SAS 70

BADM 559 – C

Jong Choi

Table of Contents

Executive Summary

Service users are constantly looking for more assurance in order to make a better, more informed decision in this ever-changing business environment. As a consequence, reliability of company service and its internal controls have been a critical source of the service users' confidence. In 1992, American Institute of Certified Public Accountants (AICPA) developed Statement on Auditing Standards No. 70 (SAS 70) to provide more assurance on the service organization's control to these service users or also called as user organization.

SAS 70, which soon became internationally recognized auditing standard, assesses contracted internal controls of a service organization and provides report with which user organization may use to examine a company's reliability of accounting information. There are two types of a report, Type I and Type II, and each report is composed of 4 phases which are "opinion of service auditor", "description of controls", "control objective", and "other information provided."

This paper will also explain the benefits of SAS 70 from the perspective views of both service organization on which auditors perform SAS 70 and user organization who uses the SAS 70 report generated by the auditor. Furthermore, Grant Thornton's practical approach to perform SAS 70 work will be discussed.

In conclusion, SAS 70 benefits service organizations to demonstrate that the organization has effective controls in place. Moreover, SAS 70 benefits user organizations in terms of providing greater understanding and assurance of the internal controls at service organizations.

Overview of SAS 70

SAS 70 helps service auditors to assess operational and technical controls of a service organization and issue a service auditor's report. Service organization is an entity that provides services or processes transactions. In another words, service organization provides outsourcing services that impact the control environment of their customers who refers to be service users or user organization. Typical service organizations may include insurance and medical claims processors, hosted data centers, application service providers, and credit processing organizations.

In this dynamic global economy, it is critical that service organizations must demonstrate that they have dependable operational and technical controls that their user organizations can rely on. In many incidents, these service organizations input their users' sensitive data which must be kept confidential and produce requested outputs. There must be a convincing assurance that the user organizations' data is secure. SAS 70 can assure the user organizations that service organizations have adequate controls in place. Specifically, auditors performs an in-depth audit of the service organization's control objectives and control activities, which may deeply associated with controls over information technology and related processes.

Furthermore, numerous authoritative acts and legislations strengthen the importance of SAS 70. To name a few, the Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act of 1999, and most distinctly, Section 404 and 302 of Sarbanes-Oxley Act of 2002 are the prominent examples. These legislations mainly urge service organizations to strengthen its ability to protect user's privacy, corporate accountability, and establish adequate internal controls. As a result, service organizations file SAS 70 to be compliance with these acts and provide high level of assurance and confidence for user organizations.

Background

SAS 55

AICPA's effort to establish requirements to assess the internal control started with issuance of SAS 55. In 1988, the AICPA issued SAS 55, named "Consideration of the Internal Control Structure in a Financial Statement Audit". Being compliant with SAS 55, a service organization had to allow auditors to assess its internal control which may impact user organization's financial reporting objectives. Especially when the user organization outsourced its critical process which had direct impact on the financial statement to service organization, the each user organization's auditors had to test service organization's internal control separately to see if there is any failure or fraud in the system. However, in reality, too many user organization's auditors were required to perform the same internal control test to be practically eligible. Service organizations had to spend devastating amount of resources which were economically inefficient to comply with the SAS 55. AICPA had to eventually amend the existing issuance to SAS 70. Contrasted to SAS 55, SAS 70 required only one internal control review to be performed and the service auditor's report was allowed to be used for all of the clients' auditors.

SAS 94

As technology advances in business industry, AICPA introduce SAS 94, named "The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit" in 2001. This SAS 94 amended existing SAS 55 to emphasis on the elevating importance of information technology on meeting financial reporting objectives. Eventually, SAS 70 also focuses on importance of information technology in the control environment.

Type I and Type II

To properly plan the adequate plan procedures and evaluate associated controls risks, auditors must first gain a thorough understanding of controls at the service organization. Then, auditors can effectively communicate the information about the controls to a service organization through a service auditor's report. There are two types of service auditor reports.

A Type 1 includes the service auditor's opinion on the fairness of the presentation that describes the service organization's control placed in operation as of a specified date. It also reports whether such controls' design is adequate and suitable to provide reasonable assurance in purpose of achieving the specified control objectives. However, because the report provides assurance over only a single day, there may be limited value to the third parties or information users.

A Type II includes the information contained in a Type I report as well as the service auditor's opinion on whether the specific controls were operating effectively. The auditor's opinion is produced after detailed testing of the service organization's controls over a period of time, which is typically a period of six months or longer. The opinion covers not only the fairness of representation of the control and the design of controls to examine its ability to meet the defined control objectives but also the operational effectiveness of the control after being tested. The third parties can find great value to this report which provides auditor's verification of the controls for a substantial period of time.

The following table 1* further explains and clarifies the difference of Type I and Type II.

TABLE 1. CONTENTS OF TYPES I AND II REPORTS

Information	Type I	Type II
SAS 70 Service Auditor's Report	Required	Required
Description of Controls	Required	Required
Information Provided by the Service Auditor (a detailed listing of controls and testing of operating effectiveness)	Optional	Required
Information Provided by the Service Organization	Optional	Optional
User Organization Control Considerations (controls that user organizations have in place)	Optional	Optional

* Source: Christopher Nickell

Organization and Content of Report

Each report has four sections as follows

Section I: Opinion of Service Auditor

Section II: Description of Controls

Section III: Control Objectives

Section IV: Other information provided

Section 1

Section I is about an opinion letter prepared and signed by an independent service auditor. The opinion letter, whose contents are responsibility of the service auditor's, communicates service auditor's opinion of the internal controls to a service organization. The opinion deals with 1) whether the service organization's description of controls is stated fairly 2) whether the design of

controls placed in operation is capable of meeting specified control objectives, and 3) whether the controls is actually operated effectively as designed on a specified date.

Section II

Section II includes description of controls from service organization's management. The service auditor may assist the management in the process of preparing the description, but the ultimate responsibility for contents written in the description remains for the management. The description of controls primarily contains information about the service organization's internal control environment. This information is mandated to follow five components of COSO framework (Frazier) (Exhibit 1). The components include control environment, risk assessment, control activities, information and communication, and monitoring.

- Control Environment

  The control environment describes how risk is viewed within the firm. It helps the auditors to examine service organization's foundation for core values of internal control. Example includes risk management philosophy and risk factors, integrity and ethical values, and the way management allocate authorities and responsibilities to the organizations.

- Risk Assessment

  Risk assessment identifies and analyzes not only external but also internal risks that prevent the firm from achieving specified control objectives. Therefore, risks should be analyzed in terms of possibility and potential effect to be determined how they should be managed. Furthermore, the firm should clearly establish the firm's operating objectives

before assessing these risks. Because of consistently changing economic conditions, more creative and updated approach should be implemented to deal with unexpected risks.

- Control Activities

  Control activities represent policies and guidelines which should be established and implemented in support of ensuring the risk responses to be carried out effectively. Necessary controls should be put in place throughout the entire organization to effectively achieve the operating objectives. Unless all levels and all functional groups follow the controls, the activities will not work. These activities include the right authorization procedures, fair operation performance review, proper segregation of duties, and etc.

- Information and Communication

  Relevant information should be recognized and communicated throughout the entire organization top to bottom and vice versa in an appropriate form and timeframe so that people can understand their responsibilities. Examples of the information may include operational, financial, and compliance-related data relevant to the control of the firm's operation. These information may be not only internally but also externally generated.

- Monitoring

  Ongoing systematical monitoring and separate evaluations should be implemented so that management can effectively supervise the internal control system. As any deficiencies are identified, management should report the concerns to the upper management so that necessary modifications could be made to improve the process of monitoring.

Section III

The third section focuses on explaining control objectives with further explanation of control activities and tests that are performed by the service auditor. Generally, control objective is to provide reasonable assurance that either newly-created or enhanced from existing application are thoroughly tested by service auditors, approved by managements, and document for future usage. For example, if a control activity is to provide assurance on whether a customer authorization is secured via Task Order Authorization (TOA)", service auditors should, depends on the quantity, randomly or entirely select the TOA for further examination. Then, service auditors should test whether TOA secured the customer authorization and whether the necessary documents were recorded in the procedure for potential improvement.

Section IV

Section IV is about any additional information that was not discussed above. Usually this section is not required. However, some service organizations use this section to present any information that they want to communicate to their clients yet was not included in the description of controls. Examples may include upcoming system changes or organizational restructurings, further explanations about certain exceptions in this report, and summary of disaster recovery plan.

Benefits to a Service Organization

A SAS 70 report with an unqualified opinion can add significant value to a service organization by providing assurance on the foundation of effective internal control put in operation within the firm. The service organization may also provide other benefits to the client or information users. By performing SAS 70 audit, the service organization can build up the firm's reputation by

demonstrating that they are confident in their internal control system and they are willing to go even beyond the client's expectation with additional document which is not actually required.

Moreover, with SAS 70 report, clients do not need to send its auditors to make sure the internal control is operating well as designed. Frequent audit request from the user auditors will consume the service organization's resources in terms of time and effort. SAS 70 can reduce these kinds of unnecessary operating costs for the firm.

Furthermore, if the service organization is engaged in Type II report, the firm may be advised on its existing control policies and procedures. Typically, SAS 70 providers are well-experienced consultants who have various types of understandings in areas such as in accounting, auditing, and information management. Those professionals can identify significant opportunities and provide recommendations for improvement in the firm's operational areas.

Benefits to a User Organization

With SAS 70 report, a user organization can receive assurance regarding the service organization's control system. The user organization can obtain the detailed descriptions of control as well as independent auditors' opinion on whether the control is effectively designed and being operated. This assurance could be critical when the user organization tries to decide whether it will invest in the service organization or cooperate with the organization.

Additionally, when the user organization's auditor performs an audit of the user organization's financial statements, SAS 70 report could be extremely beneficial. As mentioned before, the service auditors examine the service organization's internal controls with highly constructed and reliable COSO framework. The user auditor does not need to additionally figure out what would be the best way to examine the service organization's internal controls beyond the COSO

framework. Furthermore, while the user auditors are performing audits, the service organization can effectively assist in completing the audit responsibilities with SAS 70 already performed. Consequently, the user auditor may pay fewer visits to the service organization, and the user organization can ultimately save more money because many user auditors are paid by hour.

Grant Thornton's Approach

Grant Thornton has the following four-phased approach when performing SAS 70 work.

Phase 1 – SAS 70 Readiness Review

Phase 2 – Fair Representation and Suitability of Controls

Phase 3 – Test and Observe

Phase 4 – Report and Attest

Phase 1

In phase 1, Grant Thornton (the Company) gains adequate understanding and identifies the key business processing and information technology controls within a service organization. Then, the Company identifies current status and desired future stage of the firm's internal controls with the management. With clear understanding of what is expected and what should be done, the Company finally create systematical action plan to provide quality work in timely manner.

Phase 2

Grant Thornton primarily evaluates the service organization's representation of control description and suitability of controls. The Company has to study whether the management fairly represented the description of its internal controls. As uncertainties and questions regarding the description come up, the Company can discusses them with Grant Thornton to

provide clearer representation. Then, the Company assesses the effectiveness of the control design to assure whether the control can achieve the specific objectives especially which can impact the clients' financial statement.

Phase 3

In phase 3, Grant Thornton primarily tests and observes the service organization's controls to see whether it operates as described by the management. The Company performs inquiry, inspection, observation, re-performance to test the specific control activities (Exhibit 2). Such test may include observation of control being processed, inquiry to management regarding the existing controls, and inspection of control guidelines and procedures.

Phase 4

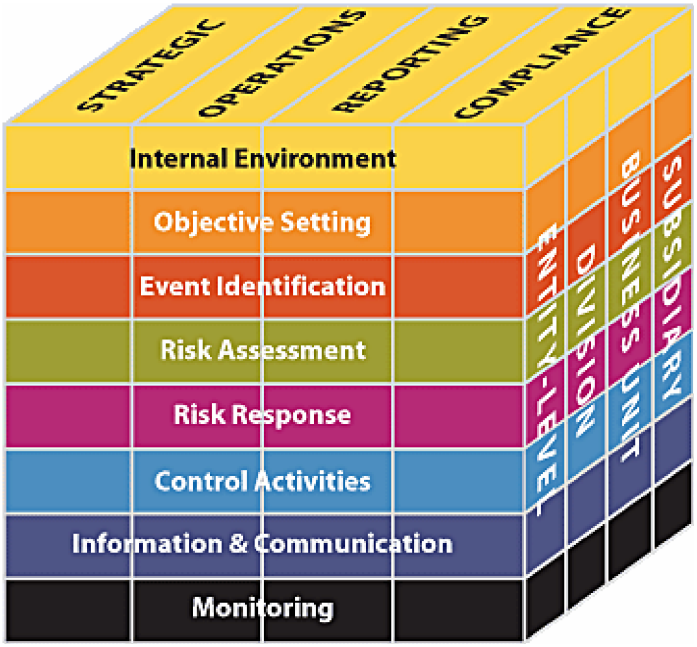
Finally, Grant Thornton develops Independent Service Auditors' Report for the SAS 70 engagement. As mentioned earlier, the report contains information which shows whether descriptions of controls are represented fairly, whether control design are suitable to achieve specified objectives, and controls are operating as designed on a specified date. For Type II report, the Company also includes its opinion on operating effectiveness of the service organization's control for a certain period of time.

Conclusion

Over the years, SAS 70 is gaining its importance in providing assurance of a service organization's control to a user organization. A well-constructed description of internal control as well as auditors' results of operating effectiveness indeed provides trust and confidence to both the service organization and the user organization. Specifically, SAS 70 helps service organizations to demonstrate that the firm has effective controls in place. Furthermore, SAS 70

provides benefits to user organizations in terms of offering greater understanding and assurance of the internal controls at service organizations. SAS 70 will unquestionably help both service organizations and user organization to make better and more informed decisions.

Exhibit 1*



*COSO is model for evaluating internal controls developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Source: COSO

Exhibit 2

TYPE	DESCRIPTION
Inquiry	Inquired of appropriate personnel. Inquires seeking relevant information or representation from [COMPANY A] personnel were performed to obtain among other things: • Knowledge and additional information regarding the policy or procedure. • Corroborating evidence of the policy or procedure. As inquiries were performed for substantially all controls, the test was not listed individually for every control shown in the accompanying matrices.
Inspection	Inspected documents and records indicating performance of the controls. This includes among other things: • Inspection of reconciliations and management reports that age or quantify reconciling items to assess whether balances and reconciling items are properly monitored, controlled and resolved on a timely basis. • Examinations of source documentation and authorizations to verify propriety of transactions processed. • Examination of documents or records for evidence of performance, such as existence of initials or signatures. • Inspection of [COMPANY A] systems documentation, such as operations manuals, flow charts and job descriptions.
Observation	Observed the application or existence of specific controls as represented.
Reperformance	Re-performed the control activity as described by [COMPANY A]. This includes among other things: • Reperformance of a reconciliation process to confirm the accuracy of the reconciliation. • Reperformance of a review of supporting documentation to confirm that all necessary documentation was present to support the transaction. • Reperformance of a system calculation to determine the accuracy of the calculation.

*Source: Grant Thornton

Reference

SAS 70 and Treasury, Time for a Change.Preview, Rieger, John R., AFP Exchange, December 2006, Vol. 26 Issue 10, p20-20

The New SAS No. 78. (Statement of Auditing Standards). David R. Frazier and L. Scott Spradling. *The CPA Journal* 66.n5 (May 1996): pp40(10)

An introduction to SAS 70 audits.(Statement on Auditing Standard). Christopher G. Nickell and Charles Denyer. *Benefits Law Journal* 20.1 (Spring 2007): p.58(11)

Committee of Sponsoring Organizations of the Treadway Commission. "Enterprise Risk Management - Integrated Framework." September 2004 <http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf>

Grant Thornton, “Report of Independent Service Auditor”, December 15 2008 <https://compass.uiuc.edu/webct/urw/lc5116011.tp0/cobaltMainFrame.dowebct?ICPRODID=yHg6JG4TjxzspFr3Ty1S55XQC9TgvZ4Jsvd2pvLy4wR9BRgNVc3!-877021073!icprod04d.cites.uiuc.edu!8080!-1!1252379963!icprod01b.cites.uiuc.edu!8080!-1>