**SOC 2 for Startups: Is it Worth It?**

When it comes to security frameworks, there is no shortage to choose from. From industry-agnostic to industry-specific, it can be overwhelming deciding which security framework is right for your company. Odds are that your organization is weighing SOC2 vs. ISO27001 for your primary framework. In this article, we will cover some of the costs, benefits, and reasons why an organization may choose a SOC2 attestation.

**Quick Overview of SOC 2**

When it comes to ISO27001 vs. SOC2, the first big difference is that SOC2 is not a certification. Unlike ISO27001, which has a certification body that will allow consultancies to certify against the standard, SOC2 only allows accredited accounting firms to perform an audit, make observations and attest to the security control efficacy for the organization.

Additionally, SOC2 is different from ISO27001 in that it has two different levels, or observation periods, for attestation. There is a SOC2 Type I, which is a single point-in-time audit of controls, and a SOC2 Type II which is an audit over a period of time (usually no less than 6 months and as long as 12 months). The Type I audit is meant to show the control operation at a single point in time while the Type II attempts to show that the control is not only implemented but performing consistently over time. Most organizations requesting a SOC2 will not accept a Type I, so an organization looking for attestation against SOC2 should take that into account.

Beyond the key differences in the audit outcome, the versions of SOC2, the other key difference is in the structure of the requirements. ISO27001 is broken into clauses (program management requirements) and statement of applicability or the controls that the organization will implement within their security program. Whereas SOC2 is broken down into Trust Services Categories (TSC), with Security being the only one required. There are 4 additional TSC that an organization can choose to add to their attestation: Availability, Processing Integrity, Confidentiality, and Privacy.

**Why Would a Startup Consider SOC 2?**

Revenue is what every startup is chasing and attempting to remove any blocker in attaining. The reality is that no certification or security framework is going to alleviate all blockers or friction in building trust with prospective clients but having something, almost anything, certainly helps. Having a SOC2 attestation will make the conversation easier when the prospective client’s security team gets involved and could possibly eliminate a request for an audit by their security team which could make ongoing management of customers that much easier. Would you rather have 10 customers auditing you on a yearly basis with differing security control requirements or work towards a common framework like SOC2?

Add in primarily operating in the United States, and SOC2 has become almost table stakes for most organizations as for requirements for their vendors. In some cases ISO27001 will suffice for an organization in North America but in general, ISO27001 is more recognized and required outside the US. SOC2 has picked up popularity in Europe over the last 5 years due to the number of US-based companies that are operating in the market, but it is not as commonly requested outside of these two large markets.

Another reason to consider a SOC2 for your security program is that it will provide direction and coverage for your security controls. This will allow your organization to more easily establish a set of expectations and requirements to operate within and which will make any future security frameworks or requirements easier to attain and manage. By selecting a framework to build a security program foundation on, it is easier to adapt and map to additional frameworks as needed and will allow for rapid maturity of the security program.

**More Important for Some Businesses Than Others?**

The reality is that SOC2 attestation may not be extremely relevant for a company that is a business-to-consumer company. Most consumers are not going to ask for a SOC2 attestation before doing business with that company. However, it could still help in establishing a strong set of controls and requirements to assist with meeting all the varying data privacy requirements that exist. It will not satisfy them or show compliance with the data privacy regulations but will certainly establish a foundation to assist with meeting the requirements.

For any SaaS-based or more importantly, business-to-business company, it very well is a base requirement to have a SOC2 attestation or other equivalent certification. Further, there are industries that will have more stringent requirements for a partner to have an attestation or certification. Some of these industries include banking or finance, insurance, investments, and working with any large Fortune 100 company.

Why is it something that is expected or required by these industries and larger companies? Well, SOC2, as it is an attestation, is a little different than other frameworks that only provide a certification. Since this is an attestation of compliance, the report itself provides high-level information on how the control is designed, operated, and if there were any observed exceptions or operational issues with the controls. This is extremely powerful for prospective client security teams to better understand the internal security program without needing to conduct their own audit.

**When Would SOC 2 Make Sense for a Startup?**

The reality is that security is expected to be baked into a company from the start. However, this is not always feasible in that their may not be enough operational budget or personnel to take on the added tasks. So, why reality may not be able to met, the realistic expectations would be that founders start to think about security and security frameworks from the beginning. This can be accomplished by using the frameworks to help build and operate the systems without attaining certification or attestation. The reason this is recommended is that it is easier to build it right the first time than to rebuild it to meet the requirements.

If this is not the case, then any startup should start to work towards a framework once the first one or two clients have been signed. As more clients are signed, or as the company continues to grow, a level of maturity will be expected, regardless of age. With additional revenue, data, and customer information, a company will become a larger and larger target which means the security of the systems, people, and data needs to improve to prevent a breach. As a young company, any sort of data or security breach could end any hope of taking over the world.

Knowing that security should be considered early, the next question is when to go after a SOC2 attestation. This is really dependent on the TSC that the company is looking to certify against. If it is simply the Security TSC, an organization could attain that much quicker than adding additional TSC to the audit. Some of the common items that will need to be in place would be:

* Security program management, reporting, and improvement tracking
* Risk management program
* Inventory management process or procedure, tracking, and identification
* Access management process or procedure that includes onboarding, offboarding, and auditing of rights
* Physical security of office space, data center, or secure areas
* Network and application security and operational procedures
* Security operations and monitoring to detect potential security events, triage, and respond
* Vulnerability and patch management process or procedure
* Disaster Recovery and Business Continuity Plan
* Change management for software, infrastructure, and network

**The Process for Startups to Get SOC 2**

When it comes to attaining an attestation of compliance against SOC2 there are several decisions that must be made upfront before jumping into the process. First, what TSC are applicable, needed, or required for your company? Second, are you going to attain Type I or Type II? If you are attaining a Type I, is it simply to show that the controls are in place until such time as you have built up enough evidence to attain a Type II? Lastly, for Type II, what is the period you will have in scope for the audit, 6 months, 12 months? Once those questions are answered, you can start to work towards attaining the attestation.

Now that you have decided on the TSC, type of attestation, your company will then need to work through the TSC to determine the scope of the audit. Once the controls that are in scope are identified, it is recommended to perform a thorough gap assessment against those controls in scope to determine where the company needs to invest to meet the requirements. This will then involve determining how best to close those gaps, and potentially working with vendors to assist with this. Until the gaps are closed, the audit evidence will not be able to start, so it is important to work quickly to address any deficiencies in the program.

After the gaps are closed and evidence of control operability is gathered, the company can then work on picking their auditor to complete the attestation. There are many certified accounting firms, large and small, that can provide this service so it should not be hard to find one. Once key ask should be if the period you plan to gather evidence in for the Type II is sufficient for your preferred vendor. Some vendors will require 12 months while others may shorten it down to as little as 3 months. Once a vendor is selected, it is highly recommended that your company conduct a readiness assessment prior to the audit to make sure that no major gaps or deficiencies would be identified during the attestation audit. After this, the vendor will conduct an audit looking over the evidence that has been gathered over the time period to assert that the controls have been operating as designed for the period of time. This could be reviewing all evidence or reviewing a sampling of evidence.

**How Much Will a SOC 2 Cost a Startup?**

When it comes to attestation costs, there are three main buckets that a company will incur costs in; control implementation, consultancy services, and audit itself. Odds are the largest bucket will be the control implementation as a company working towards attaining its first certification or attestation will have quite a few gaps in controls and capabilities which then leads to additional costs in consultancy services. For a more in-depth review of the cost factors associated with SOC2 attestation, we have broken down the factors of SOC2 in the following [article](https://networkassured.com/compliance/soc-2-certification-cost/).

For this article, the focus will be on the attestation itself. When it comes to audit costs, the two main drivers are the number of employees in scope for SOC2 and the TSC in scope. As an organization has more employees, it means more evidence that will need to be audited, which requires more time by the auditing firm. For most organizations, depending on the size and TSC in scope, Type II attestation can be attained for somewhere between $20,000 and $100,000.

**How Startups Can Accelerate SOC 2 Attestation?**

What can a startup do to make the process go more smoothly? Get certified more quickly? How can they save on costs as they're going through the process? List 4 or 5 tips/strategies that are likely to make the biggest improvements to their compliance journey.

There are not really any proven ways to successfully accelerate the attestation process without a strong buy-in from leadership. A security team, or security leader, cannot force compliance with the framework without all of the business assisting as the controls reach outside of a single team. With that in mind, the following are some ways an organization can attain an attestation in an accelerated fashion.

Automated SaaS

There are several vendors in the space that offer automated tools to assist with gathering, cataloging, and providing guidance for control implementation for security frameworks. In many cases, these tools claim that they can shorten the time period to attain attestation from months to weeks, which seems pretty aggressive. There is no doubt that a tool that is integrating through APIs with all the core tools, services, and infrastructure can assist in managing and attaining evidence to assist with certification. Oftentimes, the trade-off of the additional cost for this SaaS solution is that the attestation will be streamlined and lower cost.

Utilize MSP

There are many MSP out there that can help with standing up core controls or competencies to meet SOC2. In fact, there are companies that are designed to take responsibility for whole sets of controls to make the process faster, easier, and more efficient.

Engage SOC Consultant Experts

When in doubt, money at the problem. While not all organizations can throw large amounts of money at consultants to fully stand up their program, every little bit can help speed up the process. Even if your company can only afford 2 weeks of help, this will significantly increase the ability to properly design and implement the controls needed. It’s not uncommon for them to already have a strong set of tools, documents, or recommendations to assist with attaining certification.

Limit Scope

If the entire company does not need the attestation, then don’t attain it for the full organization. Scoping the audit to the right set of applications, business units, or infrastructure can significantly assist with speeding up the process. This would allow your company to attain the attestation for the required business or application unit until such time as the company can fully be compliant.

**Weighing The Costs & Benefits of SOC 2**

It can be difficult to determine if there will be ROI on attaining a SOC2 attestation. One of the best ways is to evaluate how many customers or external entities are asking for a SOC2. Add in any external entity that would be willing to drop audit rights for SOC2 and this could help with establishing the potential ROI for the business. A great example is that if you have 4 customers that have audit rights and you spend 1 week each conducting an audit with them, how much could the business save by utilizing SOC2?

Beyond customers requiring or asking for audit or security certifications, the reality is that a SOC2 can be hard to justify. After all, the attestation was built with the purpose of helping organizations to better understand the security posture of vendors, partners, and customers.