The Essential Guide to SOC 2:

What It Is and Do You Need It?

CYBERGUARD COMPLIANCE

Table of Contents

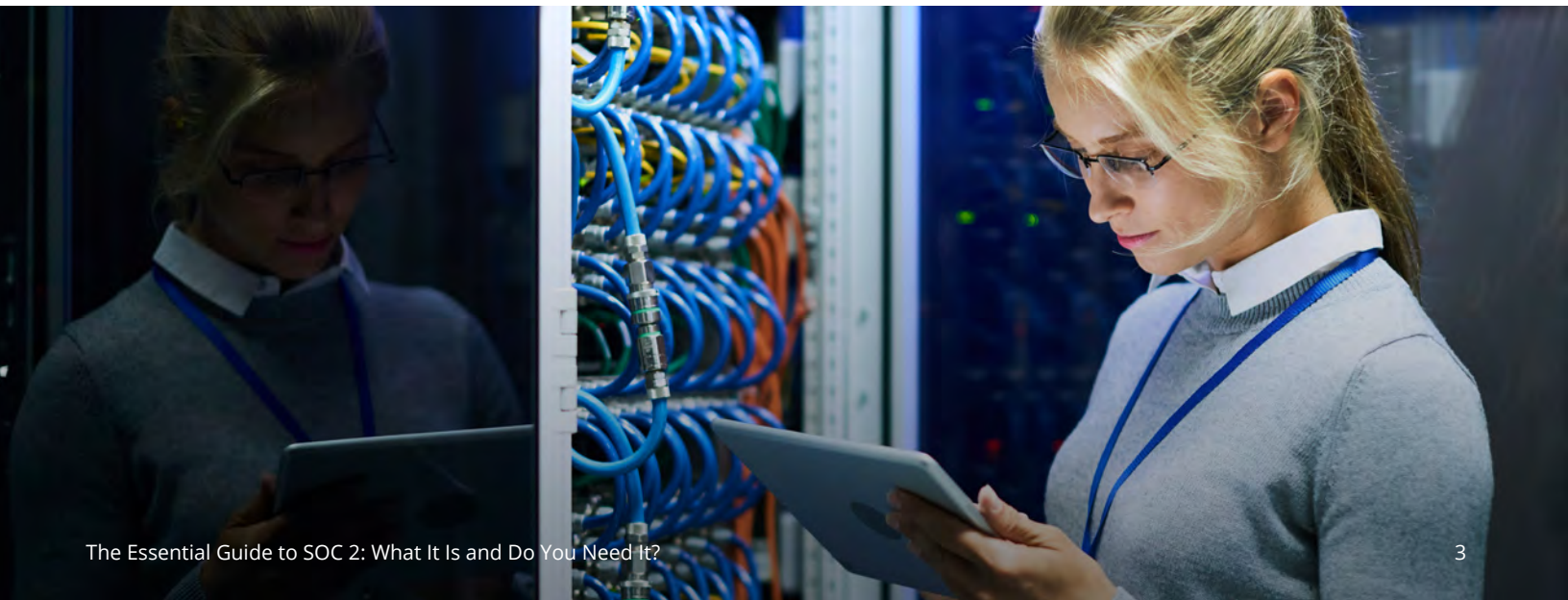
Introduction

Data breaches are bad for business. Even the possibility of one can scare away customers.

The bad news is, the more a company relies on third-party vendors, the more the company is at risk of a costly data breach. Twenty-eight percent of organizations using one to five vendors had to manage public scrutiny after a breach. Eighty percent of companies that used more than 50 vendors experienced reputation-damaging breaches, according to the Cisco 2018 Annual Cybersecurity Report.

All told, 55 percent of the respondents to Cisco's survey reported having to manage public scrutiny stemming from a breach in the past year. Cisco reported that 53 percent of all attacks resulted in damages exceeding $500,000, including lost revenue, customers, opportunities, and out-of-pocket costs. Finance, operations, intellectual property, and brand reputation were most commonly affected.

As cybercrime damages mount, companies want their third-party vendors to prove that they are properly protected by completing a SOC 2 audit.



While you could forego a SOC 2 audit and turn down potential customers who want one, it would be more beneficial for your company to undergo an audit, not only so you can grow your business with new customers, but also to provide the peace of mind that comes with the confidence of knowing you have a solid internal control environment.

In verifying that you comply with requirements related to vital concerns such as security, availability, processing integrity, confidentiality, and/or privacy, a SOC 2 audit provides the assurance that existing clients and prospective customers need when doing business with your company.

Data breaches are bad for business. Even the possibility of one can scare away customers.

Besides, companies' legal teams often require them to include a SOC audit in the request-for-proposal process for vendors. If your company plans on handling customer data, your potential customer wants assurance from an independent CPA firm that their data will be protected, instead of just relying on your word that it is secure.

Also, with cybercrime damages projected to increase to $10.5 trillion annually by 2025, according to research firm Cybersecurity Ventures, regulators keep tightening compliance. This is meant to protect consumers and companies from data breaches like those which have previously exposed sensitive information, such as medical histories, credit card information, and Personally Identifiable Information (PII).

Such data breaches result in:

- Reputational damage
- Loss of intellectual property
- Disruption of key business operations
- Fines and penalties
- Litigation and remediation costs
- Exclusion from strategic markets

A SOC 2 report from an independent auditor shows your clients that your systems are protected against data breaches and that their data is safe with your company. In getting a third party to provide an opinion saying, "Yes, XYZ company has successfully passed the SOC 2 audit," you will earn trust more quickly and get clients more easily.

Additional benefits of a SOC 2 report include:

- Credibility
- Competitive advantage
- Satisfaction of contractual requirements
- Reduction of regulatory compliance efforts
- Increased return on investment (ROI)
- More trust and transparency
- Greater investor confidence

A SOC 2 report positions your company for success by helping you show customers how you mitigate risk and improve your service organization's internal control environment.

What Is a SOC Audit?

The American Institute of Certified Public Accountants (AICPA) created three types of Service Organization Control (SOC) reports: SOC 1, SOC 2, and SOC 3. Each of these reports vary in focus and purpose.

- SOC 1 Audits: A SOC 1 audit covers an organization's internal control over financial reporting (ICFR). In doing so, it positions your organization for continued growth, client confidence, and the ability to serve a broader range of clients. SOC 1 audits have a proven and strong ROI.

- SOC 2 Audits: A SOC 2 audit details the controls of the systems used to process data and the security and privacy of that data. It is officially known as a Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

- SOC 3 Audits: Unlike SOC 1 and SOC 2 audits, which are restricted use reports, a SOC 3 audit is a general-use report. It can be freely distributed or posted on a website for one full calendar year from the date of issue. Companies may choose to undergo a SOC 3 audit when a SOC 2 audit is not appropriate. Or, more than likely, the SOC 3 audit is performed in conjunction with the SOC 2 audit.

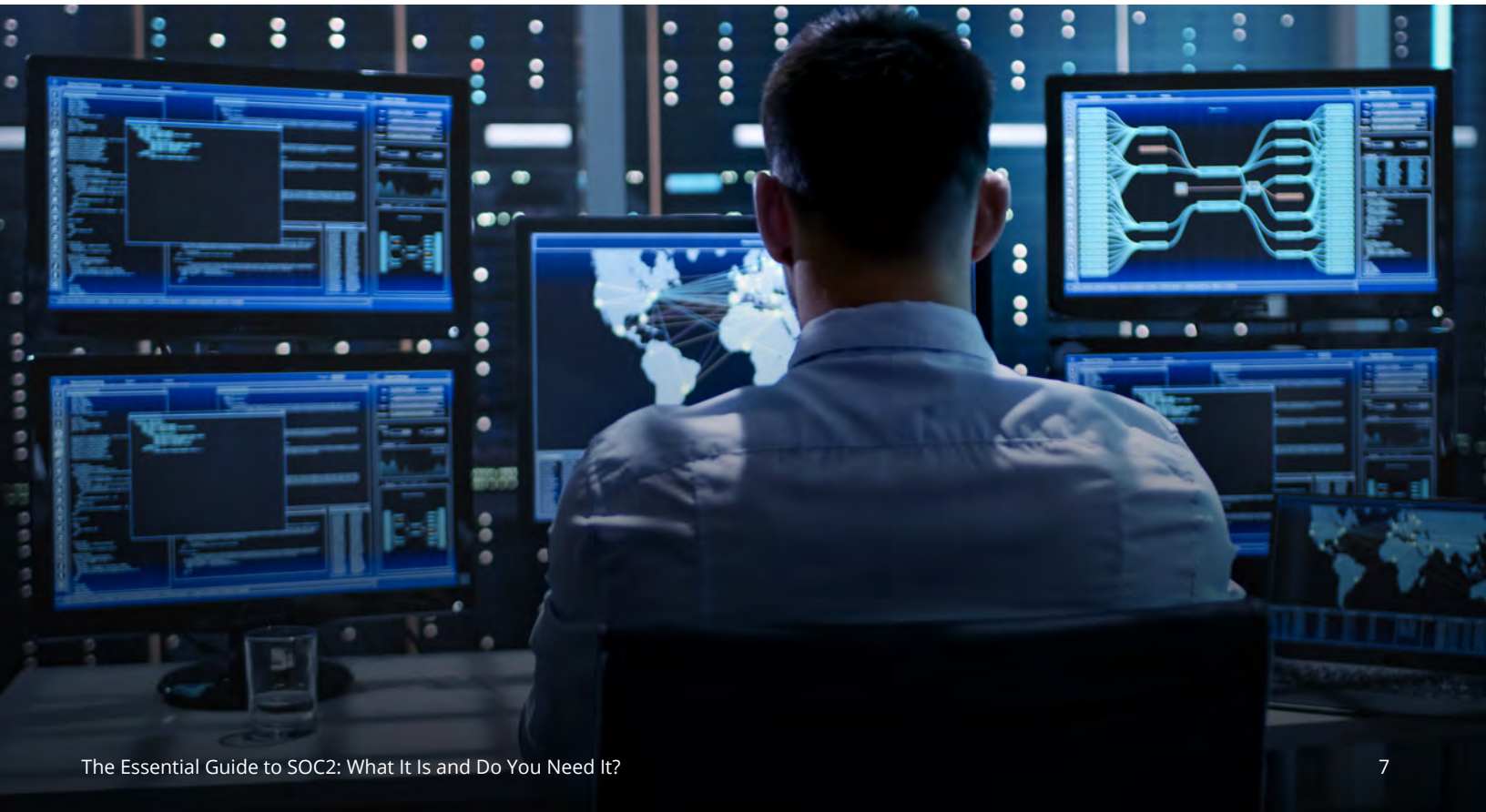
  Like SOC 2 audits, the scope of SOC 3 reports can include one or more of the following: security, availability, processing integrity, confidentiality and/or privacy.

What Is SOC 2?

SOC 2 audits are best for companies providing services that do not impact a client's ICFR.

The AICPA created SOC 2 audits to meet the needs of a range of users that need detailed information and assurance about a service organization's controls, including managers, customers, regulators, business partners, and suppliers. These reports can play an important role in:

- Vendor management programs
- Internal corporate governance and risk management processes
- Organizational oversight
- Regulatory oversight



SOC 2 audits focus on controls at a service organization relevant to the following five Trust Services Criteria.

Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Availability: Information and systems are available for operation and used to meet the entity's objectives.

Processing Integrity: System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Confidentiality: Information designated as confidential is protected to meet the entity's objectives

Privacy: Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

Companies can choose which criteria to apply (and how) when preparing for a SOC 2 audit. Consider your overall control environment and review key business operations to ensure criteria are comprehensive, objective, and complete. Current documentation of procedures and controls will be required to complete the audit.

Scoping a SOC 2 Audit

Your company may need an IT compliance audit because customers often require vendors to provide SOC 2 reports to better protect against the type of data breaches that extract significant costs financially and reputationally. Passing a SOC 2 audit will help your company continue to serve its customers while minimizing the risk associated with a cybersecurity breach.

The scope of your SOC 2 report will depend on the five core Trust Services Criteria you will need to focus on to meet your customer or compliance requirements.

At minimum, the AICPA requires your company to undergo the Security TSC when performing a SOC 2 audit. Ideally, this is all you should do during your first SOC 2 audit. Otherwise, the cost and additional level of effort to add other TSC may be overwhelming the first time through the process.

But if customers require you to include more than Security, you should work with customers and auditor to identify which Criteria to add on top of Security. Typical companies who perform SOC 2 audits include one or two Criteria. Only a very small percentage of service organizations undergo all five Criteria.

Consider which Criteria most closely relate to your customers' concerns. For example, if you store data but don't process it for clients, then availability may be applicable but processing integrity would not.

Compliance software provider Reciprocity also suggests that you consider how many systems, policies, and procedures you can effectively evaluate when scoping a SOC 2 audit.

SOC 2 Type 1 and SOC 2 Type 2 reports can be issued depending on your specific requirements and objectives.

Type 1: This is a report on your description of your system and the suitability of that system's design. A Type 1 report describes systems related to a point in time. Think of it as a snapshot.

Customers will commonly accept a Type 1 report for your first report. You also will be allowed to remediate any gaps prior to the report's issuance. Such reports can be used to get an audit report in hand much sooner than a Type 2 audit.

Type 2: This is a report on your description of your system, the suitability of that system's design, and the operating effectiveness of its controls. Think of a Type 2 report as a movie. It covers systems over a period of time.

This is the gold standard that customers prefer. Customers typically will require you to undergo the Type 2 audit for the greater level of assurance it provides.

A readiness assessment should precede your first audit to increase likelihood to pass and to create efficiencies in your audit process. Most first-time auditees follow the readiness assessment with a Type 1 report and then finish with a Type 2 audit six months later.

A Type 2 audit of a six-month period is often sufficient your first year. Once your first Type 2 audit is complete, all future Type 2 audits should cover a period of twelve months.

Choosing an Audit Partner

Auditors check for everything from industry best practices to security standards to government regulations. In issuing your security program a pass or fail, auditors examine your policies, infrastructure, and practices. They identify your strengths as well as ways to improve, in regard to complying with specific standards and regulations.

> ***The right auditing partner will help you improve your business, as well as your security, by addressing operational and technical areas of risk.***

The right auditing partner will help you improve your business, as well as your security, by addressing operational and technical areas of risk. You can also build a relationship in which the auditing partner can help you identify and work toward improvements between audits, which may vary in frequency. These auditors can clearly communicate the steps you must take to improve and help you measure progress toward your goals.

Given that your auditor will determine whether or not you meet the auditing requirements, you should pick one with ample experience and a good reputation. Qualifications are important because your organization's reputation is at risk.

Don’t pick based on price alone. The cheapest firm may be the least experienced and qualified. Companies lacking experience with a SOC 2 audit may offer the lowest price but then provide poor service.

If a CPA firm registered with the Public Company Accounting Oversight Board (PCAOB) conducts your SOC 2 audit, both your management team and your clients can rest assured that your auditor will be held to the strictest of auditing standards. If you have publicly held clients, the fact that your company's audit was performed by a PCAOB-registered CPA firm will give your clients the comfort they need when relying on your audit report.

Follow this process to choose the best auditing firm for your organization.

- Confirm that the auditing firm conducts the audits you need.
- Assess the individual/collective experience of the auditing firm.
- Find out which certifications the auditing team holds.
- Check whether the firm is registered with the PCAOB.
- Determine if the firm has a strong reputation for being timely and responsive.
- Review the firm's pricing structure.
- Learn the firm's auditing approach.

Complying with SOC 2

Though the scope of your SOC 2 audit will be tailored to your organization, adhering to cybersecurity best practices in the following general areas will help you comply. These are four things to know about SOC 2 compliance.

1) Monitoring

Protecting customer data begins with knowing what you know and what you don't know. You must know how your systems work when working properly in order to know what to look for when they are not. Customers also want to know that you are watching for threats and how you're doing it.

2) Alerts

Customers also want to see that you will be quickly alerted to any threats so that you can respond promptly should their data be potentially compromised. Showing how you receive alerts for risks like unauthorized access, file transfers, exposure of data, controls, or configurations is crucial to assuring customers of the safety of their data.

3) Audit Trails

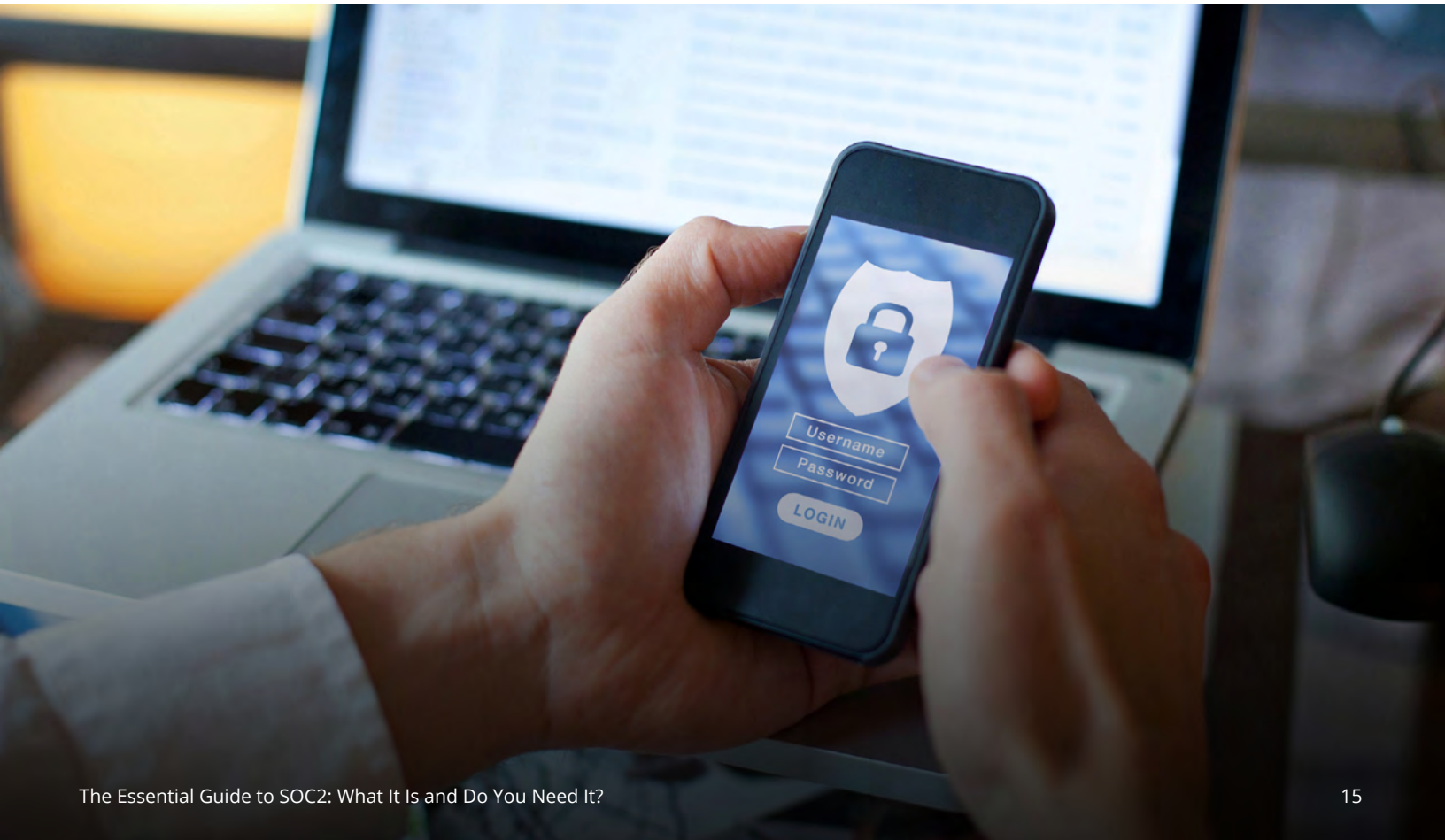
If a security incident occurs, tracing the where, when, and how of the attack lets you focus your response. Audit trails also help you determine the impact of the attack. Knowing this, you can limit damage from the incident.

4) Forensics

Learning from incidents will help you protect against similar threats in the future, establishing efficient processes for compiling all of the actionable data from an attack, like which parts of your systems were impacted and how it helps you make corrections. Customers want confirmation that you can do so.

Detailing your abilities to identify, respond to, and remediate cybersecurity threats in a SOC 2 report assures customers that their data is safe. A SOC 2 audit will help you prove that customer data is secure and protected against data breaches.

Having third-party verification of your security in a SOC 2 report will give you a competitive advantage as well. You can compete for and win more business by providing prospective clients the assurance that they seek.



CYBERGUARD COMPLIANCE

Want to learn more about a SOC 2 audit for your organization? Contact us for a free consultation regarding your audit needs.

CONTACT US