SOC Report Standards – Benefits & Pitfalls for Tech Companies

wolfandco.com/resources/insights/soc-report-standards-benefits-pitfalls-for-tech-companies

March 18, 2020

The healthcare and financial services industries are well versed in the benefits of System and Organization Controls (SOC) reports, as well as the pitfalls of not getting one. However, on the other side of the market, early stage technology companies, with their sights set on moving fast and innovating even faster, may not fully understand the critical role a SOC report can play in their business.

This entrepreneurial spirit leads some tech companies to avoid taking the time to engage an audit firm to produce SOC reports—a decision which could prove detrimental to company success, customer relationships, and marketplace advancement. SOC reports are given after a CPA firm audits internal controls related to IT systems and security processes. SOC standards were created to ensure that service providers (such as technology companies) have been through a professional examination of their internal controls. These reports provide information on the provider's internal controls to their customers, using a standardized reporting format.

Meeting these guidelines is not required by any current regulations. However, technology companies can obtain a competitive advantage by proving that they have the proper internal controls and safeguards in place. More often than not, prior to doing business with your tech company, your customers will want reassurance and evidence that you have the proper security protocols in place to protect their data.

If your company wants to sell to customers like money-center banks, hospitals, and other institutions that take a sophisticated approach to managing risk, meeting the SOC reporting standards is crucial.

SOC Report Types

There are three types of SOC reports, which include:

- SOC 1: These reports cover controls for financial reporting
- SOC 2: These reports cover information systems and evaluate their security, availability, privacy, confidentiality and/or processing integrity
- SOC 3: These reports cover the same criteria as a SOC 2 report, but the reports are intended for widespread public distribution and include an official seal of certification

These SOC reports can come in the form of Type 1 or Type 2. So, for instance, a company can obtain a SOC 1 Type 1, SOC 1 Type 2, SOC 2 Type 1, or SOC 2 Type 2, etc.

- Type 1
  Type 1 SOC reports are as of a point-in-time. That is, the relevant controls only need to be in place as of a specific, predetermined date.
- Type 2
  Type 2 SOC reports, by contrast, are for a period of time. That is, the relevant controls need to be in place and operating effectively for a predetermined period of time (usually 12 months, but can range from 6 to 18 months or more).

Early stage technology companies may be particularly interested in knowing about SOC 2 and SOC 3 reports, since these companies' products often handle substantial amounts of sensitive customer data.

SOC Report Compliance: It Takes Time

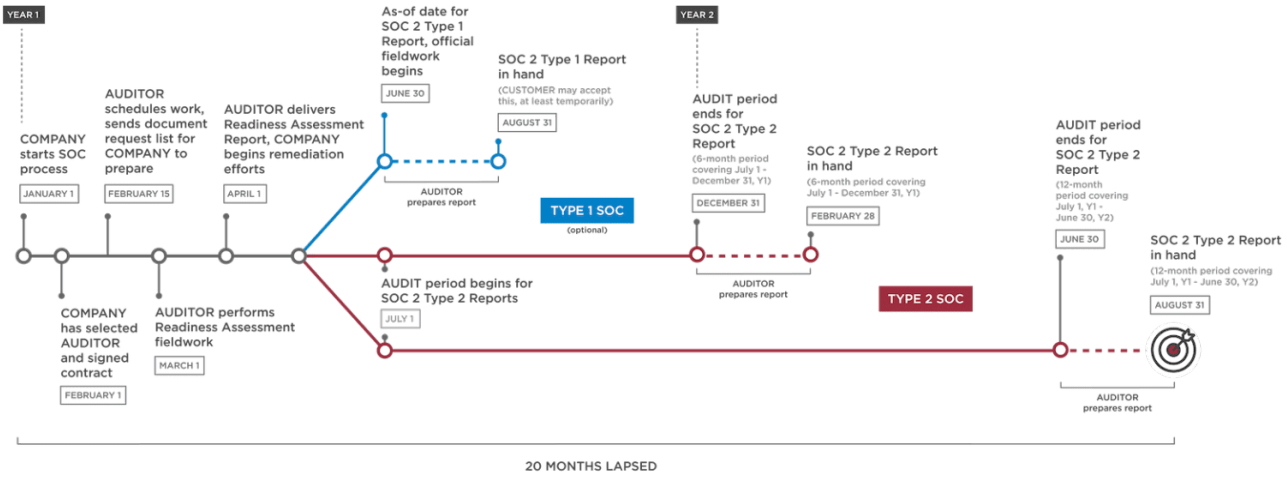
Technology companies thrive on innovation and speed. They can be intentionally less controls-focused in order to spur creativity, relying on their own confidence in their security systems rather than putting them to the test. But to a customer, it doesn't matter whether you have the best security protocols in the industry—you have to be able to prove it.

Oftentimes, if technology companies do not already have a SOC report, they find their backs against a wall when it comes time to sign a contract with a customer. The customer has asked for a SOC report before making the business relationship final, and the tech company must now react quickly. Your inability to produce a SOC report when asked can severely hurt the provider-customer relationship.

Most customers of technology companies will request a SOC 2 Type 2, but if you are starting from zero (i.e. your tech company has never engaged an audit firm to prepare them for SOC reporting), those types of audits take time to complete.

SOC Procedures

If you are caught in a situation where you are almost at the finish line of securing a customer, but then the customer asks for a SOC 2 report and you do not have one on hand, this is the realistic timeline of when you can expect to receive that report to give to the customer.



Readiness Assessment

First, your auditor will provide your business with a readiness assessment, where they analyze your business procedures, look for gaps, and then send you away with a list of processes that need to be fixed or optimized. This process will take a month or two.

Realistically, and based on the number of control gaps found, it could take your business months to implement the proper controls. By the time you have fully remediated the findings from the readiness assessment, it could have been six months since the customer asked you to produce a SOC report.

Type 1

A Type 1 report is entirely optional, but in situations like this, it is recommended that tech companies engage an audit firm for a Type 1 report because it is the quickest and easiest way to obtain a signed SOC report in the hands of a prospective customer. A Type 1 (point-in-time) report is a clear stake in the ground for a Type 2 (over time) report. Type 1 prepares the tech company for the rigor and requirements of Type 2 and sets the stage for a smooth and successful Type 2 audit process.

It will take about two months for an auditor to generate this report.

Type 2

For customers of tech companies, Type 2 reports carry more weight because it shows that the proper security controls have been in place and operating effectively for a substantial amount of time. Usually, from the time your Type 1 report was completed, you will have to wait a full year before an auditor can return to generate a Type 2 report. However, the Type 2 can cover a shorter period of time. Some companies opt for 6-month Type 2 report to have it completed sooner.

It has now been about 20 months since your customer asked for your SOC 2 Type 2 report (or 14 months, if a 6-month audit period was requested). Although auditors will respond in a reasonable and timely manner, this kind of delay could cost your company the sale, and preparing for SOC reports ahead of time could help your company avoid a painful and stressful situation.

Conclusion

You may have the utmost confidence in your technology company's security controls, but none of that confidence matters if you cannot prove your security posture to your customers. Getting new customers is hard, and the last thing you want are roadblocks to closing a sale. Having a SOC report in hand can be invaluable in pushing that deal over the finish line. So, don't wait to be asked—start now!