## How to Prepare for an Audit

### Define Your SOC 2 Audit Scope

**Announcement**

Make a company-wide announcement on your SOC 2 compliance initiative.

Beyond unlocking sales and fueling growth, compliance protects your brand reputation and builds trust with customers.

**expectations**.

Explain how the compliance process may affect daily operations and workflows, including processes and tools used.

Change is difficult, but people will be more open to it if they understand the causes and benefits of that change.

### What is SOC Report?

A SOC 2 report is a way to build trust with your customers. As a third-party service organization, Nexelus works directly with a lot of clients’ most sensitive data. A SOC report is evidence that you’ll handle that customer data responsibly.

To get a SOC report, you have to undergo an audit by a third-party auditor. A SOC auditor will be either a CPA or a firm certified by the American Institute of Certified Public Accountants (AICPA). They’ll evaluate your security posture to determine if your policies, processes, and controls comply with SOC requirements.

### SOC 2 Compliance Requirements

SOC 1 is designed specifically for service organizations that provide financial reporting services.

SOC 2 is a standard for information security based on the Trust Services Criteria. It’s open to any service provider and is the one most commonly requested by potential customers.

SOC 3 is also based on the TSC but is less thorough, with results that can be shared publicly.

#### What Are the Requirements for SOC 2 Compliance?

Before you begin a formal SOC 2 audit, you’ll need to understand the details of the Trust Service Criteria(TSC), since they're the basis for all SOC 2 requirements.

**Information security**: How do you protect your data from unauthorized access and use?

**Logical and physical access controls**: How does your company manage and restrict logical and physical access to prevent unauthorized use?

**System operations**: How do you manage your system operations to detect and mitigate process deviations?

**Change management**: How do you implement a controlled change management process and prevent unauthorized changes?

**Risk mitigation**: How do you identify and mitigate risk for business disruptions and vendor services?

#### Do You Need a Type I or Type II Report?

Most often, the decision boils down to how fast you need a SOC 2 report.

Type I reports evaluate your internal controls at a single point in time.

Type II reports assess how well your controls perform over an extended period of time.

Because of the nature of the different report types, Type I reports can be completed much faster than Type II reports.

If you can’t wait months to put systems in place, a Type I report or a 3-month Type II report is likely the best option for your business. Going straight for a Type II report is recommended since more customers are refusing a Type I report. If your customers include finance or insurance companies, they may require a Type II report to work with you.

### Establishing a SOC 2 Project Plan

Get Buy-in Across Your Organization

Form a SOC 2 Leadership Team

Define Audit Scope

Write Policies and Processes

Implement Technical Configurations and Controls

Conduct a Readiness Assessment

### SOC 2 Policies and Procedures

### SOC 2 Compliance