History of SOC reporting

This blog helps you understand the history and background of SOC reporting and a brief overview of how it came into existence and evolved as a way of addressing risks associated with outsourcing services.

Brief History

The increased prominence on governance, risk management, and compliance has steered companies to focus on internal controls over all aspects of their operations. Service organizations providing outsourced services (IT, business processes, etc.) often engage a third party audit firm to certify the design and operating effectiveness of these controls. The auditor's inspection of an organization's internal control and the impact that a service organization may have on the entity's control environment has long been an area of focus in designing an acceptable audit approach.

The original standard for attesting was known as SAS 70 and was an established way by which service organizations could illustrate the effectiveness of their internal controls. The SAS 70 audit was performed by a CPA and the result was a report on the effectiveness of internal control over financial reporting (ICFR). This report was often used by the organizations to show that a vendor was secure and safe to work with. However, the report was principally was not meant for that purpose.

Introduction of SSAE 16

The technology evolved and so did the AICPA's attestation standards. SSAE No. 16 reporting standards was completed by the AICPA in January 2010. SSAE 16 beneficially replaced SAS 70 as the reliable guidance for reporting on service organizations. SSAE 16 was officially issued in April 2010 and became effective on 15th June 2011. SSAE 16 was drafted with the objective and purpose of updating the US service organization reporting standard so that it reflects and adheres to the new international service organization reporting standard – ISAE 3402.

SSAE 16 also established a new attestation standard called AT 801 which contained guidance for performing the service auditor's examination. Many service organizations that had previously performed a SAS 70 examination now switched to the new standard in 2011 and now had an enhanced SSAE 16 report (also referred to as a Service Organization Controls (SOC) 1 report).

The upgraded SSAE 18

The SSAE no. 18 (Statement on standards of attestation engagements) used for SOC reporting is the latest periodic statement issued by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) effective from 1st May 2017. Following were the key changes in transforming from SSAE16 to SSAE18:

- SOC as defined under the SSAE-16 Standard stood for '***Service Organization Control***'. Under the new Standard, SOC now stands for '***System and Organizational Controls***', and applies to other types of organizations and both system and/or entity-level controls.

- In the SSAE-16 Standard, complementary user-entity controls (CUEC) were defined as those controls at user-entity organizations that were both necessary and unnecessary to achieve control objectives stated in management's description. Under the SSAE 18 Standard, CUEC are now defined as those controls that are only necessary to achieve control objectives stated in management's description.

- The new SSAE-18 Standard adds requirements related to subservice organizations (SSO) and vendor management processes. When subservice organization is carved out, the inclusion of SSO controls are now

provided in management's description similarly to CUECs. Also, vendor management processes to monitor the effectiveness of controls at SSO have been stressed upon.

- The new SSAE-18 Standard requires that the Management Assertion letter accepting responsibility for the description be signed. Previously, a Management Assertion letter was required but it did not have to be signed.

- The new SSAE-18 Standard has also included revisions to the language used in the Management Assertion Letter and Service Auditor's report to accommodate general changes and those associated with complementary user-entity and subservice organization controls.

The following table summarizes some of the Statements relative to internal control, the effect of information technology on a financial statement audit, and service organizations, that have been made since SAS No.70 standards introduced in 1992.

Statement Name	Date Issued	Title of Statement
SAS No. 70	April 1992	Service Organizations
SAS No. 78	December 1995	Consideration of Internal Control in a Financial Statement Audit: An Amendment to Statement on Auditing Standards No. 55
SAS No. 88	December 1999	Service Organizations and Reporting on Consistency
SAS No. 94	May 2001	The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit
PCAOB No. 2	March 2004	An Audit of Internal Control over Financial Reporting in Conjunction with an Audit of Financial Statements. (*Note: Appendix B refers to Service Organizations*)
PCAOB No. 5	May 2007	An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statements. *(Note: Appendix B17-B17 covers Service Organization considerations.)*
ISAE No. 3402	December 2009	Assurance Reports on Controls at a Service Organization
SSAE No. 16	April 2010	Reporting on Controls at a Service Organization
SSAE No. 18	May 2017	Concepts common to all Attestation engagements (with more stress on system details, CUEC (complimentary user organization controls) and SSO (sub-service organization) controls.)

Hope this blog would have added to your understanding the knowledge related to SOC reporting standards. Stay connected and feel free to reach out for knowing more about different types SOC reporting.