CEP Magazine - December 2022

Wesley Van Zyl (wesley@scytale.ai) is a Compliance Success Manager for Scytale in Johannesburg, Gauteng, South Africa.

Beginner's guide to SOC 2, Part 1

By Wesley Van Zyl

The reason we have auditors today is simply because people do not trust one another. Let's say financial statements reveal $1 million in net profit. If you are a shareholder, do you believe this? Is it less, or is it more? Do we trust the chief financial officer?

So, if an organization uses a Software as a Service (SaaS) provider or outsources elements of IT, the organization (being the client) would often raise the concern, "Is our information secure?" This is often followed by a more difficult question, "How do you know?"

SaaS and IaaS (Infrastructure as a Service) or cloud solutions have matured over the years. Economic conditions have resulted in many organizations seeking to increase efficiencies and decrease costs through outsourcing some of their services. So, the above two questions require answers, and if an organization is competing on a global scale or has plans to grow into a global competitor, these questions will need to be answered from a compliance point of view.

Why do you need a SOC 2 report?

SOC 2 compliance has increasingly become a "must-have" for organizations. Organizations may be more familiar with the SOC 1 report (also called ISAE 3402, SSAE 16, or formerly SAS 70). This is a report on controls that impact the user entity's internal controls over financial reporting and are typically used in support of the audit of a client's financial statements. The SOC 2 report, however, follows the same approach but is focused on the controls over IT or more, specific, controls over the SaaS or IaaS.[1]

The SOC 2 reporting standard is an audit opinion report over internal controls related to information technology. It is based on the AICPA's Trust Service Principles of security, availability, process integrity, confidentiality, and privacy.[2]

It is key to note that the organization cannot outsource the risks around IT. The organization should protect the information of their business and customers, even when using a service organization. A SOC 2 report will assist by assuring the controls are in place at the service organization. The organization may want to make a positive SOC 2 report part of the contractual agreement between their organization and the service organization, demonstrating information security compliance.

The benefits of a SOC 2 audit include:

- An edge over competitors, as demonstrating an official SOC 2 report confirms just how serious an organization is about protecting customer data and the security of its systems and procedures.

- An organization can break into new markets, especially with United States customers, as SOC 2 is highly recognized in this region.
- The service organization can undergo one audit and distribute the report to multiple customers, reducing the time spent with individual auditors.
- The Trust Service Principles relate directly to the core service obligations and commitments of IT, cloud, and hosting providers, including SaaS services.
- Staff throughout the service organization gain improved insight into risk, governance, and internal control.
- Independent assurance over the controls operated by third-party service organizations.
- A comprehensive report of the processes and controls in place at the service organization.
- Clearly articulated controls that need to be performed by your organization when working with the service organization.
- Insight into control gaps as highlighted in the report or rather areas of improvement.

You are probably thinking to yourself now, "How do we do it?" There are a lot of stages in a SOC 2 process, but they can generally be broken down into the following six steps:

1. Consider finding a SOC 2 consultant or partner
2. Identify your scope
3. Perform the gap analysis
4. Gather evidence for each control
5. Perform the audit
6. Review the SOC 2 report