GILLIAM SECURITY

# SOC 2: Why Should I Care?

***Offering the third opinion of your information security state to your stakeholders.***

Often times an organization is asked “Do you have a SOC 2?” when one wants to find out about an organization’s information security state; however, do we know what benefit that really provides?

A SOC 2 Report is a report that helps prospective customers, current and future auditors, investors, and company stakeholders understand the controls that an organization has in place. All reports are not alike, however, in that the report may include security controls as well as some of the following areas:

- Confidentiality;
- Processing Integrity;
- Data Privacy; and,
- Availability.

It is important to read the report in detail as the only required area to cover is security controls and not any of the areas in the bulleted list above. Secondly, each area may have an *exception*. An exception on a SOC report is defined as “any instance where a control was not designed appropriately or did not operate as intended,” according to DRATA.com.

An example of this can include the failure of performing a background check of an employee during onboarding. It is important to understand that an auditor performs sample testing of the population in which the control was in place during the reporting period.

Layman’s terms: If you onboarded 100,000 people and 1,000 random records were sampled showing every person onboarded had a background check but the 1,001 record on the list did not, no exception would be noted.

Next, it is important to note the scope of the document. The scope of the document relates to the area that was subject to the audit. For example, a company called *ACME Widgets* may use Microsoft Teams Online, AWS for hosting its website and an on-premise PeopleSoft DB2 instance for inventory management; however, the scope of the report may only cover the PeopleSoft DB2 instance with a carve-out for the Microsoft environment and the AWS environment. In the case of a carve-out audit, the only controls that would be tested as part of the SOC Report would be the PeopleSoft DB2 instance.

Last, one must understand if the SOC 2 report is a Type I or Type II. A SOC 2 Type I audits with the design of the controls, as it reflects a moment in time. A SOC 2 Type II audits the design and testing of the controls, as it covers a period of time.

Need help understanding a SOC 2 report or preparing for a SOC 2 audit? Reach out to Gilliam Security and we would be glad to help. Our team of experts has built teams in organizations that have been through SOC 2 audits and would be glad to help your organization.

*Why Gilliam Security?*

*Gilliam Security has recognized consultants from major fortune 500 companies with certifications such as the CISSP, CISM, CISA and CRSIC. Each consultant also has experience in building the information security, as well as privacy, function from inception to maintaining operations.*

*Contact Us Today at sales@gilliamsecurity.com*