The What and Why Behind SOC 2

CARET Legal

What is SOC 2?

All organizations – particularly those that outsource crucial business operations to third-party technology businesses and SaaS companies – must ensure that their data is handled properly, protecting customers from data theft, extortion, and malware attacks. Service Organization Control 2 (SOC 2) provides a framework to help stakeholders ensure that vendors protect the interests of the company they serve and the personal data of vulnerable clients.

Being SOC 2 compliant has many benefits. Among them, it helps assure your customers and clients that you have the infrastructure, tools, and processes in place that will protect their personally identifiable information (PII) from unauthorized access coming from inside and outside the organization.

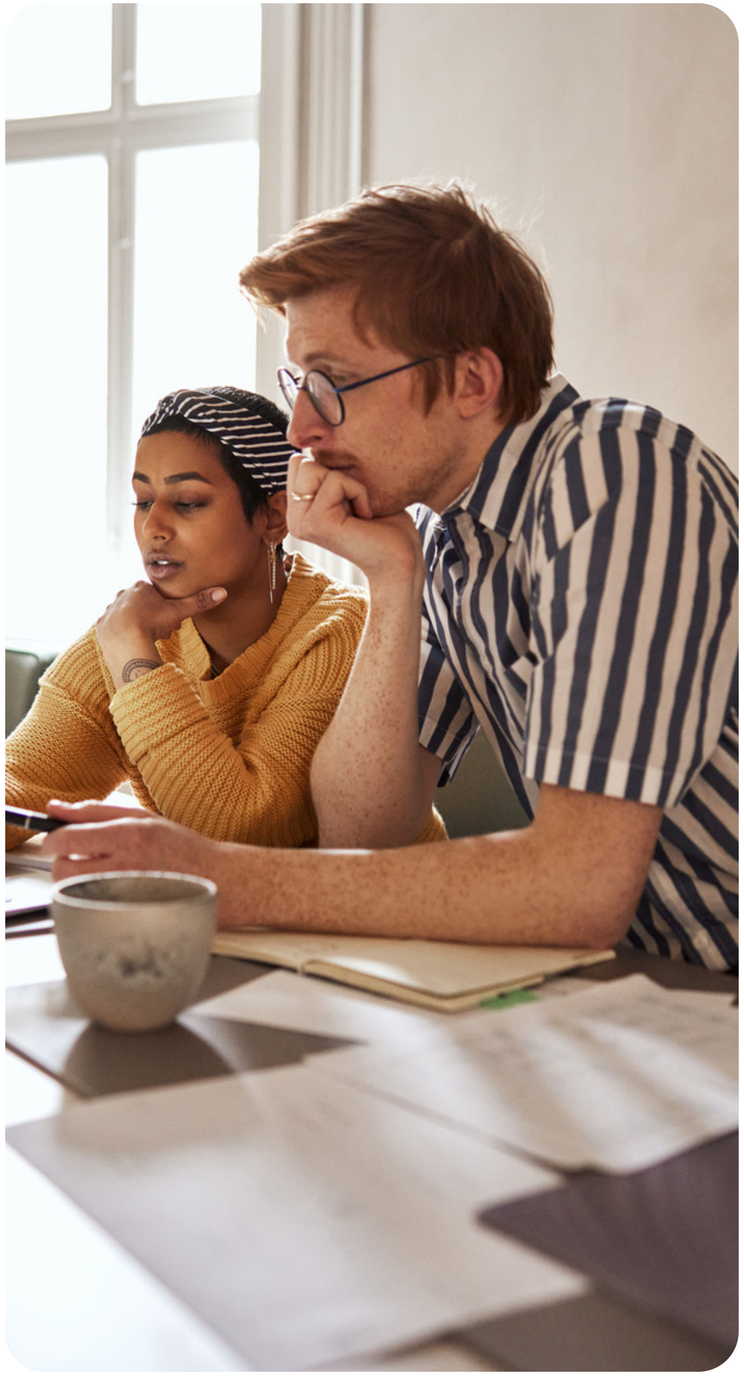
SOC 2 is an auditing process developed by the American Institute of CPAs (AICPA) to help ensure that service providers manage data securely to protect organizations and maintain client privacy. SOC 2 requires organizations to establish and follow strict information security policies and procedures surrounding the five "trust service categories" regarding customer data:

- **Security.** The security category assesses the level of protection of system resources against unauthorized access. Security tools like web application firewalls, two-factor authentication, and intrusion detection are proven ways to prevent security breaches that may lead to unauthorized access to systems and data.
- **Availability.** The availability category examines the accessibility of the system, products, or services as outlined in the contract or service level agreement (SLA) using security-related criteria such as network performance, site failover, and security incident handling.
- **Processing integrity.** This category monitors the integrity of a data processing system to determine whether it is performing in a complete, valid, accurate, timely, and authorized manner.
- **Confidentiality.** The confidentiality category encompasses the access and disclosure of sensitive information. Encryption, network and application firewalls, and thorough access controls should all be used to safeguard information processed or stored on computer systems.
- **Privacy.** The privacy category reviews how the system collects, uses, retains, discloses, and disposes of personal information under the AICPA's generally accepted privacy principles and determines whether controls are in place to protect clients' PII from unauthorized access.

Generally, any organization that handles customer data is encouraged to be SOC 2 compliant. Some industries that have a need for a SOC 2 report include:

- Cloud computing
- Legal
- IT security management
- Software-as-a-Service (SaaS) vendors
- Insurance claims processing
- Medical claims processing
- Financial processing
- Customer relationship management (CRM)

SOC 2 reports provide valuable information about your organization for an informed audience that typically has a vested interest in the audit's findings.



Why Require SOC 2

SOC 2 compliance is not mandatory. However, many companies require SOC 2 compliance from their service providers because it provides various people-related benefits:

- **Customer satisfaction.** Protecting their data from unauthorized access is most likely a priority for your clients, and without SOC 2 attestation, they could lose confidence in your firm.
- **Cost control.** According to a recent report by IBM and the Ponemon Institute, the average cost of a data breach in 2021 was $4.24 million, and $1.07 million higher when remote work was a factor. A SOC 2 audit is a proactive measure that helps organizations avoid costly security breaches.
- **Competitive advantage.** Choosing SOC 2 certified solutions gives your firm an edge and provides clients peace of mind when considering your firm over competitive law firms that use non-certified vendors.
- **Security.** Successfully passing a SOC 2 audit helps guarantee company management that data is being collected, used, disclosed, and disposed of securely. According to the IBM report, customer PII was the most common (and expensive) type of record lost or stolen in a data breach.
- **Value.** A SOC 2 report provides critical insight into a company's risk and security position, vendor management, internal governance, and regulatory oversight – valuable information for those inside and outside the organization.

CARET Legal

SOC 2 reports provide valuable information about your organization for an informed audience that typically has a vested interest in the audit's findings. Although obtaining SOC 2 compliance can be a long process requiring teamwork, advanced planning, goal setting, collaboration, and much more, the peace of mind gained from addressing cybersecurity risks is well worth the effort. In addition, once you've obtained SOC 2 compliance, following up with annual audits will save you time, money, and lost sleep.

CARET Legal is the first cloud-based, end-to-end legal practice management platform to achieve SOC 2 compliance, delivering the highest levels of security, confidentiality and privacy to our clients. Our infrastructure resides at industry-leading facilities in the United States which have achieved compliance with an extensive list of global quality and security standards, including PCI DSS.

To learn more about CARET Legal's state-of-the-art security protocols and procedures, review our standards and meet with a specialist.