SOC 2 for Dummies

The A to Z Basics of SOC Reports & Audits

SOC 2 for Dummies

The A to Z Basics of SOC Reports & Audits

Looking for a SOC 2 for Dummies guide (and we're not saying you're dumb!), rather, you need a guide that cuts through the complexities of what a SOC 2 audit is? If so, then welcome to the SOC 2 for Dummies pages, courtesy of NDB, North America's leading provider of SOC 2 Type 1 and SOC 2 Type 2 audit assessments.

With that said, if you're new to the world of SOC 2 compliance, take note of the following points for gaining a greater understanding of what it really takes to get ready – and become – SOC 2 compliant.

1. Know What the SOC 2 Framework is all About
2. Find an Auditor who Knows Your Industry
3. Scoping & Readiness Assessment
4. Determine which TSP's are in Scope
5. Remediation is Critical to becoming Compliant
6. Remediate!
7. SOC 2 Compliance is NOT an Overnight Process
8. It is an Annual Requirement (Typically)

SOC 2 for Dummies

1

Know What the SOC 2 Framework is all About & What it Isn't

SOC 2 is an assessment conducted on an organization's internal control environment. What are internal controls? They are an organization's policies, procedures and processes. SOC 2 has become one of the most widely accepted and well-known regulatory compliance assessments performed on service organizations. So, what's a service organization? It's an organization that essentially offers services to another company. Think Software as a Service (SaaS) providers, e-commerce businesses, data centers – almost any organization that's providing essential services to another business.

2

Find an Auditor who Truly Knows Your Industry

Sounds easy enough right? Well truth be told, some industries really require the knowledge & expertise of a CPA who can understand your business from the beginning to end. The more familiar a CPA firm is with your industry, the greater the efficiencies on the overall audit, no question about it, so keep this in mind. To learn more about NDB's industry expertise, please contact Christopher Nickell, CPA, directly at 1-800-277-5415, ext. 706, or email him at cnickell@ndbcpa.com today.

3

Get Started with a Scoping & Readiness Assessment

One of the best activities to undertake for any SOC 2 report is a SOC 2 scoping & readiness assessment and for some very obvious reasons. When performed correctly, a SOC 2 scoping and readiness assessment helps to determine the actual audit scope, which items require remediation, what personnel are to be involved in the audit, what third-parties are involved & much more. It is an essential component of any SOC 2 audit process from beginning to end. Contact us today to learn more.

4

Determine which TSP's are in Scope

The following five Trust Service Principles can be included within the scope of a SOC 2 assessment:

Security: The system is protected, against unauthorized access.
Availability: The system is available for operation and use agreed to.
Processing Integrity: The System processing is complete, accurate, timely, and authorized.
Confidentiality: Confidential Information is protected as agreed.
Privacy: Personal information is collected, used, retained & disclosed in conformity with the commitments in the entity's privacy notice and with the privacy principles put forth by the American Institute of Certified Public Accountants

The A to Z Basics of SOC Reports & Audits

5

Remediation is Critical to becoming SOC 2 Compliant.

Every service organization – and we mean "every" – has some type of remediation that must be performed prior to the actual audit. Perhaps its missing policies and procedures. Maybe an annual risk assessment needs to be performed, or security awareness training needs to be conducted. Bottom line – every service organization should fully expect to undertake some form of remediation in the world of SOC 2 audits. How little or how much remediation is dependent upon one's control environment and how mature it is or isn't – that's really what it comes down to.

6

2 Main Categories of Remediation Regarding SOC 2 Audits

There are 2 main categories when it comes to remediation regarding SOC 2 audits, so let's take a look at each of them.

Documentation: You will need to quickly come to an understanding of the importance of documentation – specifically – information security policies and procedures.

Technical: Perhaps your password complexity rules may need to be strengthened, firewall rules need to be re-configured, or backups need to be performed,

7

SOC 2 Compliance is NOT an Overnight Process

Hey, Rome wasn't built in a day! Luckily, becoming SOC 2 compliant won't take years, but it is a process that begins with a SOC 2 Scoping & Readiness assessment and culminates with the issuance of a SOC 2 Type 1 or a SOC 2 Type Service Auditor's Report from a licensed CPA firm. With that said, expect to spend 2 to 3 weeks performing the readiness assessment, and then anywhere from a few weeks to a few months on remediation. Remember, remediation is the big X factor as no one can really predict how long it could take.

8

It is an Annual Requirement for most service organizations

SOC 2 compliance is not a "one-and-done" deal. Once your organization has entered into the world of regulatory compliance, expect to stay there. And why? Because your customers demand and expect security controls that are functioning and securing their data properly. Companies are sharing and exposing their data, IP, and other sensitive information more than ever, and they want assurances of the safety and security of such information. SOC 2 is here to stay, so work with a firm that's got a proven track record of providing fixed-fees and high-quality service.

To learn more about NDB's industry expertise, contact NDB at:

☎ 1-800-277-5415, ext. 706 ✉ audits@ndbcpa.com