How To Get SOC 2 Type 2 Without Slowing Down Your SaaS

Table of Contents

1. What is SOC 2 Type 2?

Figure 1: 'Service' SEO Test Image

Employing third-party service companies to handle certain business functions is commonplace in the commercial world as no organization can do it all. It almost always makes commercial sense for businesses, or 'user entities' in this context, to delegate tasks outside their speciality to companies that can execute them with expertise and efficiency. This strategy allows the delegating company to focus its resources on its primary business function, making it easier to reduce costs and operate optimally. However, it is paramount to assess these service organizations to ensure they uphold and maintain reasonable standards of operation that guarantee quality service delivery.

a. The Service Organization Control (SOC) Report Framework

The American Institute of Certified Public Accountants (AICPA), at the beginning of the 2010s, introduced the Service Organization Control (SOC) report framework. AICPA's SOC reports include SOC 1, SOC 2, and SOC 3, with each report type serving a specific purpose. The first type of report, the SOC 1, relates to an organization's control over financial reporting. SOC 2, this article's focal point, addresses the data security and privacy controls for data processing systems belonging to service organizations. And since this specific standard caters to service organizations that employ cloud storage for their client's data, it applies to every Software-as-a-Service (SaaS) company. Lastly, SOC 3 is a general use report.

b. The SOC 2 Report

Figure 2: 'SaaS' SEO Test Image

The SOC 2 Type 2 report helps user entities understand how a service organization's system and controls compare within the five Trust Services Criteria (TSC) categories. The TSC categories derive from the trust service principles of data. They are security (or common criteria), confidentiality, integrity, availability, and privacy. The SOC 2 Report duly serves knowledgeable stakeholders that understand a service provider's system, how the system interfaces with user organizations, the nature of their service, the internal controls, and inherent limitations. The information obtainable by a SOC 2 report helps a user entity conduct a comprehensive risk assessment associated with outsourcing a business function to a specific service organization and allows the user entity to monitor the service delivery quality provided by the service company.

c. Types of SOC 2 Reports

The SOC 2 standard features two reports: SOC 2 Type 1 (or SOC 2 Type I) and SOC 2 Type 2 (or SOC 2 Type II). Type 1 reports take place on particular points (dates) in time. It reports on the suitability of the design of a service provider's controls as of that date. Contrastingly, Type 2 reports cover a time range. This second report type builds upon the Type 1 variation. In addition, it features the opinion of an auditor on the service organization's controls' adequacy in meeting the TSC. It also includes test descriptions of the said controls and the associated results for these tests.

2. Why Comply to SOC 2 Type 2?

Figure 3: 'Compliance' SEO Test Image

Not long ago, Cisco recently projected that 75% of enterprise workloads would be SaaS-based by 2021. So it is unsurprising that SOC 2 is shifting from 'ideal' to 'mandatory' for Software as a Service (SaaS) entities. Thus, compliance with the SOC 2, precisely the Type 2 standard, is now a baseline requirement when a service provider offers SaaS.

Figure 4: 'Advantages' SEO Test Image

As a service provider looking to offer their services to other companies, there are numerous benefits to complying with the SOC 2 Type 2.

a. Trust and Transparency

It is indubitable that the SOC 2 Type 2 standard set by the American Institute of CPAs is widely recognized and trusted. Thus, an independent auditor's assessment based on such reputable standards can help build an image of transparency and foster trust amongst stakeholders, especially amongst prospective customers. The estimate is that 80% of prospective customers research their options online before committing to a purchase. So leveraging a compliant status in marketing, online, and beyond can help a service organization stand out from the competition, potentially resulting in a higher market share.

b. Centralized Compliance Strategy

SOC 2 Type 2 can help service organizations establish a centralized compliance strategy to satisfy multiple customers. It can then eliminate the need for these customers to execute independent audits. There are two implicit benefits in this scenario. Firstly, a SOC 2 Type 2-compliant service provider potentially saves new customers the resources they could have committed to an independent assessment. This position presents the service company with an opportunity to build positive customer relationships with these new customers from the get-go. Secondly, since the new customer would not have to conduct an independent assessment, establishing a business relationship with the service organization may happen more quickly.

c. Cyberattack Mitigation and Reputation Protection

Apart from the competitive edge associated with compliance, third parties entrusted with sensitive data must ensure that they can safeguard the information effectively. Between 2020 and 2021, data breaches cost $4.24 million, which is around a 10% increase. Additionally, the reputational damage inflicted by these breaches amounted to the highest segment of total costs of lost businesses, at around 38%. So, any forward-thinking SaaS provider would want to protect their brand by using SOC 2 Type 2 compliance as a metric for determining and possibly raising their information security standard.

3. Why Does SOC 2 Type 2 Take Longer Than SOC 2 Type 1?

Figure 5: 'Audit' SEO Test Image

As stated before, SOC 2 Type 1 Report focuses on the design and implementation of controls, mainly only assessing the suitability of these internal controls in achieving a service provider's objectives. The SOC 2 Type 2 Report is similar to the SOC 2 Type 1 Report, but it features a broader time coverage and a wider scope.

a. SOC 2 Type 2 Time Coverage

The SOC 2 Type 1 Report concerns itself with the state of a service organization's internal controls 'as of a specific date.' In comparison, the SOC 2 Type 2 Report addresses a much broader period of time, usually twelve months. This time range makes the SOC 2 Type 2 audit exercise more arduous for service companies and auditors.

b. SOC 2 Type 2 Scope

Like the SOC 2 Type 1 Report, the SOC 2 Type 2 Report also addresses the design and implementation of controls. However, it also considers the effectiveness of a service provider's controls as evaluated by an independent auditor and expands into a few critical areas. These include System Overview, Assertion, Independent Auditor Report, Infrastructure, Control Environment.

i. The System Overview Section

This section provides in-depth details about the service provider's system and comprehensive information about their business. This information includes details such as the industry, location, service, system attributes, and more specific information like how the user organizations will use the service provider's system.

ii. The Assertion Section

In this section, an auditor verifies whether a service provider's system accurately represents the audit report by benchmarking the system description against the trust service principles of data.

iii. The Independent Auditor Report

This section features a summarised opinion of the auditor about the effectiveness of the controls within the TSC context.

iv. The Infrastructure Section

This section presents comprehensive descriptions of the service provider's internal processes and policies, their IT infrastructure, and the service provider's compliance history.

v. The Control Environment Section

This section concerns itself with the various aspects of a service provider's internal controls. These include how the service provider assesses risks, the information systems used in managing their controls, and how the service provider monitors the processes related to these controls.

4. How to Speed up the SOC2 Type 2 Audit

Figure 6: 'Efficiency' SEO Test Image

Having overviewed, reviewed, and understood the relational complexity of the SOC 2 Type 2 Report, how do we plan a SOC 2 Type 2 audit to ensure that it runs smoothly? Before answering this question about efficiency, it is essential to emphasize that a successful audit is the best way for a service company to showcase the quality of its security controls to stakeholders. So, in addition to executing it efficiently, service providers must ensure that they do it correctly.

a. Find an Auditor ASAP

It is vital that a company looking to undergo an audit endeavors to find an auditor as soon as possible if they have the opportunity to do so. However, it is an activity worth executing methodically by evaluating the auditor's experience in their industry, the auditor's auditing process, and the auditor's reputation.

i. The Auditor's Experience

It is ideal to enlist an auditing firm familiar with the industry and understand the technology, procedures, risks, and problems prevalent in the sector. For SaaS providers, it is crucial to look out for an auditor with a rich understanding of cloud computing security, data breaches, unauthorized access, customer data, and personal information preservation.

ii. The Auditor's Process

Another recommendation when picking an auditor is to assess their auditing processes. While the auditor's governing body may layout a standard procedure, each firm may use a variation of this workflow which could be incompatible with a service organization's processes in a practical sense.

iii. The Auditor's Reputation

It is also crucial to consider an auditor's reputation and brand recognition. Working with a well-recognized auditor can go a long way in improving a service provider's image.

b. Be Honest in Your Audit

If an audited business cooks up evidence, it automatically complicates the auditing process by forcing itself into a position where it will have to remain cagey and non-forthcoming. This situation may even arouse an auditor's suspicion, potentially leading them to more combatively challenge the audited company's decisions and processes every step of the way. So, an honest and forthright approach is an ideal path (Limoncelli 2019) because it will preserve the audited company's reputation and make the process go smoother. A legitimate business undergoing an assessment will naturally be transparent and forthcoming with information, translating into improved efficiency of the auditing process.

c. Choose Your Criteria

For SOC 2 audits, companies can choose from the five trust service principles discussed earlier.

The security criterion addresses governance, security awareness controls, controls for risk management, control monitoring, operations, and change management controls.

The availability criterion addresses system recovery, disaster recover, data backup controls, and capacity administration controls.

The confidentiality criterion addresses controls related to the acquisition, disposal, and boundary protection of systems. It also covers third-party confidentiality, internal confidentiality awareness.

The integrity criterion addresses controls for data processing accuracy, modification management, storage, system input integrity, and data processing error management.

The privacy criterion covers IT security controls, data quality, compliance monitoring, privacy notices, data collection processes, privacy policies, and internal access controls.

However, it is noteworthy to mention that only the security criterion is mandatory. Depending on the service organization and the service they offer, it may not make sense to incorporate all criteria. However, when a service provider provides software as a service, the other criteria also apply as they are all relevant to information security. And, while it is possible to select additional criteria outside the TSC, service providers must assess the benefit, as tacking on other criteria will counter the efficiency of the assessment.

d. Create a Timeline

Figure 7: 'Project Management' SEO Test Image

As hinted earlier, it takes around twelve months for a first SOC2 Type 2 audit. However, just because management schedules an on-site auditing test does not mean they can forget about it until D-day. Instead, it is ideal to consider the scheduling as the beginning of a one-year-long arduous but rewarding project. Because to improve the chances of a speedy and efficient audit experience, the early months following the on-site test scheduling event are critical to getting ahead with preparation and planning.

The first month is ideal for defining the audit scope, shortlisting, and selecting an auditor based on the auditor qualities and attributes previously discussed.

In the second and third months, companies should start acquiring and refining their audit checklist and mapping their controls, ensuring that it aligns with the criteria they have selected for the audit.

By the fourth and sixth months, companies should start conducting remediation and readiness audits. Additionally, they must ensure that they have already established a strong compliance team. A competent compliance team must include legal personnel, IT security personnel, and authors. And if they desire efficiency, project management personnel must be a must.

Further on the project management matter, reflecting on the above activities, one can easily observe that these steps need airtight planning and execution. So, a business looking to get through the SOC 2 Type 2 audit efficiently must execute the project in a near-perfect manner. Thus, an ideal move after

scheduling an audit is to contract the skills of an experienced project manager specializing in helping SaaS companies get through SOC 2 Type 2 audits.

Around months 7 and 8, the compliance team should thoroughly review and organize their documentation and complete any final verification checks in readiness for the start of the audit.

Following a first audit, companies must establish internal processes to ensure regularity and consistency in compliance effort. Section 801 of AICPA's '*Reporting on Controls at a Service Organization*' states that a SOC 2 Type 2 report covering a period fewer than six months is unlikely to serve the needs of neither user organizations nor auditors (American Institute of Certified Public. Thus, it is ideal to conduct subsequent audits religiously every six to twelve months after the first one.

5. Other Things to Remember

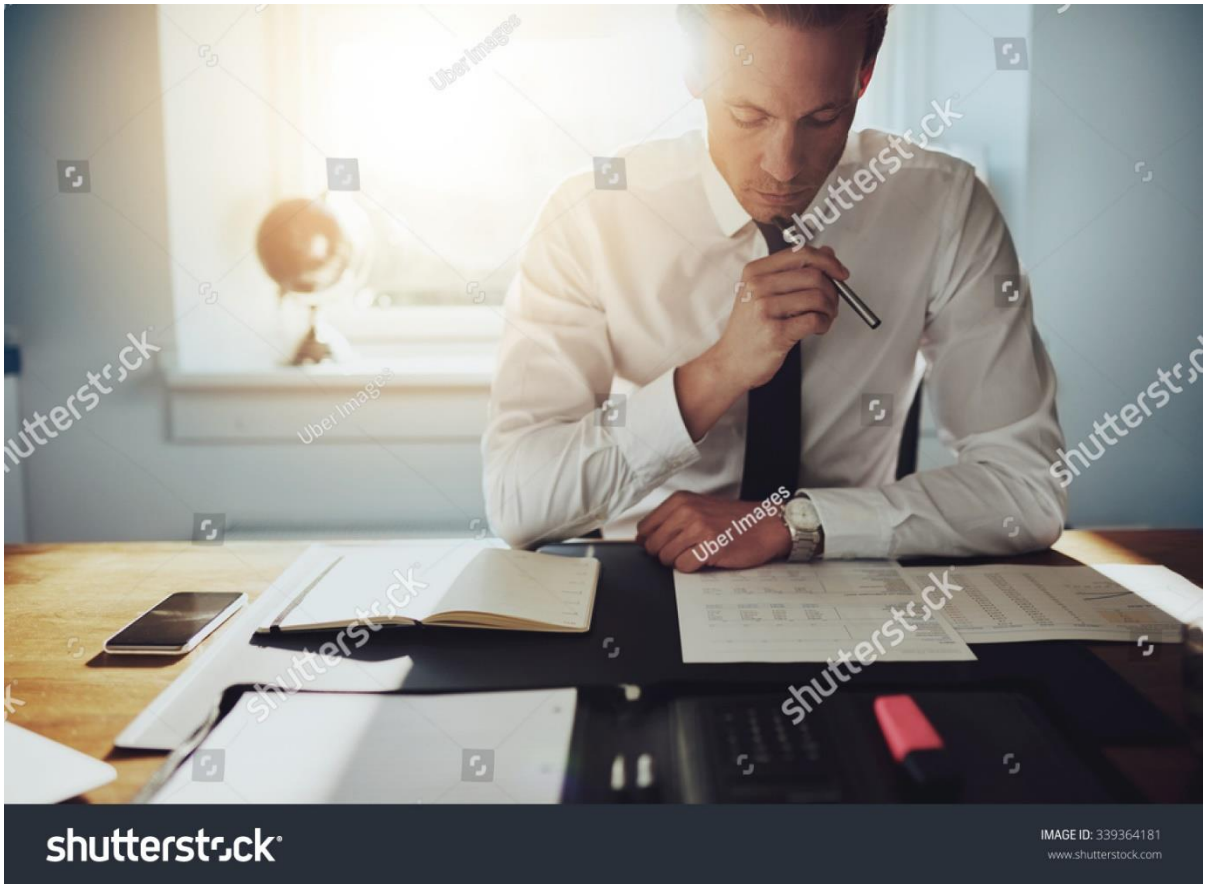

Figure 8: 'Serious Businessman' SEO Test Image

Finally, besides the points in the preceding sections, there are a few miscellaneous points worth mentioning regarding SOC 2 Type 2 audits.

a. Mutually Aligned Interests

It is crucial for companies that are about to undergo a Soc 2 Type 2 audit to keep in mind that their interests align with the auditor. While any reputable auditing firm would want to carry out an honest audit, they do not wish to find your business non-compliant on every level. Such an adverse outcome would neither favor the auditee that would have to repeat the laborious process nor the auditor, who would most likely lose repeat business.

b. Audit Documentation

It is noteworthy to state that companies need to ensure that they appropriately document the outcomes of every audit exercise. These documentations are not only crucial for subsequent audits and regulatory matters, but they also prove invaluable as part of a disaster recovery strategy. When cybersecurity attacks occur, a comprehensive root cause analysis is almost always mandatory. Such analyses help to uncover the root causes of problems, making it easier to identify appropriate solutions. Documentation associated with audits usually serves as goldmines for gaining insights needed to respond adequately.