

Redpoint Global

---



# SOC 3 Compliance

Assurance on  
Your Service  
Organization's  
Controls

---

January 2022

# Table of Contents

- What is a SCOC 3 Report?
- Purpose and Use
- AICPA Trust Services Principles
- Who Needs a SOC 3 Report?



# What is a SOC 3 Report?

- A System and Organization Control (SOC) 3 report focuses on internal controls as they relate to the AICPA's five Trust Service Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. SOC 3 is similar to the SOC 2 report, however, the difference lies in the details provided in each report. The SOC 3 report is shorter and does not contain the detailed controls and testing procedures. This report is designed for organizations that do not possess the need for or the knowledge necessary to make use of the comprehensive details contained in a SOC 2 report.
- Because SOC 3 reports are considered to be general use reports, there is the option to distribute the report for marketing purposes, such as posting it to your website.



# Purpose and Use

- The SOC 3 report is designed for users who want assurance on a service organization's controls, but do not have the need for the detailed, comprehensive SOC 2 report.
- Essentially a smaller scale SOC 2 report, the SOC 3 is easy-to-read and can be viewed by anyone (general use).



# AICPA Trust Services Principles

Like SOC 2, a SOC 3 reports on if the service organization achieved one or more of the five AICPA Trust Services Criteria, which include:

- 1. Security** – The system is protected against unauthorized physical and logical access
- 2. Availability** – The system is available for operation and used as agreed upon
- 3. Processing Integrity** – System processing is complete, accurate, timely and authorized
- 4. Confidentiality** – Information designated as confidential is protected as agreed upon
- 5. Privacy** – Personal information is collected, used, retained, disclosed, and/or destroyed in accordance with established standards

Because of the lack of detail in a SOC 3 report, the audit must be a Type 2 report



# Who Needs a SOC 3 Report?

- Organizations that should consider a SOC 3 report include Cloud Service Providers (e.g., SaaS, IaaS, PaaS), enterprise systems housing third party data, IT systems management, and data center colocation facilities.  
If you want to communicate your organization's controls are properly designed, implemented and operating effectively, but do not want to reveal the details of controls, then the SOC 3 report may be right for you.



