

Third Party Assurance Engagement (SOC 2)

Third party organisations that successfully complete a SOC 2 audit can offer their clients reasonable assurance that controls relate to operations and compliance; meet the criteria prescribed by AICPA for the five TSCs.

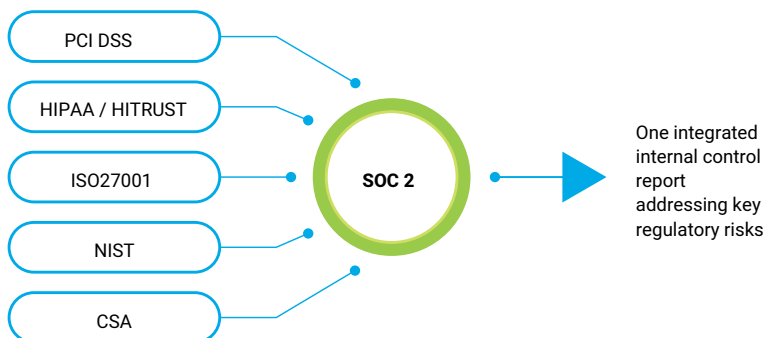
WHAT IS SOC2?

Service organisation controls (SOC) 2 is an internal controls offering that utilises the American Institute of Certified Public Accountants (AICPA) standards to provide an audit opinion on the security, availability, processing integrity, confidentiality and/ or privacy of a service organisation's controls.

Today's organizations do business within a broad ecosystem. Customers, partners, agents, affiliates, vendors, and service providers make up an "extended enterprise" of third parties, many with operations around the world. The growing use of outsource service providers (OSPs) to carry out a wide array of functions, many of them missioncritical, has fueled concern over greater enterprise risk exposure.

STREAMLINED APPROACH

SOC 2 reports can be tailored to meet the needs of specific industries. The trust services criteria used in SOC 2 reports have been mapped to various other standards. As a result of this mapping, the SOC 2 testing can be used to support other certifications, resulting in a streamlined approach to testing. The mapping allows one set of testing to provide assurance against multiple standards.



Trust services principles

SOC 2 reports can provide assurance over non-financially related processes, and provide assurance in relation to one or more of the five trust services principles, which are:



Security - The system is protected against unauthorised access (both physical and logical).



Availability - The system is available for operation and use as committed or agreed.



Processing integrity - System processing is complete, accurate, timely, and authorised.



Confidentiality - Information designated as confidential is protected as committed or agreed.








Privacy - Personal information (e.g. Personally Identifiable Information) is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.

For more information

Visit www.ecomsecurity.org or E-Mail us at sales@ecomsecurity.org.

INCORPORATING MULTIPLE FRAMEWORK INTO SOC 2

	Framework	Example
	PCI-DSS (Payment Card Industry – Data Security Standard)	An OSP payment processor stores credit card information for future payments. Its customers want to know the details of the OSP's controls beyond the PCI certification. In situations where there is no PCI certification, there is a need to demonstrate what controls are in place.
	HITRUST (Health Information Trust Alliance)	An OSP claims processor must have access to HIPAA data in order to execute its responsibilities. To demonstrate that it is adequately safeguarding personal health information, it maps its controls to the HITRUST framework.
	Cloud Security Alliance (CSA)	A data center provider possesses its clients' information in both public and private clouds. Due to the unique security configurations, its clients have required a SOC 2+ with STAR.
	NIST	A company that maintains governmental contracts for building roads and bridges has contractual obligations to demonstrate how it meets the latest revision of NIST.
	ISO 27001	A data center provider has data centers and clients around the world. It continues to get security questionnaires and requests for understanding how it manages security. Rather than addressing each questionnaire individually, the center chooses to compile a SOC 2+ mapped with ISO 27001 to demonstrate its information security controls.

