SOC 2 for Startups

Security has been an all-time concern for the business organizations which has become more significant in rapidly changing technology world with increasing reliance on the cloud infrastructure. With growing security number of vulnerabilities, it is important to stay compliant and protect your organization from any security threats irrespective of the size of your organization.

One might think that it's easy to obtain a SOC 2 report for a startup due to its small size, limited locations and limited number of applications. However, startups may miss on key things like elaborated policies & procedures, mature change management processes, addressing incidents in a timely manner which are important from a compliance perspective.

In this blog we will talk about why a SOC 2 compliance is important for small organizations like startups and how it can help them build a mature and robust control environment.

Following are key aspects to be taken care by a startup when planning for a SOC compliance

Starting with Scoping & SOC Readiness Assessment

The first step for a startup when planning for SOC 2 assessment is scoping & readiness assessment. This will help you obtain an end to end understanding of the SOC 2 auditing process and the intermediary phases. Following are the key points covered during a readiness assessment:

- Brief overview of the AICPAs SSAE18 attestation standards and the SOC 2 framework
- Assessing the internal control, policies, procedures, and processes, and identify any gaps need that may need to be fixed before getting into an actual SOC 2 audit.
- Deciding the scope of audit including the business processes to be covered, people who will be involved, physical locations to be covered and any third-parties to include within the scope of the audit
- Preparing an engagement plan for the audit to ensure timely completion of SOC engagement

Correcting the Documentation

Startups tend to have less number of people performing a wide range of tasks, one often may find that people are more focused on business activities and may not have developed the standard set of policies and procedures (information security and operational policies). Below are some of the key policies to be taken care of:

- Logical and Physical access policies
- Application change management procedures
- Financial data backup policies and procedures
- Incident management policies and procedures
- Acceptable usage policies and procedures

Accorp also offers a service for developing your key policies and help you prepare for the SOC audit.

accorp

Fixing Security and Operational Areas

After you have your standard policies in place, it's time to implement them and make sure that the IT systems are aligned with the standards documented in the policies. It's important to devote time in remediating and putting in place the security and operational measures that have been found during the actual SOC 2 scoping & readiness assessment. Following are few the implementation measures to be considered:

- Reconfiguring the IT infrastructure
- Implementing two-factor authentication solutions
- Implementing vulnerability scanning and application monitoring tools
- Setting up data encryption and security solutions
- Conducting security awareness trainings
- Testing the incident response plan

Apart from the above mentioned, you can also consider implementing any other solutions that may be required to bridge the gaps identified during the readiness assessment.

Performing a demo

By this step, we have remediated any identified gaps in Step 1 with a SOC 2 scoping & readiness assessment. It's now time to perform an official "dry run" before the actual audit starts. The best way is to follow the AICPA SOC 2 standards (SSAE18) and evaluate your internal controls and policies, procedures, and processes against the applicable Trust Services Criteria. Once you are confident enough, you are good to go ahead and get into an engagement with a CPA firm for performing the actual SOC 2 audit.

Expectations from the Audit

Generally auditors send out a standard list of deliverables for the audit. Many auditors refer to this as a PBC List (A "Prepared by Client" list of items). A fair number of these items will be asked to be provided to auditors prior to showing up onsite, just so they can get a better idea of your internal controls and relate processes.

Further, auditors look for the following types of evidences:

- **Policies and procedures:** Having well-written information security and operational documentation is key to the success of your overall audit as mentioned earlier
- **Screenshots of system settings:** Expect to provide screenshots of various system settings, such as server configuration, software versions etc.
- **Proof of operational evidence:** Auditors will request materials that can validate you have performed an annual risk assessment, performed security awareness training and tested your incident response plan
- **Interviews:** Auditors will often spend a considerable amount of time interviewing personnel for finding out more about their roles, responsibilities, and related processes
- **Signed memos:** Auditors will often ask you to document a control via a signed memo

Last but not the least, communication with your auditors is absolutely key to the success of your SOC 2 audit. Don't make assumptions as the auditors are just doing their jobs. It's important to be transparent with them at all times.

Summary

Since, majority of the software companies are making use of cloud solutions to store customer data. SOC 2 is one of the most important and sought after security compliances to go for. Getting SOC 2 certification for your company will not only increase credibility and trust, it will also produce security benefits that will help the organization to become mature.

Please contact us if you would like to know more about data security or need any help to perform a SOC/ GDPR certification for your organization.
Visit our website https://accorppartners.com/soc/index.php or visit https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html to read more articles related to SOC reporting.