NOVEMBER 1, 2022

SOC1 / SOC2: A BRIEF INTRODUCTION TO DATA SECURITY

WHITE PAPER BY AUUDITR

Introduction

Modern world is standing on data, and information is created and processed daily. Businesses and services work on building clients' trust and their ability to prove that they are worthy of that trust. Organizations must perform regular compliance checks and work on non-conforming issues to achieve complete confidence in their processes for better performance. System and Organization Controls (SOC) is a well-known standard for data security, especially in North America. This standard analyzes, detects, prevents, and responds to cybersecurity incidents.

Moving forward, we are discussing more related to the standard, its main content, and what Auuditr offers to help you achieve compliance

.

"Businesses and services work on the building of clients' trust and their ability to prove that they are worthy of that trust."

Keywords: SOC, SOC 1, SOC 2, AICPA, Cybersecurity, Information Security, Auuditr, Confidentiality, Security, Privacy, Integrity

Context

SOC1 / SOC2 standards are similar to ISO 27001 in data security but comparatively less stringent. ISO 27001 focuses on creating an Information Security Management System or ISMS, while SOC1 / SOC2 standards focus on the implementation and regular monitoring to upkeep cybersecurity. The primary function is to detect vulnerabilities and investigate and respond to threats efficiently to avoid data breaches and security issues. SOC1 / SOC2 standards work on the hub-and-spoke model, where the standard's hub is cybersecurity and the prevention of data breaches. Following security measures can be taken to keep up with the hub:

1- Vulnerabilities Assessments
2- Database and applications scanners
3- Intrusion Prevention Systems
4- User and Entity Behavior Analytics
5- Endpoint Detection and Remediation
6- Threat Intelligence platforms

The primary goal of SOC1 / SOC2 is to find any blind spots within the current systems to avoid the cause of breaches. As other standards work on strengthening overall security with different levels of hurdles in the way, SOC works with finding the exploitable points within the security framework.

SOC1 / SOC2 works on the following major principles:

- Security
- Privacy
- Confidentiality
- Integrity

The security framework is analyzed using SOC Reports. Typically there are 2 types of SOC Reports. Type 1 describes the trust level of the vendor's systems. Type 2 gives the details of the effectiveness of the operations of those systems. SOC1 / SOC2 reports are further explained in the upcoming section.

SOC Reporting and contents

"A SOC 1 report is usually demanded by the companies from their vendors, so they know where they stand in terms of the risk and controls."

SOC Reporting depends upon the type of organizations going for compliance. Different kinds of companies go for types of reporting that suit their service the best. Service providers such as software houses that sell financial software related to payroll, income, and expenditure and provide such data reports dealing with sensitive information must provide their clients with a report ensuring the trust in their security controls. SOC reporting is divided into SOC 1, SOC 2, and sometimes SOC 3 when an integrated report is required.

- A SOC 1 report focuses on the third-party services that impact the company's financial reporting. The companies usually demand a SOC 1 report from their vendors so they know where they stand regarding risk and controls. *Service providers include IT infrastructure providers, payroll software, recordkeepers, cloud services, etc.*
- A SOC 2 report gives complete oversight of an organization. This report aims to address one or more of the basic trust services principles of AIPCA. SOC 2 reports are usually for businesses with elaborated customer relationships and digital services.

SOC 2 reports are more complicated, and compliance depends upon the following controls:

- Physical and logical access controls
- System operations for the detection of unusual procedures
- Change Management to prevent unauthorized changes to the system
- Risk management to identify risks and mitigation activities

AICPA, the founder body of the SOC1 / SOC2 controls, has the following trust criteria:

- Availability of the services and accessibility that the service user can rely on.
- Integrity is about delivering the correct data available on time and accurately.
- Confidentiality focuses on restricting access according to the level of the information needed by different entities.
- The Privacy principle is about being able to keep the information always contained.

Services Offered by Auuditr

As a consultancy firm, we offer our team the expertise to help you with SOC1 / SOC2 compliance. We provide the following services:

- A readiness assessment

- SOC Reports
- Consultancy sessions

Auuditr will help you understand what type of report is the most suitable for you and will monitor the progress along with you. The complete end-to-end solution with a detailed roadmap of compliance is our goal.

Further information on

www.Auuditr.com