SOC 2 vs. PCI DSS Compliance

In the era of rising technologies and increasing dependencies on network systems, on-line information security could be a massive concern for any individual/organization, particularly those who source their key business operations to third-party shoppers (such as Software-as-a-Service cloud-computing providers). Any event of knowledge mishandling, particularly the information with application and network security suppliers, will reveal vulnerabilities resulting in information thieving and malware misconduct.

Many organizations are unsure on the distinction between a SOC 2 (System and Organization Control) report and PCI DSS (Payment Card business knowledge Security Standard) compliance. However, the two might have overlapping areas of focus, they're quite completely different. A PCI DSS compliance is restricted to businesses that settle for card payments and SOC 2 covers a broader vary of organizations that hold, store, and/or method client data. Neither standard is required by law, but non-compliance with either one has considerable consequences.

SOC 2 Reporting

SOC 2 reports are comprehensive reviews of your organization's data security controls, in line with the standards determined by the American Institute of Certified Public Accountants (AICPA). The trust services criteria of the SOC 2 are derived from five Trust Service 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 use 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.

The TSC that must be included in a SOC 2 report is Security (also known as the Common Criteria). Other TSCs (Availability, Confidentiality, Processing Integrity, and Privacy) can be included at the discretion of management at the service organization depending on the criteria applicable to the organization's system and services. The service auditor can also assist management in determining what criteria are applicable once the scope of the examination has been set.

Generally, SOC 2 examinations are performed by a licensed CPA auditing firm with experience in Information Security audits.

PCI DSS Certification

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards established jointly by American Express, VISA, MasterCard, Discover Financial Services and JCB International. The certification aims to secure credit and debit card transactions against possible data theft and fraud. It helps protect sensitive data, and assist businesses in building a trust relationships with customers.

PCI-compliant security services provide businesses data security standards, and enables customers know that their personal data is protected. A PCI compliance is known for offering secure transactions to its customers.

PCI compliance consists of four levels based on the total number of card supported transactions for business processes on an annual basis. The classification level determines what an enterprise needs to do to remain compliant.

- Level 1 – Applies to merchants processing more than six million real-world credit or debit card transactions per year. They must undergo an internal audit once a year and must perform a PCI scan by an Approved Scanning Vendor once a quarter.
- Level 2 – Applies to merchants processing between one and six million real-world credit or debit card transactions annually. They're required to complete an assessment once a year using a Self-Assessment Questionnaire. In addition a quarterly PCI scan may be required.
- Level 3 – Applies to merchants processing between 20,000 and one million e-commerce transactions per year. A yearly assessment using the relevant SAQ must be completed, and a quarterly PCI scan may also be required.
- Level 4 – Applies to merchants processing fewer than 20,000 e-commerce transactions annually, or those that process up to one million real-world transactions. An assessment using the relevant SAQ must be completed annually, and a quarterly PCI scan may be required.

In line with these compliance standards, PCI CSS has identified 12 additional requirements for cardholder data management and network security. Below is a brief overview:

1. Secure network - Firewall configuration must be installed and saved
2. Safe card holder information - Cardholder data stored should be protected
3. The transfer of cardholder information to social networks must be encrypted
4. Risk management
5. Antivirus software should be used and updated regularly
6. Secure programs and applications must be designed and maintained properly
7. Access control - Cardholder data access must be restricted and each user with access must be given a unique ID
8. Physical access to cardholder information should be restricted

9. Network monitoring and evaluation

10. Access to details of card holders and network equipment should be monitored and monitored

11. Security systems and procedures should be monitored regularly

12. Information security policy relating to data security must be adhered to

The big difference

In summary, SOC 2 and PCI DSS are two different levels that work for different types of organizations. The following are the main differences between the two certificates:

SOC 2 Report	PCI DSS Compliance
SOC 2 reporting is performed in accordance with SSAE 18 standard issued by AICPA	PCI DSS standard is administered by the PCI SSC
SOC audits are performed by licensed CPA firms	PCI DSS assessments are performed by qualified security assessors.
Applicable to organizations that hold, store, and/or process customer data	Applicable to organizations that accept, store, process, or transmit cardholder data.
SOC 2 allows much more flexibility in adhering to its trust service principles. A company striving to meet SOC 2 compliance standards can tailor its business and security strategies to meet its specific needs.	PCI DSS standard is more detailed about what a business must do to secure payment card transactions.

Please contact us if you would like to know more about data security or need any help to create an SOC / GDPR / certificate for your organization.

Visit our website https://accorppartners.com/soc/index.php or https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html to read more articles related to SOC reporting.