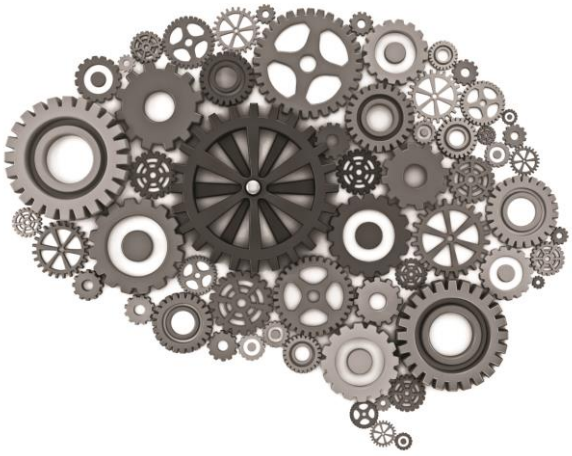
Service Organization Controls (SOC) Primer



AN OVERVIEW

As the demand for your company's services increase, so do the requests from your customers for assurance. *Assurance*, that you've taken the steps necessary to protect the privacy and confidentiality of their data as well as the security, availability and processing integrity of your systems. You are not alone. Looking to reduce infrastructure costs, many organizations are utilizing outsourcing and Cloud Computing solutions. Similarly, the demand for *assurance* of the integrity of these outsourced applications and functions has expanded as well.

As a service organization providing outsourced or cloud computing, you are an extension of your customers' system of internal control and your customers rely upon you to protect them from the risk of fraud, unauthorized use of data, loss of data and violation of privacy.

The American Institute of Certified Public Accountants (AICPA) has provided the solution to demonstrate the reliability of your system of controls and to provide *assurance* to your customers by providing three Service Organization Control (SOC) reporting options, SOC 1, SOC 2 and SOC 3.

SOC 1 reports address controls at a service organization that are likely to be relevant to an audit of a customer's financial statements.

SOC 2 and SOC 3 reports address controls at a service organization related to operations and compliance as identified in the AICPA's Trust Service Principles

By offering these three reporting options, the AICPA is providing a means to address your needs and the needs of your customers for *assurance* of your system of controls and their data.

SOC 1 Reports

SOC 1 Reports provide an opinion on controls at a service organization that are likely to be relevant to a user entity's Internal Control Over Financial Reporting (ICOFR). The financial reporting controls reported on are identified by the service provider. In efforts to align with international standards the AICPA issued SSAE 16 which replaced the superseded SAS 70.Thus a SOC 1 is a restricted use report under SSAE 16 intended for management of the service organization, customers and customer's auditors which replaces the SAS 70. There are two types of SOC 1 reports:

Type 1 provides a report on the service organization's description of its system, assertions regarding the description of the service organization's system, and the suitability of the design of the controls.

Type 2 expands on a Type 1 to report on tests of the operating effectiveness of controls and the results of the tests of operating effectiveness.

SOC 1 reports provide significant value to clients and internal management. These reports are a necessity for all service organizations that need to demonstrate well designed and effective controls to customers, in other words provide *assurance*. Organizations that previously utilized SAS70 reports will find the SOC 1 meets their needs.

Evolving Landscape

One of the challenges identified by the AICPA as they undertook the efforts to revise the auditing standards was that many services organizations were getting SAS 70 reports when the services they provided had little impact on ICOFR. For many cloud computing providers and other service organizations the standards did not address the risk areas that were really relevant to their customers. As a result the AICPA has issued standards that allow for the issuance of a SOC 2 and / or a SOC 3 report to address this gap.

SOC 2 Reports

SOC 2 Reports provide an opinion on controls at a service organization that are related to the AICPA's Trust Service Principles (TSP): (1) security; (2) availability; (3) processing integrity; (4) confidentiality; and 5) privacy. The focus of a SOC 2 report is on controls relevant to one or more of the TSP. Similar to SOC 1, there are two SOC 2 reporting types.

SOC 2 reports provide significant value in situations where clients and internal management must have confidence in the service organization's system of controls to provide security, confidentiality, processing integrity and privacy. In addition to addressing the internal needs the SOC 2 report is of value to your existing customers in demonstrating assurance in your systems and processes as evidences by a CPA signed report under robust standards.

Data centers and cloud computing providers among many others will find the SOC 2 report(s) provide the necessary level of *assurance* for clients and internal management.

SOC 3 Reports

The SOC 3 report is intended to be used as a marketing tool to an unrestricted expanded audience compared to that of a SOC 2 report, such as potential customers, investors, etc. Similar to a SOC 2 report the SOC 3 report provides an opinion on controls relevant to one or more of the TSPs. The SOC 3 report is unique in its lack of use restrictions and the use of a SOC 3 seal to be used on your website making it the perfect marketing tool for customers that must have confidence in the service organization's system of controls to provide security, confidentiality, processing integrity and privacy.

Sensiba San Filippo's Role

Sensiba San Filippo's *Business Process Assurance Group* can help you evaluate your needs and determine which SOC reporting option(s) will best serve your business and your clients.

Sensiba San Filippo is a leading regional accounting, tax and business-consulting firm focused on providing superior service and expertise to clients throughout Northern California. Our firm has the nimbleness of a boutique-consulting firm, the deep expertise based on over 35 years experience, and a sophisticated client service approach. Our firm includes 18 partners and approximately 120 additional professionals. We have six offices across the Bay Area to serve our clients including Pleasanton, San Mateo, San Jose, Morgan Hill, Oakland and San Francisco.

Our size gives us the nimbleness to deliver the highest quality of work, while giving our partners the time to cultivate and maintain personal relationships with our clients. As a matter of record, Sensiba San Filippo has one of the highest client retention rates, with an average of 92% of our clients remaining with our firm year over year.

For more information please contact one of our *Business Process Assurance Group* leaders below:

Jeff Stark, Audit Partner
jstark@ssfllp.com

Jeff works extensively with professionally managed venture-backed companies seeking to grow and ultimately be acquired or pursue an IPO path. He works with clients in enterprise software, cloud/SaaS, network equipment, internet security software, fab-less semi-conductor, development stage enterprises, healthcare, internet advertising, print media, market research, and communications.