WHITEPAPER

Understanding the Importance of SOC 2 Certification

segura® | Futureproof Identity Security | segura.security

Introduction

SOC 2 Certification is critical to ensuring an organization's security and compliance. It increases competitiveness, as customers prefer to work with secure and reliable providers. Moreover, the SOC 2 criteria make it easier to obtain other important certifications, such as ISO 27001 and HIPAA. This certification offers numerous advantages to organizations.

With increasing digitalization, information security is increasingly important for companies of all sizes and industries, including those that rely on specialized providers to conduct their core operations. Lack of proper data protection can expose a company to risks such as malware attacks, extortion, and information theft.

SOC 2 is an auditing standard that ensures the secure management of data by service providers, preserving the privacy of customers and protecting the interests of the company.

This whitepaper will provide more detailed insights into what SOC 2 is, its principles and benefits, and other relevant information on the subject. Keep reading to get a complete understanding.

What Is SOC 2 Certification

SOC 2 is a cybersecurity compliance framework created by the American Institute of Certified Public Accountants (AICPA) to ensure the secure storage and processing of data by third-party providers. This framework defines requirements to maintain high data security standards based on the following principles:

- Security
- Privacy
- Availability
- Confidentiality
- Processing Integrity

Not all countries adopt SOC 2 as a way to validate that a corporation securely stores and processes data, but with user privacy becoming a global priority, this trend should be reversed in the coming years.

In any case, it is important to know there are three different SOC audit reports (SOC 1, SOC 2, and SOC 3) and, within each of them, two types.

SOC Audit Reports

As we have already mentioned, there are three different SOC audit reports. These are:

- **SOC 1:** It examines an organization's financial reports.
- **SOC 2:** It evaluates how well a company commits to internal controls associated with one or more of the AICPA's Trust Service Criteria — Availability, Security, Processing Integrity, Confidentiality, and Privacy.
- **SOC 3:** It is a new approach to SOC 2, interpreted with an aim at wide distribution, in order to be comprehensible to the public.

SOC 1 and SOC 2 audit reports can also be of Types I and II. In Type I, the controls are evaluated case by case and, in Type II, the efficiency of these controls is analyzed within a certain period, which can be from six months to one year.

In turn, the SOC 3 audit report is based on the results of a Type II SOC 2 assessment.

The SOC 2 Type II report is the most solid among all these alternatives. Thus, a Type II SOC 2 audit guarantees organizations validation before an external auditor on the adequacy and effectiveness of their data controls, covering aspects such as:

- Logical and Physical Access Controls
- System Operations
- Change Management
- Risk Mitigation

The 5 Principles of SOC 2

The American Institute of Certified Public Accountants defines SOC 2 as a framework that service providers should use to audit and report on how their management of sensitive data works. In practice, SOC 2 refers to a set of standards and guidelines that describe how an organization should ensure five principles, or trust criteria. Companies define the certification scope based on the selection of principles, having the obligation to the security principle.

Here are the five principles:

Principle 1 — Security

In a Zero Trust approach, it is necessary to authenticate and authorize human and machine users without exception. SOC 2's security principle encompasses application security design and how sensitive information, including intellectual property, financial data, and personally identifiable information (PII), is controlled and protected. In this approach, SOC 2 validates access controls, the use of Multi-Factor Authentication (MFA) and intrusion detection, and threat protection.

Principle 2 — Availability

Users expect that services made available in the cloud can be used at any time. In this way, the availability principle analyzes whether service providers are able to maintain availability, monitoring performance along with processes necessary to respond to security incidents.

The Zero Trust security principle requires monitoring capabilities that enable companies to quickly analyze

and identify threats by responding to security incidents appropriately.

Principle 3 — Processing Integrity

This principle focuses on how data is processed. Quality and monitoring controls enable companies to validate the security of data storage, delivery, modification, and retention processes.

However, to deal with the controls that ensure the protectio n of customer data, the organization must prepare for this.

This preparation is an essential aspect of the Zero Trust approach, as it allows the company to remain ready to detect and respond to threats, before malicious agents obtain privileges that, consequently, cause great damage.

Principle 4 — Confidentiality

Confidentiality is indispensable, especially in the case of distributed SaaS systems. Organizations need to ensure their data classified as confidential or sensitive is effectively protected from improper access. SOC 2 validates the form of protection through access controls, data encryption, and firewalls.

In the Zero Trust approach, security solutions validate individual identities, protecting access to critical environments. For this, one must authenticate this identity accurately, authorize it, and allow its access, restricting the privilege over the assets considered confidential and being able to audit at any time. In this way, they provide transparency on compliance with security policies and, in turn, the process.

Principle 5 — Privacy

The privacy principle analyzes how the application or service processes information provided or generated by an individual, based on the data policy from AICPA's Generally Accepted Privacy Principles (GAPP).

Thus, proper access controls should be adopted in order to avoid undue access and privileges. For this, it is imperative to verify users, validate devices, and limit privileged access through a Zero Trust approach.

Benefits of SOC 2 Compliance

Here are some benefits of having SOC 2 certification

SOC 2 compliance proves your company has taken all necessary measures to prevent data breaches and improve its reputation in the market, in addition to gaining the trust of its customers.

This certification can also give you a competitive advantage over other organizations from the same industry, as many customers prefer providers that are secure and able to prevent data breaches, and SOC 2 compliance is a way to demonstrate your company's security.

Having a SOC 2 report can also be a marketing advantage for your company, since many competing companies do not have this certification to prove their security.

Adopting best practices in security and operational efficiency, which allow you to obtain SOC 2 certification, can optimize your organization's processes and controls, based on knowledge of the digital security risks faced by your customers.

The criteria of SOC 2 facilitate the process of obtaining ISO 27001 and HIPAA, as they are complementary structures.

Complying with SOC 2 demonstrates your ability to protect your customers' cybersecurity by preventing breaches and preserving their privileged data, as well as evidencing your commitment to overall IT security and your compliance with industry best practices.

SOC 2 certification ensures the effectiveness of the control and information security environment, as the audit criteria for SOC 2 Type II require proof of the operational effectiveness of controls in place for at least six months.

A SOC 2 report provides valuable information about the risks faced by your company and its security posture, including aspects such as supplier management, internal controls, governance, and regulatory oversight, among others.

The Importance of SOC 2 Certification for Segura®

We, from Segura®, seek to work following the best security practices in the market. That's why we achieved SOC 2 Type II certification in 2022 for SaaS 360o, our cloud solution.

The analysis for SOC 2 compliance was performed between June 1 and November 30, 2022, using information about the system controls that Segura® has designed. This assessment was based on relevant trust service criteria for security, availability, processing integrity, confidentiality, and privacy — requirements established by AICPA.

The SOC 2 report detailed the following aspects:

- The nature of the services provided by the company
- How the company's system interacts with users, business partners, service providers, and other parties
- Internal controls and their limitations
- Complementary user and company controls, including how these controls work together with company controls to achieve service commitments and system requirements
- User responsibilities and how they may affect their ability to effectively use the company's services
- Applicable service confidence criteria
- Risks that threaten compliance with the company's service commitments and system requirements, and how controls address these risks

Conclusion

In this whitepaper, we explained what SOC 2 is and the assessment performed during an audit and addressed its importance for third-party suppliers and customers. We have also shown that Segura® recently achieved this certification, which guarantees the operation is following the reliability criteria, translated into policies and daily life, conveying confidence to its public.

WHITEPAPER

Understanding the Importance of SOC 2 Certification

segura® | Futureproof Identity Security | segura.security