Understanding a SOC Report

In current scenario of emerging technologies, most of the organizations outsource few aspects of their business to vendors which can either include performing a specific task or replacing an entire business function. Vendors can handle various functions like customer support, financial technology, data storage, software development etc. With all these advantages, organizations should also consider various inherent risks associated with outsourcing.

To get a comfort on the vendor's environment and internal controls, organizations usually ask them for a either SOC 1 or SOC report. However, on receiving a SOC 1 or SOC 2 report, most of the organizations do not know how to read it, what exactly a qualified opinion is and whether the risks you are looking to mitigate are addressed in the report. SOC 1 and SOC 2 reports are lengthy and complex, but play extremely important role in understanding the risks to your organization. In this article, we will touch upon some key components of SOC 1 and SOC 2 reports that will help you analyze the security of your vendors.

Categories and Types of SOC Reports

SOC reports are majorly of two categories i.e. **SOC 1** & **SOC 2** each of either **Type I** or **Type II**.

The **SOC 1** report attests the company's *financial reporting*. IT is particularly important for a service organization that impacts the user entity's financial reporting. Some examples of organizations which may require **SOC 1** reports are:

- Payroll processors
- Medical claims processors
- Data center companies
- Lending services
- Data centers
- Cloud service providers
- Human resources support services

A **SOC 2** report highlights the ***security and protection of customer data***. A **SOC 2** report follows a similar approach as SOC 1, but includes the controls over IT and systems processing confidential client data. **SOC 2** audits focus on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy. A **SOC 2** audit is one of the best practice for any service-based organizations that store, manage, or process client information in the cloud. The report is beneficial for any service organization processing or maintaining information that requires a controlled or secure system.

Further, each of the above reports can be of following two types:

Type I – A report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description **as of a specified date**.

Type II – A report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description **throughout a specified period**.

Structure of a SOC Report

A SOC report broadly consists of following sections each having its own purpose and containing specific information about the client's environment.

Section 1: Independent service auditors' report

This section generally starts with '*To the management*' and is signed by the service auditor /CPA. It is more of the service auditor oriented and contains following key aspects related to service organization:

- Scope explaining the type of report, testing date/duration (*Type I or Type II*) , in scope locations and any omissions
- Responsibilities pertaining to both the service organization and the service auditor
- Inherent Limitations
- Service auditor's opinion on the system description, design, and operating effectiveness to meet the control objectives
- Statement around the restricted user of the report and the intended users.

Section 2: Management's assertion regarding the effectiveness of its controls

This section provides the reader the facts and assertions made by the service organization's management related to the system(s) under audit.

- It provides the contents that will be covered in the description, i.e. the types of services provided, the components of the system, how the system captures and processes significant events, any applicable trust services criteria, and etc., as well as make the statement that the controls described are suitably designed and are operating effectively.
- It also provides the signed Management Assertion letter accepting responsibility for the description provided.

Section 3: Management's description of its system and controls

This section is the heart of the report and provides the details of the systems being reported on (*written by management*). Following are the key components of Section 3:

- Scope and purpose of the report explaining the type of report, testing date/duration (*Type I or Type II*) , in scope locations and any omissions
- Company overview and background and Overview of products and service which provides a brief introduction about the organization, it's background and the products / services company offers
- Details related to company's IT infrastructure including the network overview, servers, tools & softwares used and the data management.
- Company's organizational structure, policies & procedures, risk assessment, governance & oversight and details about the control environment.
- All the control descriptions with their functioning, subservice organizations, user entity controls, and other system information
- Inclusions in this section should be capable of being audited to meet the control objectives

Section 4: Applicable trust services principles' criteria and control activities

This section depicts the test results and the overall effectiveness of the control objectives. For a type 1 report, you can only see the conclusion and for a type 2 report both the test procedures and the conclusions. It shows the following four columns of information:

- Control objective (*related to the applicable trust service principles/ controls over financial reporting*)
- Controls in place at the service organization to meet the objectives
- Auditor's tests (*explaining the test procedures performed*)of the controls
- Overall results and conclusion of the tests

Section 5: Other information provided

Lastly, we come to Section 5, which is other information not covered by the auditor's report. This section is available for any additional information that you would like to provide to the users of the SOC report concerning your services system. In this Section, management can discuss items such as a strategic plan or a business continuity plan, or any other items that they feel would be beneficial for the report users.
All sections listed above apart from the Independent Service Auditors Report (Section 1), are the responsibility of management of the service organization. It is important to be as detailed as possible when creating your SOC report in order to explain the services system and the controls over that system in way that is helpful to the report users, and supportive in trying to arrive at a desired audit opinion.

You can also visit below link to read AICPA articles related impact of COVID 19 on audit and assurance.

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html

Please reach out to us in case you would like to discuss more on this topic or if you have any queries related to SOC reporting.