[Company Name] Has Announced Our Latest SOC 2 and SOC 3 Reports. Here's What That Means For You.

[COMPANY NAME] recently received our latest SOC 2 and SOC 3 reports. But what do these reports mean for us as an organization—and for you as our customer?

At [COMPANY NAME], keeping customer and stakeholder data secure is our top priority. To ensure that our systems and controls have been designed appropriately to achieve that goal, we sought out third-party attestation from a qualified auditing firm. Our SOC 2 and SOC 3 reports are the result of their examination.

In this blog post, we'll explain what these reports are, what they cover, and why we chose to undergo this rigorous compliance audit.

WHAT IS A SOC 2 REPORT?

Obtaining a System and Organization Controls (SOC) 2 report is one way for a service organization to attest to the security of its digital environment.

Completing a SOC 2 examination through an accredited third-party auditor does not result in any certification. Instead, the resulting CPA's report functions as a tool to help an organization communicate whether the internal controls they've put in place governing the security of customers', partners', and stakeholders' data are properly designed, implemented, and maintained.

In simpler terms, a SOC 2 report provides an avenue for current and potential stakeholders to assess risk by giving them a closer look at the policies and procedures put in place to ensure the organization's services are provided safely and reliably.

WHAT IS A SOC 3 REPORT?

A SOC 3 report is similar in scope to a SOC 2 report, but the information is packaged more concisely. This makes SOC 3 reports easier to read and a better fit for widespread distribution.

Both reports result from the same audit, and both can help communicate that an organization's controls are properly designed and implemented and operating effectively.

WHAT DO THESE REPORTS COVER?

SOC reports result from an examination performed by an accredited CPA firm under the standards defined by SSAE 18. An auditor tests the effectiveness of the internal controls outlined by the organization, then maps those controls to one or a combination of Trust Services Criteria established by the [American Institute of Certified Public Accountants (AICPA)](#).

In our case, [that criterion includes/those criteria include]:

- **Security**: The system is protected against unauthorized access (both physical and logical).
- **Availability**: The system is available for operation and use as committed or agreed.
- **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Confidentiality**: Information designated as confidential is protected as committed or agreed.
- **Privacy:** Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

The scope of a SOC report can also vary with regard to the time period covered. SOC 2 Type II reports examine controls over a period of time, usually between three and 12 months, and include both a list of the controls tested as well as the auditor's test results.

The reporting period for [COMPANY NAME]'s latest SOC 2 and SOC 3 reports spanned from [DATE] to [DATE].

WHY DID WE UNDERGO THIS EXAM?

Receiving our SOC 2 and SOC 3 reports marks a huge step forward in [COMPANY NAME]'s efforts to demonstrate our commitment to data security and ensure that we're prepared to face the challenges of the ever-changing cybersecurity landscape.

"We are pleased that our SOC 2 and SOC 3 reports have shown we have the appropriate controls in place to mitigate risks related to [INSERT APPLICABLE TRUST SERVICES CRITERIA]," said [COMPANY REPRESENTATIVE NAME AND TITLE]. "[INSERT EXPLANATION OF WHY RELEVANT PRINCIPLES ARE IMPORTANT TO YOUR ORGANIZATION]."

WHERE CAN I GO FOR MORE INFORMATION?

Our auditing partner, BARR Advisory, has provided a comprehensive overview of the different types of SOC examinations and their unique requirements for cloud service organizations.

Current and prospective customers interested in obtaining a copy of [COMPANY NAME]'s latest SOC 2 Type II or SOC 3 reports may contact [NAME] at [PHONE/EMAIL].