SOC 2 Type 2 Security FAQs

Guardian Research Network (GRN) is proud to have successfully completed the SOC 2 Type 2 Attestation for Security. Below are questions and answers that address this popular form of cybersecurity audit.

What is SOC 2?

An audit that evaluates the controls an organization has in place to protect and secure systems and services. System & Organization Controls (SOC) is a component of the American Institute of CPAs System & Organization Control reporting platform.

Why is SOC 2 important?

Its goal is to make sure systems are set up to assure security, availability, processing integrity, confidentiality, and privacy of data.

Who certifies SOC 2?

An unbiased third-party audit firm—in GRN's case A-LIGN—who is a member of the American Institute of CPAs. This firm verifies strict adherence to the strongest data security controls, providing strong protection for critical data and IT systems.

What does SOC 2 require?

It requires development and use of security policies and procedures, written and followed. Compliance verifies processes and practices that guarantee oversight across the organization, specifically, IT monitoring for any unusual, unauthorized, or suspicious activity—both known malicious activity (a phishing scheme or obviously inappropriate access) and unknown malicious activity (a zero-day threat or a new type of misuse).

SOC 2 Basics

Compliance satisfies the five SOC Trust Services Criteria

What does SOC 2 completion mean?

This audit attests to both the design and operating effectiveness of security controls over a period of time, typically 3 to12 months. A SOC 2 audit provides assurance of both how systems are set up and how they are used on a daily basis. SOC 2 Type 2 confirmation generally provides a greater level of trust to a customer or business partner due to the increased visibility of systems as it relates to the organization's IT system as a whole and a detailed descriptions of the auditor's tests and test results of the controls.

Who should have SOC 2 verification?

SOC 2 applies to any organization that processes or manages data in the cloud or in data centers and wants to demonstrate a commitment to security. Although the audit is purely voluntary, those who should be verified include technology-based service organizations that store customer data. That means it applies to pretty much every SaaS company and any company that stores a customers' information.

What is the difference between SOC 1, SOC 2, and SOC 3?

There are three types of SOC audits: SOC 1, SOC 2, and SOC 3. When it comes to cybersecurity, SOC 2 has become the standard. The difference between SOC 1 and Soc 2 is that the SOC 2 report addresses a service organization's controls relevant to operations and compliance. A SOC 3 report is a summary of the SOC 2 report with less technical information, making it suitable for an organization to share publicly on its website or to hand out to prospective customers.

How long is SOC 2 applicable?

It should be renewed approximately every 12 months.

Is the SOC2 Type 2 report available?

Yes, please reach out to info@guardianresearch.org to request your copy.

"We're proud to have obtained our SOC 2 Type 2 attestation, for GRN and for our consortium members who provide data that must be handled with the utmost dedication to safety. It ensures GRN systems and processes protect the ongoing healthcare data our members entrust to us."

Bryan N. Ard, Chief Information Security Officer at GRN

Guardian Research Network®