

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.

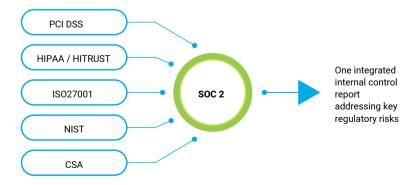
WHAT IS SOC2?

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 nonfinancially 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	k	Example
	PCI-DSS (Payment Card Industry – Data Se Standard)	future payments. It OSP's controls bey	rocessor stores credit card information for s customers want to know the details of the ond the PCI certification. In situations where ification, there is a need to demonstrate what e.
	HITRUST (Health Inform Trust Alliance)	mation order to execute its	cessor must have access to HIPAA data in a responsibilities. To demonstrate that it is arding personal health information, it maps its RUST framework.
	Cloud Security Alliance (CSA)	public and private	ider possesses its clients' information in both clouds. Due to the unique security clients have required a SOC 2+ with STAR.
	NIST	roads and bridges	aintains governmental contracts for building has contractual obligations to demonstrate itest revision of NIST.
	ISO 27001	around the world. requests for under addressing each q	ider has data centers and clients It continues to get security questionnaires and standing how it manages security. Rather than uestionnaire individually, the center chooses to mapped with ISO 27001 to demonstrate its tv controls.
Initial planning	Determine scope Expecta	Perform examination	Communicate results
Initial planning Service Organization • Identify expectations between service organization and E Com Security Solutions E Com Security Solutions • Gain high-level understanding of key processes • Establish relationship protocols • Issue project charter	 Understand key business processes and system design: Understand Company's business, contractual relations and user expectations Determine scope of the Perform prelimination assessment of - Perform prelimination - Perfo	inary • Remediation Suppi f controls: • Policy developm assessment • Olicy developm endescription • Identify & Access ols • Training & Awar of operating • Technology & Cha able for • Strategy & Governation operating • Strategy & Governation	ort hent s eness in nge ance Results SOC Report Control recom
Service Organization E Com Security Solutions • Identify expectations between service organization and E Com Security Solutions • Gain high-level understanding of key processes • Establish relationship protocols • Issue project charter	 Understand key business processes and system design: Understand Company's business, contractual relations and user expectations Determine scope of the report Perform risk assessment Identify risks Identify controls Map the risks and controls Perform gap analysis and action list Identify stakeholder expectation Threat & Vulnerability Perform Read Company's business, contractual relations and user expectations Determine scope of the report Evaluate system effectiveness: Design is sufficient effectiveness Vendor Risk Mathematication is the system of the respectation is the system environment is the system of the respectation is the	inary • Remediation Suppi f controls: • Policy developm assessment • Olicy developm endescription • Identify & Access ols • Training & Awar of operating • Technology & Cha able for • Strategy & Governation operating • Strategy & Governation	ort tent s eness in nge ance Results SOC Report Control recommendations



© Copyright E Com Security Solutions

E Com Security Solutions' provide Compliance, Application Security, Infrastructure security and advisory services through the cloud, managed security services and software that help clients protect their most important assets from evolving cyber threats. As the global professional services and consulting network, with approximately 300 security consultants world wide, we bring world-class capabilities and high-quality services to our clients.