Pivot Point SECURITY

SOC 2 “CliffsNotes” for SaaS Firms

What Every SaaS Firm Needs to Know When Considering Attaining a SOC 2 Attestation

Why SOC 2 is Potentially Important to a SaaS Firm

If your SaaS firm is selling into regulated verticals like healthcare, pharmaceuticals, or financial services, it’s hard to close a contract without a solid security attestation on the table. Regulated businesses can’t easily outsource or use your software as a service unless you can prove your solution won’t weaken your potential client’s security/risk posture.

For companies operating primarily in the US, a SOC 2 report is one of the commonly requested attestations when evaluating service providers’ security (Third Party Risk Management (TPRM)). Part of the American Institute of CPAs (AICPA)’s Service Organization Control (SOC) reporting platform, SOC 2 reporting provides a widely respected, independent attestation as to whether a third party can keep client data secure.

Should You Get a SOC 2 Report?

A positive SOC 2 attestation can make a strong statement about your security posture and overall IT maturity, but SOC 2 is a report not a certificate like, ISO 27001. It's important to note that the report can reveal both good and bad about a your security.

For SaaS firms offering one or more customer-facing applications to the US market, a SOC 2 report is a great way to demonstrate that your security controls effectively manage information security risk in accordance with best practice and relevant laws/regulations.

In general, a SOC 2 report is valuable for any SaaS business looking to prove that they are secure and compliant to key stakeholders.

What Does a SOC 2 Report Cover?

SOC 2 reports cover a wide spectrum of controls in a high level of detail. The heart of a SOC 2 report is the Trust Service Principles: Security, Availability, Confidentiality, Processing Integrity, and Privacy. The entity being audited can choose which of these five Principles are in scope for it's SOC 2 report.

Security is always in scope per the SOC 2 guidelines. In our experience, the great majority of SOC 2 reports for SaaS offerings also includes Availability controls. Confidentiality and/or Processing Integrity are most often in scope for banks and other entities that provide payment services, or whose business revolves around performing highly accurate calculations.

Likewise, Privacy may be important if you are processing a lot of Personal Information and receiving Data Privacy Addendums from your clients.

How Does SOC 2 Compare to SOC 1 & SOC 3?

A Common Source of Confusion is SOC 2's Relationship to the Other SOC Reports

- **A SOC 1 report focuses on controls critical to accurate financial processing only. It is valuable to clients, partners and other stakeholders that have a strong interest in verifying that the controls you have in place provide assurance that the financial data you process can be trusted.**

- **A SOC 3 is an additional report that entities holding SOC 2 reports can request. A SOC 3 is basically an "open to the public" statement about your information security and IT posture. It offers much less detail than a SOC 2, which should only be shared under non-disclosure.**

Should You Get a SOC 2 Type 1 or a SOC 2 Type 2 report?

It’s easy to confuse the SOC terminology; for example, mixing up SOC 2 Type 1 with SOC 1 Type 2. The “types” pertain to both SOC 1 and SOC 2, and their meanings are pretty simple

- **A Type 1 report is a “point-in-time” report. That is, you only need to provide one piece of evidence for a control to be rated as effective. In short, Type 1 reports attest to whether an entity’s controls are designed effectively.**

- **A Type 2 report is an “over time” report that requires multiple pieces of evidence per control. The sampling period, which the audited entity determines, is usually six to twelve months. In short, Type 2 reports attest to whether an entity’s controls are designed and operating effectively.**

- **Experience shows that most clients and prospects asking a SaaS vendor (like you) for a SOC 2 report are referring specifically to a Type 2 report, as it provides a higher level of confidence that you are operating in a sound manner and following your own procedures. However, especially for startups that don’t have a long enough track record to attain a SOC 2 Type 2 report, a SOC 2 Type 1 report can still be very useful as an interim step.**

What does a SOC 2 engagement look like?

Scope

As you'd expect, working towards a SOC 2 report starts with a scope definition discussion, which provides background on the business, and key services you provide. This yields the "system description" section of the SOC 2 report, which the audited entity is responsible to develop. During scoping you should also be assessing the maturity of the SOC 2 controls in place and gaining an understanding of information security risk.

Risk & Gap

Post scoping, you should perform a formal Risk Assessment (a requirement of SOC 2) to ensure that risks are well understood and properly managed. For those risks that are not yet effectively managed, Risk Treatment plans should be generated. Now, understanding scope, risk, and control maturity you can identify any additional gaps in the implementation of controls specified by the Trust Service Principles that are in scope.

Remediation & Controls Matrix

In line with remediation is the development of a controls matrix, which the audited entity provides to the SOC 2 registrar during the formal audit. The controls matrix is an "audit roadmap" that tells the auditor what to audit to confirm compliance. A final preparatory step before the formal audit is a readiness assessment. This validates the artifacts that you will present during the SOC 2 audit achieve their requirements.

Its Time to Take The Next Step

Where are you in your SOC 2 journey?

Still Researching SOC 2 and whether its something you need

Great! Here are some more resources to keep you going

Click here!

Looking into other forms of attestation like ISO 27001

Even better! We have an entire podcast episode dedicated to this topic.

You can find it here

Need to talk to someone about SOC 2... now!

Let's do this! Here is a link to book some time on our SOC 2 experts calendars

Click here!

Pivot Point

SECURITY

Any questions? Reach out!

☎ 609-581-4600

@ info@pivotpointsecurity.com