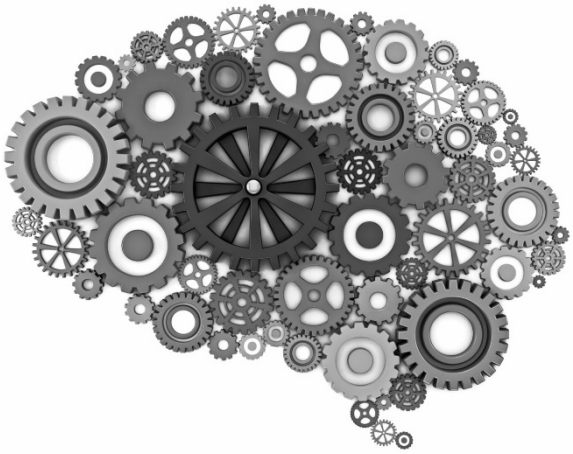
System & Organization Controls (SOC) Engagements



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 on you to protect them from the risk of fraud, unauthorized use of data, loss of data and violation of privacy.

To address this concern, the American Institute of Certified Public Accountants (AICPA) has provided three reports to demonstrate the reliability of your system of controls and to provide *assurance* to your customers. Previously known as "Service Organization Control," (SOC) the three reports are now known as System & Organizational Controls and include SOC 1, SOC 2 and SOC 3 report options.

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 Services Criteria.

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 In an effort to align with international standards, the AICPA issued SSAE 16 which replaced the superseded SAS 70.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 (now SSAE 18, as of 2017) intended for management of the service organization, customers and customer's auditors.

SOC 1 reports provide significant value to clients and internal management. These reports are necessary for all service organizations that need to demonstrate well designed and effective controls to customers. Organizations that previously utilized SAS70 reports will find that a 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 data centers, 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 Services Criteria (TSC): (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 TSC categories.

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 existing customers in demonstrating assurance in the systems and processes as evidenced 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 TSC categories. The SOC 3 report is unique in its lack of use restrictions and the use of a SOC 3 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.

Reporting Options

There are two types of SOC 1 and SOC 2 reports:

Type I 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. This type of report is as of a specified date.

Type II expands on a Type 1 to report on tests of the operating effectiveness of controls and the results of the tests of operating effectiveness. The report covers a period of time, most often 6 months or 1 year.

Many times clients will begin with an initial engagement as a Type I and then follow up with recurring Type II engagements as they go.

SENSIBA SAN FILIPPO READINESS ASSESSMENT

SSF can perform services to assess our client's readiness to undergo a successful SOC 1, 2 or 3 assurance engagement.

During the assessment, SSF's team will:

- Meet with appropriate members of management / customers / vendors to determine existing environment
- Review existing documentation and perform procedures necessary to determine consistency of documentation with actual operating environment
- Provide a report of findings specifying recommendations and a project implementation plan for compliance with SOC requirements
- Provide a budget and fee schedule for all elements identified in the SOC project implementation plan and recommended time-line

ABOUT SENSIBA SAN FILIPPO

Sensiba San Filippo is a leading regional audit, tax and business-consulting firm focused on providing expertise to clients throughout Northern California and the Silicon Valley. Our firm includes 22 partners and principals and approximately 140 additional professionals. We have six offices to serve our clients, including Pleasanton, San Mateo, San Jose, Morgan Hill, Fresno 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.

For more information on SOC Assurance offerings please contact:

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 leads the firms technology practice and works with clients across various industries often his clients are startup, venture backed high growth clients. Jeff is also responsible for the firms service offerings related to audit and assurance services including SOC engagements.

Ramil Cortez, Senior Manager
rcortez@ssfllp.com

With over 25 years of information and technology experience Senior Manager, Ramil Cortez, specializes in information risk management and assurance advisory services. He works with clients in enterprise software, cloud/SaaS, network equipment, internet security software, manufacturing and technology industries. Ramil has in-depth knowledge of large ERPs and was one of the first auditors to perform a SAS 70. He works closely with clients on IT controls review, business processes re-engineering and process improvement. He is a certified SAP R/3 HR consultant and has extensive experience in SAP R/3 project management and implementation support.

Brian Beal, Manager
bbeal@ssfllp.com

With over 14 years of information and technology experience Manager, Brian Beal, specializes in information risk management and assurance services. He works with clients in enterprise software, cloud/SaaS, network equipment, internet security software, manufacturing and technology industries. As a past web developer and information security officer, Brian has in-depth understanding of development cycles, implementation cycles, disaster recovery plans, and implementing security policies. With this unique skill set, he assists his clients in assessing security and risk from all angles.