Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, is gradually becoming a more significant standard for companies. The increasing trend towards the outsourcing of business processes, coupled with greater demands from stakeholders for transparency and the importance of managing and reducing risks, has made SAS 70 examinations a strategic priority for service-oriented organizations. In this paper, I intend to investigate what SAS 70 is, what is disclosed in a typical SAS 70 audit, the objectives of the standard, and companies' approaches and/or views on the standard. In addition, I will address the impact of SAS 70 – what its criticisms and benefits are, and what its future outlook is.

SAS 70 Background

The Statement on Auditing Standards No. 70, or SAS 70, is a commonly recognized auditing standard that was developed by the American Institute of Certified Public Accountants in 1933.[1,2] The standard provides guidance on the factors an independent auditor should use when assessing the internal controls of a service organization. Keep in mind the key words '*guidance*' and '*should*'; SAS 70 is not a pre-determined set of standards that a service organization must meet to "pass". According to a spokeswoman for the AICPA, Judith Sherinsky, SAS 70 it does not help to measure

[1] SAS No. 70, Service Organizations, 2008, 22 November 2008 <http://infotech.aicpa.org/Resources/Systems+Audit+and+Internal+Control/IT+Systems+Audit/Standards+and+Regulations/SAS+No.+70+Service+Organizations.htm>.
[2] Craig Schneider, Stuck in the SAS 70s, 23 February 2004, 2 December 2008 <http://www.cfo.com/printable/article.cfm/3011799>.

security but to measure financial controls.[3] Generally, control-oriented professionals who have experience in accounting, auditing, and information security perform the audit.[4] They can be either the company's own independent auditor or by the auditor of the clients it serves. After the auditor completes an evaluation of the service organization's internal controls it then issues an opinion that is available for public viewing to the service organization's current and potentials users.[5]

Type I and Type II Reports

A SAS 70 audit report can be classified as either a Type I or Type II report. Type I includes the service auditor's opinion on the fairness of the presentation of the provider's description of its controls that have been in place as of a specific date during the organization's operation. In addition, a Type I report includes the auditor's opinion on how well the controls were designed to meet specified control objectives.[5] For the most part, the auditor evaluates the efforts of a service organization to prevent accounting inconsistencies, errors, and misrepresentation, and the likelihood that those efforts will produce a desired result in the future.

Similar to a Type I report, the Type II report will express the same opinions as in Type I. However, the Type II report adds one more element – the detailed testing of the

[3] Richard Bejtlich, Thoughts on SAS 70 and Other Standards, 21 December 2006, 22 November 2008 <http://taosecurity.blogspot.com/2006/12/thoughts-on-sas-70-and-other-standards.html>.
[4] "SAS 70 Overview," 2007, About SAS 70, 17 September 2008 <http://www.sas70.com/about.htm>.
[5] Carpathia Hosting, Inc., SAS 70, 2005, 23 November 2008 <http://www.carpathiahost.com/certificates/sas70.shtml>.

service organization's controls over a minimum six-month period.[6] It is here where the auditor can express their opinion whether the controls being tested were, in fact, operating with sufficient effectiveness to provide reasonable assurance that the control objectives were achieved.[4] Type II is generally preferred and performed more than Type I thanks to the greater depth it includes. In short, both types of the report say "we (as a service organization) have well-designed processes, controls and goals," but Type II has to show that the processes and controls have been practiced and they were successful in achieving their initial operational goals they set out.

Adherers of SAS 70

As mentioned before, SAS 70 provides guidance on the audit of internal controls of a service organization. But what types of companies are typically considered a service organization? A service organization is an entity that provides services or processes transactions.[7] Hosted data centers, insurance claims processors, and credit processing companies provide outsourcing services that affect the operation of an enterprise.[6] SAS 70 may also be relevant to application service providers that develop, provide and maintain the software and provide a technology environment that enables customers to process various types of financial and/or operational transactions. Other examples of service organizations include bank trust departments that invest and service assets for

[6] SAS 70, 28 June 2005, 23 November 2008 <http://searchcio.techtarget.com/sDefinition/0,,sid182_gci1095696,00.html>.
[7] Business Advisory Services Manager Walter Searcey, "Evaluating a Company's controls to Protect Information Assets - SAS 70 Overview," ed. Grant Thornton LLP (Urbana, 2008).

employee benefit plans, mortgage bankers that service mortgages for others, third party administrators, or other data processing service bureaus. [8]

The AICPA limits the scope of a SAS 70 audit to include services that affect: transactions significant to the customer's financial statements, transactions initiated, recorded, processed, or reported by the service organization, and/or storage of accounting records or supporting documentation. It also is limited to: the capture of events or conditions significant to financial statements, financial reporting process, transaction executed by the service organization which were specifically asked of by the client, and/or the audit of transactions arising from the financial interests in a partnership.[7]

Objectives of SAS 70

Why do service organizations have a SAS 70 audit performed? "In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers."[4] For instance, Symantec, a service organization, uses its SAS 70 audit results to avoid having every one of its clients perform their own audit of the company. Others, like Nexum, make similar claims, in that it is creating efficiency by saving itself the trouble of having to be audited by every potential client or having to deal with the piles of documentation in answering each clients' questions.[3]

[8] Service Organizations, 2008, American Institute of Certified Public Accountants, 22 November 2008 <http://www.aicpa.org/download/members/div/auditstd/AU-00324.PDF>.

Besides having the SAS 70 audit to create efficiencies, service providers say they are being asked more and more often for the audit.[8] With the continuous news headlines of companies committing fraud, not disclosing sufficient financial information, or lacking any controls – corporate due diligence has been increasing exponentially and resulting, in one aspect, more SAS 70 audits performed. Ernst & Young, LLP, a public accounting firm, believes SAS 70 is another form of communication, "… it is not just a tool for meeting a client's requirements. Rather it is a highly useful description of an Asset Manager's controls, processes and procedures – and can be used to communicate details of those controls and processes to its client."[9]

Having interviewed a Technology and Security Risk Services manager at Ernst & Young, LLP, only further supports companies' reasons for having the audit. "Overall, SAS 70 audits are very important and necessary for service organizations; because, they show the effectiveness of a service organization's internal controls. By having a SAS 70 performed, a company's internal controls do not have to be reviewed multiple times by different customers to gain comfort that adequate controls are in place. SAS 70 reports have become increasingly popular since Sarbanes Oxley (SOX) and the majority of large companies that service multiple customers have a SAS 70 audit/report performed. The

[9] Ernst & Young, LLP, SAS 70, 2008, 23 November 2008 <http://www.ey.com/global/content.nsf/International/Asset_Management_SAS70>.

two types of SAS 70 reports that can be performed both offer a wide variety of benefits. I anticipate that SAS 70 audits will continue to be popular and required going forward."[10]

Another illustration of why a service organization might have a SAS 70 audit is Gmail. Gmail users have been trusting Google with their private information, whether it be emails, schedules, documents, or photos. For this reason, Google has mad one of its top priorities to keep people's information safe. In the past, Google had published some of the ways it keeps sensitive data where it belongs but wanted to take it a step further and have an external independent security specialist audit its systems and procedures to provide additional assurance to its users. Subsequently, an independent public accounting firm verified the effectiveness of Google's technical processes and controls and completed a SAS 70 Type II report, thus creating another form of assurance of security and controls to its users.[11]

Company Approaches

Keeping service organizations' objectives in mind, it is helpful to see what approaches different auditors take to perform such an audit and whether there are any distinct differences between their methods. Overall, there can be many different approaches to take when conducting a SAS 70 audit and still have sufficient results.

---

[10] "Ernst & Young TSRS Manager," SAS 70 Objective in Accounting Technology Service Interview, Christa Unangst (Chicago, 2 December 2008).

[11] Eran Feigenbaum, SAS 70 Type II for Google Apps, 4 November 2008, Google, 1 December 2008 <http://googleenterprise.blogspot.com/2008/11/sas-70-type-ii-for-google-apps.html>. Eran Feigenbaum, SAS 70 Type II for Google Apps, 4 November 2008, Google, 1 December 2008 <http://googleenterprise.blogspot.com/2008/11/sas-70-type-ii-for-google-apps.html>.

PricewaterhouseCoopers

As one can see in Figure 1, PricewaterhouseCoopers (PWC) uses an approach that combines actions to be undertaken to build and institute a Control Framework by its client, which are the lighter shaded boxes. It is at the same time as those phases where the SAS 70 Type II attestation takes place, which are the darker shaded boxes. PWC's approach involves six main steps, which include: understanding and scoping, define control objectives, document controls, gap analysis, evaluate design effectiveness, and evaluate operating effectiveness.[12]

Figure 1

The PwC SAS70 Approach

Ernst & Young

Ernst & Young has a five-step approach for a SAS 70 audit enables Ernst & Young management to measure its own effectiveness on a continuous basis. The first step is *planning and pre-assessment*, which includes determining and validating the

[12] Third Party Assurance - SAS 70, 2008, 2008 11 December <http://www.pwc.com/servlet/pwcPrintPreview?LNLoc=/extweb/service.nsf/docid/103a748ca4eb31818025718b002ea0ed>.

scope and content of the initial SAS 70 report. Additionally, the engagement team clarifies roles, determines communication methods, and validates key business processes. The primary function of this first step is to enable Ernst & Young to understand the client's control systems and considers it a necessity for smooth implementation of the next step. The second step is *identification of control objectives*. Here the team works to develop a draft report and identify the relevant control objectives, which runs concurrently with the remaining steps until completion of the audit.

The next step is *documentation*, where narratives are developed and walk-throughs are performed. Ernst & Young reasons that this step helps to solidify its understanding of the processes and key controls of each area under review. The engagement team continues to have discussions with client management to create relevance and suitability of particular control designs in achieving the control objectives. The fourth step is *design and execution of testing*. The team prepares a testing plan to assess the necessary controls and is required to test transactions throughout the period under review.

Finally, once testing has been performed, the fifth step can commence, *reporting*. This step is considered the 'wrap-up' phase in which an initial reporting to client management. It eventually ends with the production and completion of the official SAS 70 report. Usually, Ernst & Young SAS 70 auditors include the following in its report: exceptions to be disclosed in the report if there are any, items identified during the course

of the review which had controls, and lastly, recommendations for improvement that were noted during the examination. Additionally, the team performs a quality control procedure to ensure that the report accurately reflects the controls and processes that were outline earlier in the process.[13]

Grant Thornton

Another accounting firm, Grant Thornton, employs a four-phase approach when performing a SAS 70 audit. The first phase is known as the *SAS 70 Readiness Review*. According to Walter Searcey, a Business Advisory Services Manager at Grant Thornton, during this phase the engagement team makes sure that it fully understands the business processes and information technology services of its client. Furthermore, the team identifies key business processing controls, analyze and assess any gaps present, review/assist with description of controls and develop an action plan to complete the remaining three phases.

The second phase, *Fair Representation and Suitability of Controls*, is the phase where the team evaluates the description of controls to ensure fair representation of its system of internal controls. The team also evaluates the suitability of the design of the controls and of their control objectives. Next, is the *Test and Observe* phase in which validation of the controls listed are present as of a certain point in time and application of tests of Inquiry and Observation to determine appropriateness of design. The fourth and

[13] Our 5-step approach, 2008, 2 December 2008 <http://www.ey.com/global/content.nsf/Ireland/Risk_&_Advisory_Services_-_Services_-_SAS_70_-_5_step>.

final phase is *Report and Attest*. The Grant Thornton team will now develop the SAS 70 report, document results of tests, and develop and present identifying issues, findings, and any recommendations it may have. [7]

SAS 70 Criticisms

Many service organizations, auditors, and users of SAS 70 have criticisms about the auditing standard and claim that it is in need of a major overhaul. Some believe that ISO17799, NIST SP-800-53, Cobit, ISO 9000, or SysTrust, just to name a few, could better serve as an audit tool than SAS 70. These would provide better controls provided they fit the company's operations and business.[14] Other criticisms that will be further discussed include the standard being insufficient and too broad, creating more work, and how it is incompatible with Sarbanes-Oxley, especially as it pertains to Section 404.

Insufficient

Firstly, SAS 70 is an insufficient audit and is not properly geared towards complex information systems infrastructure, especially in today's business world.[15] It is too broad of an audit test and does not provide enough information on the service provider due in large part to the audited company being able to determine its own scope and controls. Then the auditor only reports on what controls are present, which are essentially chosen by the client, resulting in a lot of important information being

[14] Answering SAS 70 Criticism, 7 December 2007, WordPress, 1 December 2008 <http://blog.saije.net/2007/12/07/a-sas70-apologist/>.
[15] NDB, LLP Accountants & Consultants, SAS 70 Compliance Resource Guide, 2008, 23 November 2008 <http://www.sas70.us.com/>.

omitted.[16] Moreover, the auditor is only required to inform its users of any failures.[2] The users of the SAS 70 information are not getting any real security assurances. It lacks rating a service organization's security controls against a particular set of defined best practices.[3]

Creates More Work

Some believe that SAS 70 creates more make-work for Certified Public Accountants. In order for accountants and auditors to be able to perform a SAS 70 audit and the corresponding tests, they are now obtaining technology certification. When, in reality, the service organization would be better handled engaging with a technology-consulting firm who conducts specialized technology testing.[15] Furthermore, some consider the standard is designed to drive up billable hours. The SAS 70 audits are expensive because the auditors are there the whole time since the controls have to be tested over time. [14] As a result of the standard creating more work, consultants are stating that service organizations and auditors alike are skipping all the hard work and treating the standard merely as a 'security stamp', place it somewhere really obscure, and then never read it.[3]

Incompatible with SOX

Opinionates find that SAS 70 is not a technology audit but instead is a compliance audit that examines the characteristics of internal controls as it relates to a service

[16] The Roadmap to SAS70 Success - Selecting an External Auditor, 5 March 2008, WordPress, 22 November 2008 <http://blog.saije.net/tag/sas70/>.

organization. However, even the standard does not guarantee compliance with SOX. Should the audit be performed out of sync with the client's reporting period it would create failure to comply. For instance, if an audit is performed in June and the client's fiscal year ends December 31st, there is a six-month gap in the attestation of the internal controls. The controls could falter in the second half of the year and the accuracy and reliability of the client's own year-end could be compromised.[2]

The standard creates the possibility of conflicts of interest and a number of businesses to run into trouble. The PCAOB sees no difference between Section 404 compliance of SOX audits of a company's internal business processes and its outsourced processes. Either way anyone looks at the situation, an external auditor who is performing Section 404 work cannot also provide consulting services to the client or the outsourcing provider on completing a SAS 70 audit. This might dissuade other companies from outsourcing some of its business processes in emerging nations. In the short run, it will dampen outsourcing until the service providers can establish that they have adequate controls in place and evidence to prove it.[2]

SAS 70 Benefits

While there are many negative aspects toward SAS 70, there are also many positive ones. "Overall, the audit is a demonstration of both the legal and business

commitment to superior levels of reliability, availability, and security."[17] It helps to provide a sort of checks and balances. Even though there is not a single objective standard, some view that as acceptable because, for instance, a financial organization's controls should differ from a software development's controls. Additionally, there are claims that other types of audits can better serve a service organization than SAS 70. However, when a company provides services to hundreds or even thousands clients, a SAS 70 audit is more viable option. Imagine a service organization having to negotiate on an annual or quarterly basis to ensure each client's audit needs are met – one can simply have a SAS 70 audit performed.[14] Furthermore, clients of the service organization being audited can use the final report to help with their own auditor in planning the audit of the clients' organization's financial statements.

Timing was a notable criticism of SAS 70 and how it is not compliant with SOX. To help remedy this, service organizations could have quarterly auditors to fill gaps. Clients and/or users would then be able to trust that the SAS 70 audit is consistent, safe and reliable and compliant with emerging regulatory mandates. Various accountants and service organization leaders consider SAS 70, more specifically Type II reports, demonstrate that the infrastructure, applications, and processes have passed rigorous independent third party testing and have an environment that incorporate the processes and controls that are necessary for effectively hosting and exchanging corporate data and

[17] SAS 70 and SAS 70 Type II Drill Down- Important Differences Between SAS 70 and SAS 70 Type II, 2008, 1 December 2008 <http://www.usa.net/services/sas-70-type2.asp>.

financial information.[17] Another potential benefit of SAS 70 is its ability to differentiate service organizations from its peers by demonstrating the establishment of effectively designed control objectives and activities. However, even if there are many benefits of SAS 70, does that mean it is here to stay?

Future Trends

Based on current regulatory compliance demands, it appears that SAS 70 is not leaving any time soon. Companies are continually becoming more global to stay competitive in the marketplace and with the impending adoption of the revised SAS 70 audit standard as an international audit standard, the demand for SAS 70 services worldwide will continue to grow. Over the years, the number of SAS 70 audits has grown explosively due to the massive wave of regulatory compliance mandates and legislation unleashed, especially in the United States. Based on previous testimonies, presentations, and interviews SAS is here to stay, and often used as the main 'go to' audit tool. In a world that is full of uncertainty and with businesses facing crises, a SAS 70 audit certification can prove to be a powerful demonstration of a service organization's dedication to endure and grow no matter what the future has in store for it.

Conclusion

All things considered, service organizations must be able to convey trust and confidence in their controls if they are to retain and gain new customers in a world of changing auditing standards. A SAS 70 audit can help deliver this confidence but as with

any tool, it can easily be misused, intentionally or through a lack of understanding the purpose and benefits of the standard. This paper attempts to create a better understanding of SAS 70 by determining what exactly it is, what information it discloses, who it pertains to, and reasons for having it. Coupled with the background information on SAS 70, I was able to identify auditors' different approaches to completing a SAS 70 audit, what criticisms and benefits it has created and what is its future outlook. In closing, service organizations, such as IT, are becoming integrated into business strategy and being considered a partner in the business instead of a service provider who has no effect on revenue. Thus, is clear that clients value a successful completion of a SAS 70 report for it reinforces a service organization's commitment to providing the best hosting experience in the industry.