enter a new realm of oversight and regulations related to third party assurance. The Public Company Accounting Oversight Board provided guidance with regards to companies that are required to comply with SOX and how to evaluate the risk of outsourcing services to third party vendors. Within this guidance they indicated that a company could utilize a SAS 70 Type 2 audit to evaluate their vendor's control environments, igniting the SAS 70 era for service organizations.

The demand for convenient access to information has driven companies to plug anything and everything into the internet; additionally new technologies have provided organizations a level of comfort to open up their once closed networks to remote employees and third party vendors. Increased flexibility and access to information creates new risks that need to be taken into consideration; standard operating procedures are no longer good enough, organizations need to incorporate regulations and define authorizations to ensure they maintain the level of security that existed in the pre internet world. This change in the way companies' data is accessed and transmitted has propelled the SAS 70 audit to the checklist of business proposals and contract renewal requirements, failure to have a current SAS 70 audit can significantly affect potential or current business relationships.

SAS 70 Compliance | Current and Future Trends

SAS 70 has not been the single solution for service organizations; with foreign countries forming their own compliance standards, service organizations operating internationally were required to adhere to different countries' laws. Due to the varying forms of service organization reports the International Auditing and Assurance Standards Board (IAASB) felt there was a need for a common auditing standard to address the varying differences in each country's audit requirements. As a result the IAASB created and issued the International Standard on Assurance Engagements (ISAE) 3402 'Assurance Report on

Controls at a Service Organization' on December 18, 2009. ISAE 3402 is not a means to replace country specific standards (i.e. SAS 70) but provides a reporting option to address current limitations. The American Institute of Certified Public Accountants has recently updated the SAS 70 audit to more closely align the standard with ISAE 3402; the new standard is Statement on Standards for Attestation Engagements No.16 (SSAE 16) 'Reporting on Controls at a Service Organization' and will become effective in June 2011. Visit our Blog for more information on SSAE 16.

Even with all of the different changes to compliance standards that companies are facing today, as we move forward and align our clients with the appropriate rules and regulations whether it's called SAS 70, ISAE 3402 or SSAE 16 these auditor reports are a marketable and accepted form of qualification for service organizations that will continue to play a vital role in obtaining and retaining customers today and for years to come.

SAS 70 Audit | What is it?

A SAS 70 audit is performed by an independent certified public accounting firm through examining the controls and processes involved in storing, handling, and transmitting data. The successful completion of an unqualified audit illustrates an organization's ongoing commitment to create and maintain suitable controls for the protection and security of its customers' confidential information. Customers of service organizations can easily incorporate the SAS 70 report in their SOX compliance programs as proof that appropriate controls are in place for outsourced services. The SAS 70 audit can also help organizations to comply with other regulations, including HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach-Bliley Act of 1999), and ISO 27001/2.

SAS 70 Audit Services

- **SAS 70 Readiness Assessment** - is a review designed for organizations preparing for their first SAS 70 audit. Organizations who have not formally evaluated their internal controls often start with a SAS 70 Readiness Assessment.
- **SAS 70 Type 1** - provides limited assurance and reports on the design of controls as of a point in time. Organizations that have policies and procedures in place but little or no history of the policies and procedures in operation start with a SAS 70 Type 1 audit prior to undergoing the SAS 70 Type 2 audit.
- **SAS 70 Type 2** - provides the highest level of assurance for SAS 70 audits and reports on the service organization's controls and operating effectiveness over a period of time (generally at least six months).

SAS 70 Type 1 and 2 Reports

- **SAS 70 Type 1 Report** is designed to provide an overview of the service organization's description of internal controls and processes relevant to their customers. The report is helpful to gain an understanding of the controls and processes that are designed and implemented at the service organization. A SAS 70 Type 1 audit report contains an opinion and a description of relevant services under review at a point in time. What does this mean? An independent auditor provides an audit opinion on the controls in place to meet the objectives of your business services under review.
- **SAS 70 Type 2 Report** also provides a description of internal controls and processes relevant to their customers however in addition, the auditor tests these controls over a period of time to verify that the internal controls and processes are actually operating as the service organization intended. Why obtain a Type 2 report? Since your auditor provides an opinion about the operating effectiveness of controls, third parties are more likely to accept a Type 2 report verses a Type 1 report.

Composition of SAS 70 audit reports

There are 4 possible sections of a SAS 70 audit report:

- **Section 1 | Audit Opinion:** An opinion is prepared for each SAS 70 audit report to clearly explain the scope of services under review and the overall conclusion of the SAS 70 report issued. The table below illustrates the components covered in the opinion letters for both of the SAS 70 audit reports.

Opinion	Type 1 Report	Type 2 Report
(1) Whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been place in operation as of a specific date.	Included	Included
(2) Whether the controls were suitably designed to achieve specified control objectives.	Included	Included
(3) Whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.	Not Included	Included

- **Section 2 | Description of Services/Controls:** Includes a description of the company's services under review and a detailed list of the company's policies and procedures with regards to their service offerings. This list should include enough information for your customers to understand the value of the controls in place, but limited to protect proprietary information.
- **Section 3 | Information Provided by the Service Auditor:** (Type 2 Reports only) Includes the control objectives (scope of audit), relevant implemented controls, auditor's description of controls tested and results of testing.
- **Section 4 | Other Information Provided by the Service Organization:** An unaudited section of the report used for informational purposes. This section is often used to describe disaster recovering planning and other regulatory compliance procedures that do not fall within the scope of a SAS 70 audit report.

What's Covered

The SAS 70 covers the "information system" used by service organizations. The information systems are not limited to just computers and software, but any form of handling user organization's information that could affect their financial reporting. The scope of a SAS 70 audit includes procedures that cover the IT General Computing Controls (GCC) supporting your primary information systems. These controls are used in delivering services and sustaining business procedures for organizations processing financial transactions like payroll companies or electronic payment processing organizations. Details of the IT GCCs and business process procedures are as follows:

- An examination of IT GCCs is used to evaluate the integrity of data within information systems utilized in delivering services. This portion of the SAS 70 scope is relevant to all service providers and is the core of your SAS 70 audit. The IT GCCs review will cover the physical security, environmental security, computer operations, problem and change management, logical security and data communications.
- An assessment of business process procedures is used to evaluate how organizations ensure the accuracy, timeliness and completeness for processing financial transactions. This assessment is relevant for organizations like payroll providers, receivable management companies, payment processors and third party administration services. This portion of the SAS 70 scope is not relevant for organizations like software as a service, application service providers or data centers. However business process controls may be integrated in the application software such as a payroll system, retail banking system, inventory system or billing system and require some manual processes like account reconciliations.

SAS 70 Compliance for Software as a Service Providers

Challenging economic times have companies around the world cutting costs and tightening their IT budgets, the potential cost advantages of SaaS over in-house operations is appealing to many organizations. A manageable monthly expense verses a large one-time outlay will continue turning customers to pay as you go SaaS agreements. SAS 70 audits have played an important role to SaaS organizations by providing confidence and assurance to user organizations over the services being offered.

Moving critical business data outside the walls of an organization has propelled compliance departments to assess vendor risk and seek validation of risk protection from data loss or inadvertent exposure of sensitive information. Two factors play into this for SaaS providers, the first is obtaining the customer's confidence around your information security to initially win their trust and business. The second is the SaaS provider's reputational impact caused by a data breach, resulting in the loss of business revenue. A SAS 70 audit for SaaS providers is focused on providing third party assurance regarding the confidentiality, integrity and availability of user organizations data and can help gain customer confidence and reduce risk of information security weaknesses.

Simply put by a SAS 70 audited client "A SAS 70 audit tells our clients that we are doing what we promise," although this may not be the most technical answer, it is generally aligned with the purpose of a service auditor's report.
A SAS 70 audit for a SaaS provider involves reviewing seven critical areas:

1. ***Organizational Level Controls:*** also known as "tone at the top" and is the evaluation of management's oversight and internal operational level controls.
2. ***Physical Security:*** the protection of information systems as it relates to third party data.
3. ***Environmental Security:*** the protection of information systems and data from environmental threats.
4. ***Data backups:*** the availability and protection of third parties data.
5. ***System Availability:*** the availability of information systems to user organizations.
6. ***Application Change Control:*** the processing and procedures used to ensure that systems function per user requirements.
7. ***Information Security:*** the logical protection of data from unauthorized system access.

The scope of a SAS 70 audit is determined by the service organization; however a well scoped audit can ensure that sufficient information is provided to your user organization and communicates your stringent controls over physical security, environmental security, authorized access and continuous availability of services, which clearly demonstrates your organization's quality of services.

Key Benefits

Obtaining SAS 70 compliance has enabled service organizations to instill confidence and integrity directly into the hands of their customers, ensuring the reliability of sound internal controls for increased third party assurance. Key benefits from SAS 70 audits are:

- Instant credibility with current and potential customers
- Third party perception
- Independent assessment of controls
- Potential to grow market share
- Reduction of third party self assessment questionnaires
- One audit report can satisfy multiple customers
- Confirmation that controls, procedures, and processes are in place as management intends

Key Costs

Key cost areas for SAS 70 audits include your company's internal personnel time, training and your audit firm's professional fees. Depending on level of defined policies and procedures internal personnel time and training can vary significantly. The professional fees cost of a SAS 70 audit varies from client to client because all SAS 70 audits are different. However some of the factors that should be considered in

the price of a SAS 70 audit are the size of your organization, the complexity of the information systems under review, the type of services offered and possibly the location of your business.

Lessons Learned

We have found that having a clear plan and efficient execution strategies are the key ingredients to a successful SAS 70 audit. Key success factors for an efficient SAS 70 audit include but are not limited to the following:

- A project plan
- Designation of a SAS 70 project lead
- Scheduling of required resources (members of business units)
- Utilization of experience and educated auditors

Calculating the ROI

A SAS 70 audit provides organizations with tangible and non-tangible results.

- Let's start with the non-tangibles. As a component of your SAS 70 audit, your audit firm provides a complete analysis on your operations writes up a report and delivers management best practice recommendations that could benefit an organization from increase efficiencies to a reduction of fraud risk. These benefits are difficult to quantify, but still valuable information.
- Tangible costs can be found by the number of new customers that selected your organizations because you were SAS 70 audited. Also operating on a higher level of compliance will provide your organization with more leverage with regards to pricing when renewing existing customers' contracts.

SAS 70 – is an internationally recognized third party assurance audit designed for service organizations. It has become the most widely accepted compliance initiative that provides service organizations a benchmark to compare their internal controls and processes against industry best practices. Statement on Auditing Standards No. 70 was originally created in 1992 and over the past five to ten years become globally recognized as one of the highest forms of third party assurance. Organizations can benefit from obtaining a SAS 70 audit, from increasing third party confidence to growing market share.

Authored by Ben Osbrach, CISSP, CISA, QSA
Contact info: Direct 813.924.5404 | Toll free 866.669.6561
osbrach@assuranceconcepts.com
www.assuranceconcepts.com