SOC Audit Case Study for a Payroll Process

This query has been heard many times by different organization that -What is SOC 1 report? and from more than 20 years it has been trend by many organizations to outsource certain activities or business process to other organizations, this outsourcing organization is known as 'Service organization' and the organization or company which outsource its certain activities is known as 'user entity' in SOC terminology. So, a SOC 1 (also known as SSAE 18) report is called Service organization control report, this is a report on controls (Business process and IT controls) at a service organization which are relevant to user entity's internal control over financial reporting.

Let's try to understand it with below case study which highlight how we conduct SOC Audit for a company which provides Payroll Processing services to their client or user entity:

So, SOC 1 audit is an audit of a company's process that they have in placed/implemented to ensure the internal controls over Financial reporting of their services which they provide to their client or user entities. As it was the first time the company was going for the SOC Audit. so they had quite less understanding about the audit process and how to be dealt with the ongoing SOC audit and what is required to comply with that.

Since they were going for first time SOC Audit so, they faced many challenges during the SOC Audit process, such as they hardly knew what all should be covered in SOC audit and which systems and Department will be part of the Audit. They didn't have understanding of SOC audit, Readiness Assessment how to comply with it. Initially, we provided the detailed overview of the SOC Audit and its requirement with readiness assessment and Audit process. Due to the conversation happened between us and the company about the understanding of SOC audit. We made sure before starting with the SOC Audit, the company is well aware of the following terms:

- What is SOC audit?
- Why SOC audit is conducted?
- Who is user entity, service Organization and sub-service organization.
- How SOC audit helps the service organizations?
- What all are covered under SOC audit
- Difference between SOC1 and SOC2
- Duration of the SOC audit

So after detailed discussion and knowledge transfer, they come up with the decision that Payroll Process and related applications and Network Infrastructure would be covered as a scoped process for this SOC 1 Type I Audit and after that they'll go for Type II Audit.

SOC 1 Type I Audit for Payroll Process

Once the Audit scope is finalized then we started with the understanding of the business process and for that we First conduct a kick-off meeting with the senior management and heads of all departments which were scope of the Audit for Payroll Process followed by complete business

understanding about each department which includes HR department, IT department, Payroll Department, Internal audit team, Network infrastructure team etc.

After having complete business understanding of various departments, we headed towards the next step which was Readiness Gap Assessment. Readiness/Gap Assessment is generally conducted to assess the organization with basic level of hygiene check as per AICPA requirements and it is usually done a month in advance of the actual audit. This was done by going to the company's office to interview key personnel within the organization and understand the design of controls which the organization has implemented to comply with the SOC Audit requirements.

After conducting Readiness Gap Assessment, we provided the initial readiness gap assessment report to the company. The company started working on all the gaps as per AICPA requirements and they started re-framing all the policies and procedures and controls related to their payroll process. After working upon the gaps, company gave a closure to the readiness gaps assessment report with a sample evidence of the closure.

Once the organization gave the disclosure to start the actual Audit then we started our audit with the drafted controls which were provided by the service organization and then we mapped those controls with AICPA control objectives framework. Once the controls were mapped with the standard framework then sample methodology defined and we decided to take 1-2 samples for each controls to test the design effectiveness of the controls. SOC 1 Type I Audit is the report which focuses on company's internal controls over financial reporting at a particular point of time and the objectives of this audit is to test the design effectiveness of the controls.

One Personnel from the company end is designated as a point-of-contact who co-ordinate to collect the required evidence/documents from different-different departments and teams within the organization and share that with the Auditor. During the testing of the controls we observed that the company couldn't able to provide evidence for few controls requirements and those points came as an observation in the Type I report for which Management has given their plan of action to close those points. After that we successfully deliver the SOC 1 Type I report for payroll process to the company.

SOC 1 Type II Audit for Payroll Process

After Six months, the company called us for SOC1 audit and this time they asked SOC1 Type II report. The period of audit which was to be taken for Type II audit was of six months.

Soc1 Type II audit is the audit which focuses on company's internal controls over financial reporting over a period of time ranging from 6 months to 12 months.

Again all the steps were followed starting from a kick-off meeting for the complete business understanding and any changes in the process during this duration in the company and within various departments. We defined our testing procedures steps and sampled methodology to conduct the Type II report with more samples basis on the control activity frequency. Sampling is basically a simpler word is applying audit procedures to take less than 100% population size of

the data. Sampling contains high risk as the auditor's conclusion may differ if it is based on the entire population instead of a sample.

This time gain, we asked for personnel as a point-of-contact who co-ordinate to collect the required evidence/documents from different-different departments and teams within the organization and share with us. We shared the list of 'Document requirement list' with data populations details and other relevant evidence/documents as per the controls requirements. Once they shared the data Populations then we randomly select the samples as per the sample methodology and asked the relevant further evidences to conclude the testing of them. Now this time, the result of our testing was positive and we couldn't get a single control failure. After all the stages and testing, finally Type II audit report was handed over to the company after taking their signed Management Assertion and Management representation confirmation.