protranslating
A BIG LANGUAGE COMPANY

Visit protranslating.com
Call (305) 371-3972
Email info@protranslating.com

SOC 2 Type II Reports: **How to Correctly Assess a Vendor**

eBook

eBook

SOC 2 Type II Reports:

How to Correctly Assess a Vendor

Contents

Introduction

Companies have been collecting your personal data for decades. When Starbucks first began, for example, the baristas would write down every customer's order and add it to a filing system. That way, when the customer returned at a later date for another coffee, the baristas could reference the previous order and improve their level of service by anticipating the customer's needs. With the arrival of the internet in 1991, digital data collection went into overdrive, and hasn't slowed down since.

In the '90s, privacy advocates began to raise concerns about companies like Lotus MarketPlace and DoubleClick, as over 30,000 people had filed complaints against them. But this number accounted for only a tiny portion of the US population (just over 0.01%). Today, according to Internet Society and Consumers International, more than 69% of consumers are concerned about how their personal data is collected through mobile apps.

Looking back at 2020, it's evident that it's becoming increasingly difficult for consumers to ignore the importance of data protection. In 2020 alone, the US experienced just over a thousand data breaches and 155.8 million individuals were affected by data exposures, meaning that their sensitive information was accidentally exposed due to inadequate information security. As a result of the increasing public concern surrounding data security, businesses that process, store, and transmit data have taken steps to show that they take this responsibility seriously and have the relevant controls in place to ensure data security. How can consumers and businesses who want to work with a company like a language service provider (LSP) know that the company's data security claims are valid?

One of the best ways to ensure that the LSP you are working with is highly focused on security is to confirm that they are SOC 2 Type II compliant. Systems and Organization Controls for Service Organizations 2 (SOC 2) is a framework to determine if an organization's controls and practices safeguard the data security of its customers and clients. There are various SOC audits, but SOC 2 Type II reports address the posture of a company during a whole year in the important areas of confidentiality, integrity, availability, security and privacy. SOC 2 Type II reports have numerous benefits for language service providers and the organizations collaborating with them.

Comparing SOC 1, SOC 2 and SOC 3

There are three types of SOC reports, and all of them detail a service provider's control over their client data. Each SOC certification requires certain client data protection policies.

Let's take a look at the three types of SOC reports:

SOC 1	reports deal with the vendor's internal controls over financial reporting.
SOC 2	reports cover the examination of the controls of a service organization over one or more of the five categories of Trust Services Criteria (TSC): Security, Availability, Processing Integrity, Confidentiality, and Privacy.
SOC 3	is a summarized report of the SOC 2 Type II report, but is a less technical and detailed audit report, and can be widely shared.

Each SOC report comes in two different types:

Type I

reports focus on procedures and policies set in motion over a specific moment in time.

Type II

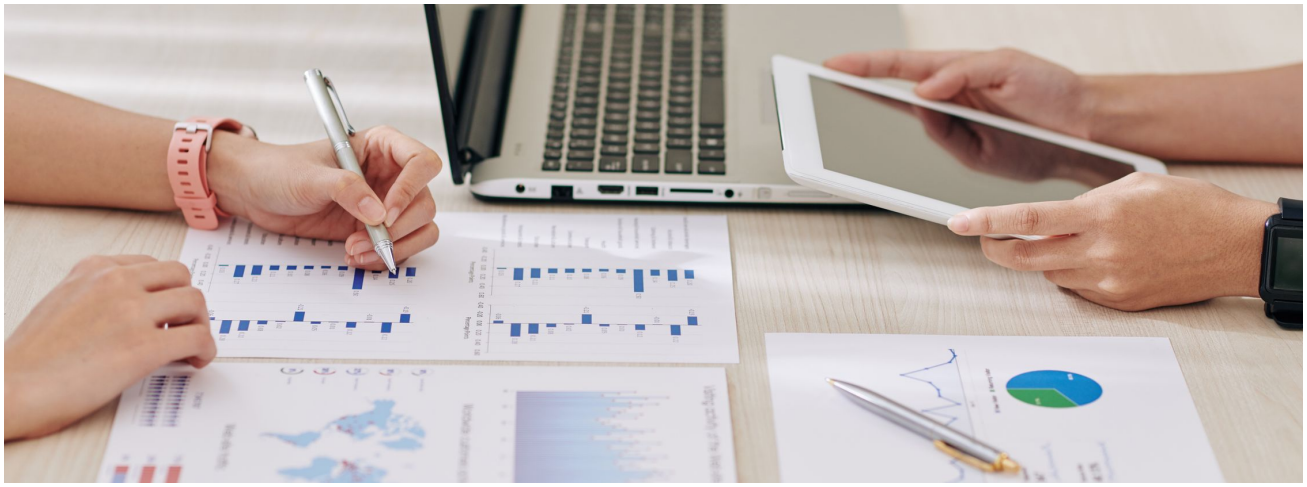
reports focus on the same procedures over a specified period. This is the more rigorous auditing procedure, wherein systems are evaluated for a minimum of six months. SOC 2 Type II is therefore the most comprehensive report for reviewing a service provider's security infrastructure.

What is SOC 2 Type II Compliance?

SOC 2 Type II reports are increasingly critical for vetting vendors.

SOC 2 is a framework used to analyze a service organization's data management. More precisely, the framework is used to determine whether the service provider's controls and practices are robust enough to safeguard the security and privacy of the data they hold.

The SOC 2 framework can be applied to any service-providing enterprises and organizations that store and process client data. The distinction between the SOC 2 Type I and Type II frameworks is duration of time and effectiveness of the controls. For example, a SOC 2 Type I report audits procedures and practices at a given time and details management's description of a service organization's systems and the suitability of the design of controls.



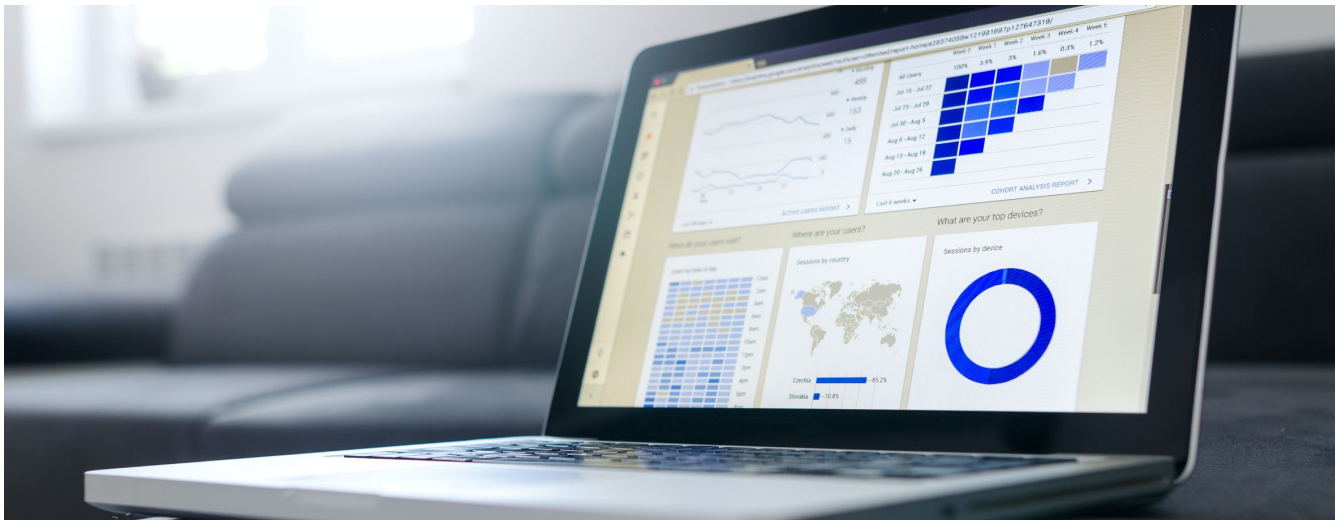
The SOC 2 Type II audit, alternatively, is carried out over six months or longer and provides more in-depth insight into ongoing practices and infrastructure, offering a more comprehensive picture. And, just as with SOC 2 Type I reports, the SOC 2 Type II report also details management's description of a service organization's systems and the suitability of the design and operating effectiveness of their controls. Risk assessment is crucial for any organization's vendor management as third parties are a common source of security breaches. It is especially relevant when you are providing sensitive business and customer data to language service providers (LSPs).

How Does SOC 2 Type II Compliance Work?

The SOC 2 Type II audit can only be performed by a Certified Public Accountant (CPA) or CPA firm, and they must be independent of the organization they are auditing. The report is based on auditing information from five key categories:

- **Security**
- **Privacy**
- **Confidentiality**
- **Availability**
- **Data Processing Integrity**

The audit is used as part of a vendor security risk assessment. Of the three types of SOC reports, SOC 2 Type II is the most useful for vendor management because it audits IT and security-related controls over a six to twelve-month period.



SOC 2 Type II compliance requires service providers to demonstrate continuous adherence to the American Institute of Certified Public Accountants' (AICPA) security protocols. In 2011, the AICPA issued the Statement on Standards for Attestation Engagements No.16 (SSAE 16), which was updated to SSAE 18 and is used in SOC 2 audits today. This results in a more insightful report that ensures the security of the vendor. Completing a successful audit is proof that the business' security and compliance meets AICPA's Trust Services Criteria (TSC) industry-recognized third-party assurance standards.

Why is SOC 2 Type II Compliance Crucial for Your Cyber Security Protocol?

The SOC 2 Type II report is specifically designed to set forth requirements for secure IT functions and account for a service provider's physical and administrative security. According to AICPA, the report will detail requirements in the following categories:

Organizational oversight

Vendor management programs

Internal corporate governance and risk management

Regulatory oversight

The report provides insight into your data security and helps develop more efficient, technology-driven processes for service providers. Being SOC 2 Type II compliant is also a significant market differentiator that sets your brand apart from the competition. While SOC 2 Type II compliance can certainly attract new customers to your business and help to assure them of your adherence to specific best practices, most of the benefits of compliance are enjoyed by the clients you serve.

Brand Protection

SOC 2 Type II compliance protects the brand reputation of your service provider and consequently your own. You might be sharing highly-sensitive customer and operational data with your LSP. The SOC 2 Type II report aims to ensure that your data is handled according to industry standards.

Competitive Advantage

SOC 2 Type II certification represents a competitive advantage both for the service provider and their client. Choosing to work exclusively with SOC 2 Type II compliant vendors demonstrates your commitment to information security. With consumers becoming increasingly sensitive to data privacy, they are certain to gravitate toward companies who work with SOC 2 Type II compliant vendors.

Superior Risk Management

Risk assessment is critical when it comes to vendor management. There's no better way to assess the data safety protocols of your vendor than with a SOC 2 Type II report. The strict auditing requirements for SOC 2 Type II compliance ensure that your vendor meets the established security criteria to protect against unauthorized access. It serves as evidence that a third-party auditor rigorously tested the internal controls of the service provider.

In addition to addressing vendor security, SOC 2 Type II compliance also provides valuable insights on the most imminent cybersecurity risks. Vendors then use this information to improve and streamline their processes. Choosing a SOC 2 Type II compliant vendor will help you pick a secure organization that takes data security seriously.

The SOC 2 Type II report itself is just a start; reviewing the information correctly is crucial. You'll see exceptions mentioned by the auditor that highlight the service provider's weakest areas.

Ideally, the SOC 2 Type II report should have no exceptions noted. If exceptions have been identified, they should be thoroughly investigated and remedied. It's important to note that there's a significant difference between holding a SOC 2 Type II report as an organization, and the Amazon Web Service SOC 2 Type II reports of brands like Amazon and Google that focus on only one section of the overall company.

It's common to see service providers build their software or application with AWS (Amazon Web Services) or other platforms. However, just because AWS has a SOC 2 Type II report doesn't mean that the LSP shouldn't have their own. An AWS SOC 2 Type II report only covers the controls that AWS is responsible for. It doesn't offer assurance of the controls that the service provider is responsible for. Therefore, your service provider should always hold their own SOC 2 Type II report to ensure all their security controls and protocols are covered

Always Request a SOC 2 Type II Report from Your Vendor

You may have all your security protocols in place, but this isn't necessarily enough to keep your data protected. Global brands tend to outsource entire functions to service providers to increase efficiency and profitability. This rising trend toward outsourcing has created new opportunities for cybercriminals and unknown risks for your organization. To ensure that your company and client data are protected from data breaches, check that your service provider is SOC 2 Type II compliant.

Here are three of the main ways SOC 2 Type II compliance protects you and your vendor from cyber attacks:

1. Extensive Audits

Auditing confirms the integrity of a vendor's organizational processes and systems. The SOC 2 Type II reports are the most comprehensive audits on data security standards.

A SOC 2 Type II audit provides a deep dive into a vendor's data protection practices, while offering insights on improving crucial system components. This enables service providers with a good IT infrastructure to continuously improve their protocols and prove the vendor's compliance with AICPA's TSC guidelines.

2. Active Monitoring and Real-Time Alerts

Active monitoring is one of the critical features of SOC 2 Type II compliance. Systems and processes are always being monitored, and any anomalies in the activity surrounding your sensitive data are detected. SOC 2 Type II compliance demands that companies monitor anomalies related to file transfers, account logins, configurations, and data modifications. This creates a solid framework for developing appropriate alert procedures. Real-time alerts will immediately notify you of suspicious activity. This will enable you to respond effectively to threats to your data integrity. With monitoring, you'll be notified about any attempted cyber attacks as they happen in real-time.

3. Cybersecurity Framework

SOC 2 Type II compliance requires that vendors keep their data environment secure, using real-time, actionable data.

Using the compliance module's auditing, tracking, and real-time alerts, vendors can quickly strengthen their protocols against cyber threats. The data from the audit can prove invaluable in fortifying their infrastructure.

Key Components of a SOC 2 Type II Report

To understand how to conduct a vendor review, you first need to identify the key components of the SOC 2 Type II reports. The report consists of seven areas:

1. **Assertion:** An in-depth description of the service provider's system controls.
2. **Independent Service Auditor's Report:** The extent to which the service provider's system controls meet the SOC 2 Type II criteria.
3. **System Overview:** A brief overview of the vendor's background in the industry.
4. **Infrastructure:** The data environment (software, procedures, data management tools, and personnel) responsible for managing internal processes.
5. **Relevant Control Aspects:** How internal work environments are controlled to minimize risk and optimize control management.
6. **User-Entity Controls:** An assessment of the client-facing controls required to meet control objectives.
7. **Trust Services Criteria, Related Controls, and Test of Controls:** This is the report's final section. It details the testing progress and the extent to which the controls meet the security criteria.

These are the fundamental elements of the report. For further reference, an illustrative SOC 2 Type II report issued by AICPA can be found here.

How to Conduct a Thorough Vendor Review

When reviewing your vendor's SOC 2 Type II report, there are the four key areas to focus on:

Section 1 - Who Issued the Report?

When you're verifying who issued the report, there are two key points to focus on.

First, ensure that the auditor was from a licensed CPA firm, as stipulated in AICPA regulations. This means that the firm has undergone peer reviews of their accounting and auditing practices every three years in order to uphold AICPA's auditing standards.

Second, your vendor's report should come from a CPA firm that specializes in information security. Given that SOC 2 Type II reports are cyber security based, they are different from the regular financial audits of CPA firms. It's best when the firm's personnel holds either CISSP, CISA, or CRISC, among other relevant cyber security certifications.

Section 2 - The Auditor's Opinion

The Auditor's opinion is one of the most critical sections of the report. In their report, you'll find their assessment of the vendor's system, system description, and controls. Based on the outcome, the auditor's opinion will be categorized in one of four ways:

Unqualified	Qualified	Adverse	Disclaimer
The auditor fully supports the vendor's system with no modifications.	The auditor cannot express an unqualified opinion; however, the issues weren't significant.	The auditor believes that there are material and pervasive issues. This means that the vendor's system is unreliable.	The auditor believes that there are material and pervasive issues. This means that the vendor's system is unreliable.

You should seek out vendors that have received unqualified opinions in their reports. If there's a different opinion, you should consult the area of the report describing the reason behind it and weigh the risks for your organization accordingly.

Section 3 - System Overview and Background

The third section of the report is the vendor's description of their system. You'll find details about background information, software descriptions, procedures, people who have access to systems, and specifics about their data management.

Section 4 - Test Controls and Results

The SOC 2 Type II report will include the exceptions found during testing. This is an important area of the report. This section will help you decide which of the vendor's controls are essential for your organization. Assess any exceptions that were noted for those areas. Any exceptions that could impact your organization's data security should be carefully assessed. Exceptions that don't affect your company data and won't potentially put it at risk will still need careful consideration to determine whether the vendor can be a reliable and trusted partner.

Never Choose a Service Provider Without a SOC 2 Type II Report

Security should always be a priority when you're looking to outsource translation and localization projects. Not every business is willing to invest the necessary time, effort, and resources required for a SOC 2 Type II audit.

Your language service provider will be handling your highly-sensitive business and customer data. Your security protocols may be excellent, but a breach by your LSP may mean your data is compromised. The challenge is that your data is your responsibility, even while it's in the hands of your language service provider.

Don't risk damage to your brand and corporate reputation. Always insist on a SOC 2 Type II report from your LSP. Working exclusively with vendors who adhere to AICPA's security standards will protect both you and your customer's data security, while also instilling confidence that your LSP takes both your, and their, security seriously.

If you're looking for a SOC 2 Type II compliant LSP, we can help. At Protranslating, we prioritize security within our workflows and are the only LSP in the world that holds a SOC 2 Type II report through AICPA.

Get in touch with us today to learn all about our commitment to data privacy and industry-leading security protocols.

Contact Us Today

BIG LANGUAGE SOLUTIONS

ISI Language Solutions · protranslating · BIG IP & LEGAL SOLUTIONS · LANGUAGE LINK · D·W·L

SECURE. UNIFIED. EFFECTIVE.

Our family of companies includes BIG IP, ISI Language Solutions, Protranslating, Language Link, and DWL, bringing over 150 years of combined expertise with offices in 26 locations worldwide. Through our portfolio, we customize and deliver language services in more than 240 languages and dialects.