SOC 2 Type 2 - Overview

In One Sentence

Generally, the SOC 2 Type 2 certification process can take between 6-12 months to complete and is typically between $20,000 to $80,000 or more.

Certification Letter / Attestation

Attestation report.

Description

SOC 2 (Service Organization Control 2) Type 2 is a report that provides assurance about the controls and processes of a service organization related to security, availability, processing integrity, confidentiality, and privacy. The SOC 2 Type 2 report is based on the Trust Services Criteria, which are a set of principles and criteria developed by the American Institute of Certified Public Accountants (AICPA).

The SOC 2 Type 2 report evaluates the effectiveness of the controls and processes over a period of time (usually 6 to 12 months). It is considered more comprehensive than the SOC 2 Type 1 report, which evaluates the design of the controls and processes at a specific point in time.

The SOC 2 Type 2 report provides valuable information for customers and stakeholders of service organizations. It demonstrates the service organization's commitment to security, availability, processing integrity, confidentiality, and privacy and provides assurance that the controls and processes are operating effectively over a period of time.

Benefits

When an organization completes a SOC 2 (Service Organization Control 2) Type 2 certification, it receives several benefits, including:

Increased trust and credibility

SOC 2 Type 2 certification is recognized as a trusted standard for evaluating an organization's control environment. By undergoing the certification, the organization demonstrates its commitment to information security and establishes credibility with customers, partners, and other stakeholders.

Enhanced risk management

SOC 2 Type 2 certification provides an independent evaluation of the organization's control environment over a period of time (usually six months to one year), which can help identify potential risks and vulnerabilities. By addressing these risks, the organization can enhance its risk management practices and better protect its systems and data.

Improved operational efficiency

SOC 2 Type 2 certification can help the organization streamline its operations by identifying and addressing inefficiencies in its control environment. This can lead to improved processes, better resource utilization, and reduced costs.

Regulatory compliance

SOC 2 Type 2 certification can help the organization meet regulatory compliance requirements, such as those set by HIPAA, PCI DSS, and other frameworks.

Third-party assurance

SOC 2 Type 2 certification provides third-party assurance to customers and stakeholders that the organization's control environment meets the Trust Services Criteria over a period of time. This can help the organization build and maintain relationships with its customers and partners.

Overall, completing a SOC 2 Type 2 certification can provide several benefits to the organization, including increased trust and credibility, enhanced risk management, improved operational efficiency, regulatory compliance, and third-party assurance.

Certification Process

The certification process for SOC 2 (Service Organization Control 2) Type 2 certification is similar to that of SOC 2 Type 1 certification, but with some additional requirements. The SOC 2 Type 2 certification process typically involves the following steps:

Define the scope

The organization and the auditor agree on the scope of the SOC 2 Type 2 audit, which includes the systems and services that are in scope for the audit.

Identify the Trust Services Criteria (TSC)

The organization and the auditor identify the applicable Trust Services Criteria (TSC) that will be evaluated during the audit. The TSCs are principles and criteria established by the AICPA that form the basis of the SOC 2 audit.

Conduct a readiness assessment

The organization may conduct a readiness assessment to identify potential gaps in its control environment and make necessary improvements before the SOC 2 Type 2 audit.

Perform the audit

The auditor performs the SOC 2 Type 2 audit over a period of time (usually six months to one year), which includes evaluating the organization's control environment against the applicable TSCs, testing the controls, and reviewing supporting documentation.

Issue the SOC 2 Type 2 report

The auditor issues a SOC 2 Type 2 report that includes an opinion on the organization's control environment and the effectiveness of its controls over the period of the audit. The report also includes a description of the organization's systems and services, the scope of the audit, and the auditor's testing procedures and results.

Maintain compliance

The organization must maintain its control environment and continue to meet the Trust Services Criteria to remain compliant with SOC 2 Type 2 certification.

Overall, the SOC 2 Type 2 certification process involves a rigorous audit of an organization's control environment over a period of time, with the goal of providing third-party assurance to customers and stakeholders that the organization has implemented effective controls to protect its systems and data.

Estimated Costs

A fair estimated price range for a SOC 2 Type 2 assessment is typically between $20,000 to $80,000 or more. Cost will vary depending on the factors below.

The estimated costs for obtaining a SOC 2 Type 2 report can vary widely depending on several factors, such as the size and complexity of the service organization, the scope of the audit, and the chosen auditor or firm. Generally, the costs for obtaining a SOC 2 Type 2 report can range from tens of thousands to hundreds of thousands of dollars, depending on the above factors. Some of the costs that may be involved in the SOC 2 Type 2 process include:

Preparation costs

These are the costs associated with preparing for the SOC 2 Type 2 audit, including identifying the scope of the audit, assessing risks and controls, and creating documentation.

Audit fees

These are the fees charged by the auditor or audit firm to conduct the SOC 2 Type 2 examination and issue the report.

Remediation costs

These are the costs associated with addressing any identified control deficiencies or weaknesses and implementing changes or improvements to the controls and processes.

Ongoing costs

These are the costs associated with maintaining the controls and processes and conducting periodic assessments to ensure ongoing compliance with the Trust Services Criteria.

It's important to note that the costs for obtaining a SOC 2 Type 2 report can be significant, but the benefits of obtaining the report can outweigh the costs in terms of increased customer trust and confidence, improved security and compliance posture, and competitive advantage.

Dependent on auditor not less than 20K.

Duration Of Certification Process

Typically, the SOC 2 Type 2 audit process takes between 6 to 12 months, including the preparation and remediation periods. However, the duration of the audit can be shorter or longer depending on the above factors.

The SOC 2 Type 2 audit process generally involves the following phases:

1. Planning and scoping

This phase involves defining the scope of the audit, identifying the Trust Services Criteria that will be evaluated, and assessing the risks and controls.

2. Testing and documentation

This phase involves the testing of the controls and processes to ensure they are operating effectively and in accordance with the Trust Services Criteria. It also involves documenting the evidence gathered during the testing process.

3. Reporting

This phase involves the auditor issuing the SOC 2 Type 2 report, which includes the auditor's opinion on the effectiveness of the controls and processes.

4. Remediation

This phase involves addressing any identified control deficiencies or weaknesses and implementing changes or improvements to the controls and processes.

The duration of each phase can vary depending on the complexity of the service organization and the scope of the audit. It's important to work closely with the auditor to ensure a smooth and efficient audit process.

6-12 months, mid-sized companies should expect a team of 3 employees to spend 3-5 hours per week each for six months to be ready for their first audit.

Lifecycle Of Accreditation

A SOC 2 Type 2 report covers a specified period of time, typically between 6 and 12 months, during which a service organization's controls are evaluated for design effectiveness and operating effectiveness. The report is issued at the end of the evaluation period and is current as of that date.

A SOC 2 Type 2 certificate does not have an expiration date. However, it is important to note that the certification is only valid for the specific period of time covered by the report. Once that period has elapsed, the service organization will need to undergo another SOC 2 Type 2 audit and obtain a new report in order to maintain the certification.

Links / Additional Information

Here are some resources that can provide more information about SOC 2 Type 2 audits:

- American Institute of Certified Public Accountants (AICPA) SOC 2 Guide: https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/2017october11aicpasoc2guide.pdf
- AICPA SOC 2 Overview: https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/2019-may-28-soc-2-overview.pdf

- SOC 2 Type 2 Criteria: https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/soc-2-trust-services-criteria.pdf
- SOC 2 Type 2 Compliance Checklist: https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/soc-2-type-2-checklist.pdf
- SOC 2 Type 2 Compliance Guide: https://www.upguard.com/blog/soc-2-type-2-complianceguide
- SOC 2 Type 2 Compliance: The Ultimate Guide: https://www.pivotpointsecurity.com/blog/soc-2-type-2-compliance-ultimate-guide/
- How to get a SOC 2 certification: A comprehensive guide. https://fractionalciso.com/soc-2-certification/