verbit

What is SOC 2 Compliance?

The nuts and bolts of what business leaders should know

Every business leader who works with vendors and partners should be aware of SOC 2 compliance. To appreciate the importance of SOC 2 compliance, business professionals can consider recent headlines like this one from The Wall Street Journal: "T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their security is awful.'"

No company wants that kind of press coverage. While business leaders may believe their company's security is up to snuff, they're likely sharing information with various vendors.

Contracting with outside partners may expose sensitive or private data and information to cyber-attacks and breaches. Weak links can cost millions of dollars and tarnish a brand's reputation. Enter the American Institute of Certified Public Accountants (AICPA) SOC 2 reports.

Corporate leaders should take a moment to learn what a SOC 2 report means, as well as why it's critical to ensure their partners are taking the proper steps to avoid a data breach.

Breaking Down SOC 2 Reports

A SOC 2 report is a document that details a vendor's security and risk management practices. The AICPA created SOC 2 to specifically address security related to service providers who store data on the cloud, including nearly all Software as a Service (SaaS) providers.

There are two types of reports:

- Type I: This report covers the company's security policies but doesn't test them. It's easier and faster to acquire but less reliable.
- Type II: It can take a few months or even a year to complete a Type II report. Not only will this include the security protections in place, but the audit will test them and disclose how effective those measures are in practice.

Reports Will Look at Trust Service Criteria

Five categories make up the Trust Service Criteria. While the security category is mandatory in all reports, the others are optional and may not apply to all business types.

1 Security

As the AICPA defines it:

"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 achieve its objectives."

Why it's included:

Every report will include this mandatory category. It addresses the protection of data from its creation or acquisition through storage or deletion. Security might involve endpoint protection and system monitoring to identify unauthorized users.

2 Availability

As the AICPA defines it:

"Information and systems are available for operation and use to meet the entity's objectives."

Why it's included:

If downtime for the system would be a problem for clients, then availability might be a good category to include in a SOC 2 report.

3 Processing Integrity

As the AICPA defines it:

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

Why it's included:

This matters for entities whose customers use the system for data processing or financial processing.

4 Confidentiality

As the AICPA defines it:

"Information designated as confidential is protected to meet the entity's objectives."

Why it's included:

If a company is storing data that it is contractually obliged to delete or that a nondisclosure agreement protects, the report should include this category.

5 Privacy

As the AICPA defines it:

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

Why it's included:

This criterion is similar to confidentiality but addresses personal information. If the business maintains HIPAA-protected data or similar private information, this category will be essential for the report.

When reviewing a SOC 2 report or certification, business leaders will want to know whether they are looking at Type I or Type II reports. Also, addressing the Trust Service Criteria can ensure that vendors maintain protections that apply to their use cases.

verbit

As more businesses look to become inclusive and meet necessary accommodations for employees and consumers, many are turning to tools like captioning, **transcription**, audio description and subtitling. Verbit provides all of these solutions and meets SOC 2 Type II and HIPAA compliance. **Contact us** to learn how our tools are helping corporations and small businesses alike to protect sensitive information, while also offering vital accessibility services.