MOORE ClearComm

-

What organisations require a SOC 2 Audit?

A SOC 2 audit is typically required for service organisations that store, process, or transmit customer data. This is particularly important for businesses that handle sensitive or confidential information. Here are a few examples of the types of companies that might require a SOC 2 audit:

1. Software as a Service (SaaS) Providers

SaaS providers typically handle vast amounts of customer data. Whether it's a CRM platform managing customer interactions or a project management tool tracking task completion, SaaS companies often have access to sensitive business data that must be protected.

2. Cloud Computing Companies

Cloud service providers, including those offering Infrastructure as a Service (IaaS) or Platform as a Service (PaaS), are responsible for protecting the infrastructure that hosts and processes customer data. Given their role in managing important infrastructure, these companies often require SOC 2 reports to demonstrate their commitment to security.

3. IT Service Providers

Companies providing IT services, including managed services, data centre services, and IT consulting, often have privileged access to their clients' systems and data. As such, these companies usually need a SOC 2 report to demonstrate that they have adequate controls in place.

4. Financial Services Companies

In the financial sector, businesses are often required to demonstrate compliance with a range of regulatory standards. A SOC 2 report can help these companies prove that they're managing financial data securely.

5. Healthcare Providers

Healthcare providers and related businesses often handle highly sensitive patient data. As such, they may need a SOC 2 report to demonstrate their commitment to data privacy and security.

6. Payment Processors

Payment processors handle sensitive financial information and, therefore, must have robust security measures in place. A SOC 2 report can help these companies demonstrate their compliance with industry standards.

7. Data Analytics Companies

These companies gather and process substantial amounts of data to provide insights to their clients. To assure clients that the data is secure and used properly, these companies often require SOC 2 compliance.

Summary

Any company that handles sensitive customer data, particularly if that data is entrusted to them by another business, should consider obtaining a SOC 2 report. However, SOC 2 isn't only for large companies or those in certain industries. Any organisation that wants to demonstrate its commitment to data security and privacy can benefit from SOC 2 compliance.

About Us:

Moore ClearComm is part of Moore Kingston Smith, a dynamic, leading professional UK firm of accountants and professional business advisers.

Our services include Data Privacy, Cyber Security, Business Continuity and Information Security for organisations worldwide.

As trusted advisers to businesses and not-for-profit organisations, we are passionate about helping our clients achieve their ambitions. Our highly experienced people have the strategic insight, drive and dedication to deliver results and help mitigate Data Privacy and Cyber Security risk.

As part of Moore Kingston Smith, a leading member of the Moore Global Network. An international family of over 30,000 people across more than 100 countries, members connect and collaborate to care for our clients’ needs – at a local, national and international levels.

#SOC 2 London

Contact us: info@mooreclear.com

www.mooreclear.com