SPOTLIGHT ON SOC REPORTS

Understanding System and Organization Controls (SOC) Reports

A Spotlight on the framework, the comparison and the different types of SOC reports

StratisAdvisory

RISK | STRATEGY | CYBER | COMPLIANCE MANAGEMENT

System and Organization Control Reports and Exam Framework

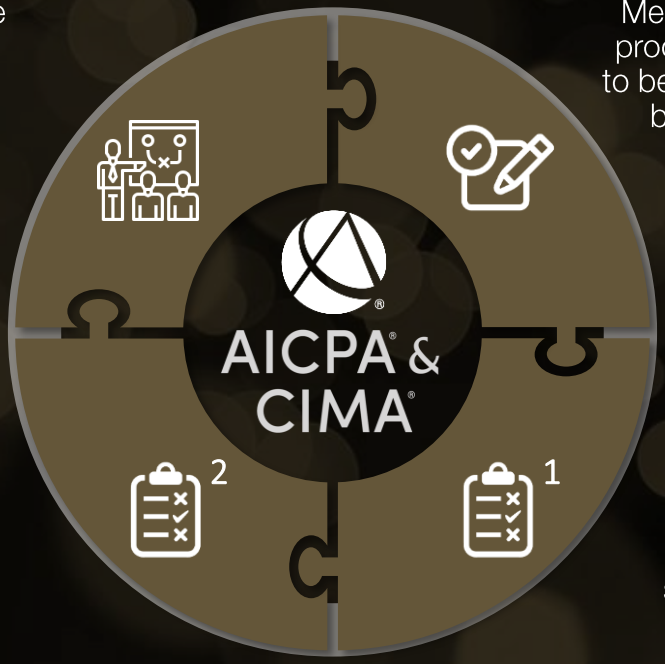
System and Organization Controls, formerly known as Service Organization Control (SOC) Reports for Service Organizations, help companies that provide services to other entities establish trust and confidence in their service delivery processes and controls. SOC Reports are the compiled result and findings of a SOC Examination, which is performed by independent Certified Public Accountants (CPAs) and designed to provide assurance over the functioning of an organization's internal controls. Steps to perform a SOC exam vary but have this basic framework:

Conduct a Planning Session

This is when the auditor meets with the service organization to agree on the scope of the system or services, the SOC report required for the organization's needs as well as the scheduling, timing and fees.

Conduct Readiness Assessment

Meetings are held to discuss policies and procedures in place or whether they need to be developed or refined. Gaps identified by the service auditor are shared to the service organization so that they are prepared for the SOC exam.



Type 2 Exam and Reporting

If the organization chooses to have the Type 2 examination performed, detailed testing will be done by the service auditor for the reporting period agreed on during the planning process. This report includes a description of tests performed. The opinion will cover whether controls are suitably designed and if the controls are effectively operated.

Type 1 Exam and Reporting

The service organization can choose to have the Type 1 exam prior to moving to the Type 2 examination to ensure that controls are implemented by a specified date. A formal report still issued by the service auditor but since no detailed testing is performed, the controls are simply listed as part of the system description.

What are the Types of SOC Reports?

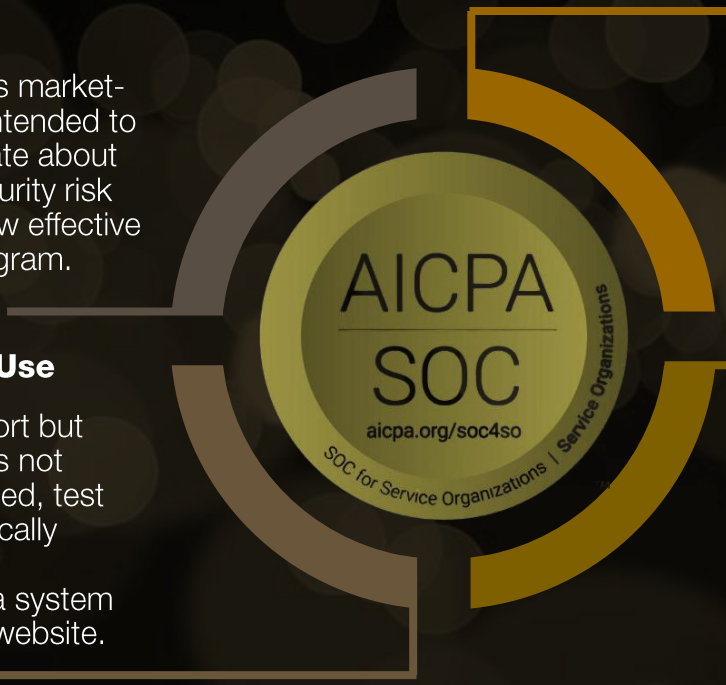
System and Organization Controls (SOC) is a suite of service offerings developed by The American Institute of CPAs (AICPA) for CPAs to use to evaluate system-level controls of a service organization or entity level controls of other organizations. These internal control reports about services provided by a service organization provide valuable information to serviced entities so they are able to assess and address risks associated with an outsourced service. Below are the types of SOC Reports:

SOC for Cybersecurity

A reporting framework which is market-driven, flexible and voluntary intended to help organizations communicate about their enterprise-wide cybersecurity risk management program and how effective the controls are within the program.

SOC 3®: TSC for General Use

Very similar to the SOC 2 Report but more for general use as it does not include details on controls tested, test procedures or the results. Typically contains the auditor's opinion, management's assertion and a system description, published on the website.



SOC 1®: Internal Control over Financial Reporting (ICFR)

A report completed by a CPA firm focused on attesting to a service organization's financial controls and how it impacts a user entity's financials.

SOC 2®: Trust Services Criteria (TSC)

A report that provides assurance to user entities that a service organization provides services securely relative to availability, confidentiality, processing integrity and privacy. SOC 2 is the most common and expected report.

NOTE: A SOC Report for Supply Chains also exists, which is intended to provide specified users with information regarding security, availability, processing integrity, confidentiality and privacy controls within business relationships involving suppliers and distribution networks.

What's in a Report: A Comparison of SOC Reports

	SOC 1®	SOC 2®	SOC 3®	SOC FOR CYBERSECURITY
Purpose	Reports on the controls of the service organization that are relevant to a user entity's financial reporting.	Reports on the effectiveness of the controls of an entity related to compliance or operations, based on the Trust Services Principles and criteria.	Supports the marketing of services to prospective and current customers.	Reports on and provides an independent, entity-wide assessment of an organization's cybersecurity risk management program.
Scope	Internal Controls over Financial Reporting (ICFR) are controls that would be relevant to financial reporting and financial audits if they were not outsourced to a third-party service provider. They include core information technology general controls such as security, as well as controls surrounding the completeness and accuracy of the processing of financial transactions.	The five core Trust Services Principles are: Security, Availability, Processing Integrity, Confidentiality and Privacy. Each principle has a set of standard criteria. In a SOC 2, you can choose to include one, several or all the Trust Principles and related criteria. Once you choose to include a principle, all the criteria related to that principle must be included in the report.	Similar to the SOC 2, the SOC 3 also uses the Trust Services Principles. However, a SOC 3 gives less detailed description of an entity's control system. The principles are selected by the service provider and specific predefined criteria are used rather than control objectives in a SOC 3 report.	Covers 3 key components: (a) the description of the entity's cybersecurity risk management program, (b) management's assertion whether the description is in accordance with the description criteria and whether the controls are effective to achieve the entity's objections based on the control criteria and (c) the practitioner's opinion about (b).
Audience	Restricted to a service organization's management, user entities and user auditors.	Restricted to a service entity's management, user entities and user auditors, vendor management, executives and regulators.	Unrestricted, general use reports but can be limited to specified users only.	Unrestricted, general use reports but can be limited to specified users only.
Report Type	Type 1 - Reports on the fairness of how management presents and describes the entity's system, control design suitability and operational effectiveness of controls as of a specified date (e.g. as of 4/15/2021) Type 2 - Reports on the fairness of how management presents and describes the entity's system, control design suitability and operational effectiveness of controls throughout a specified date (e.g. 1/1/20 – 12/31/20)		Type 2 Report	Cybersecurity Risk Management Examination Report

Discover what Stratis Advisory can do for you

SOC 2® Preparation

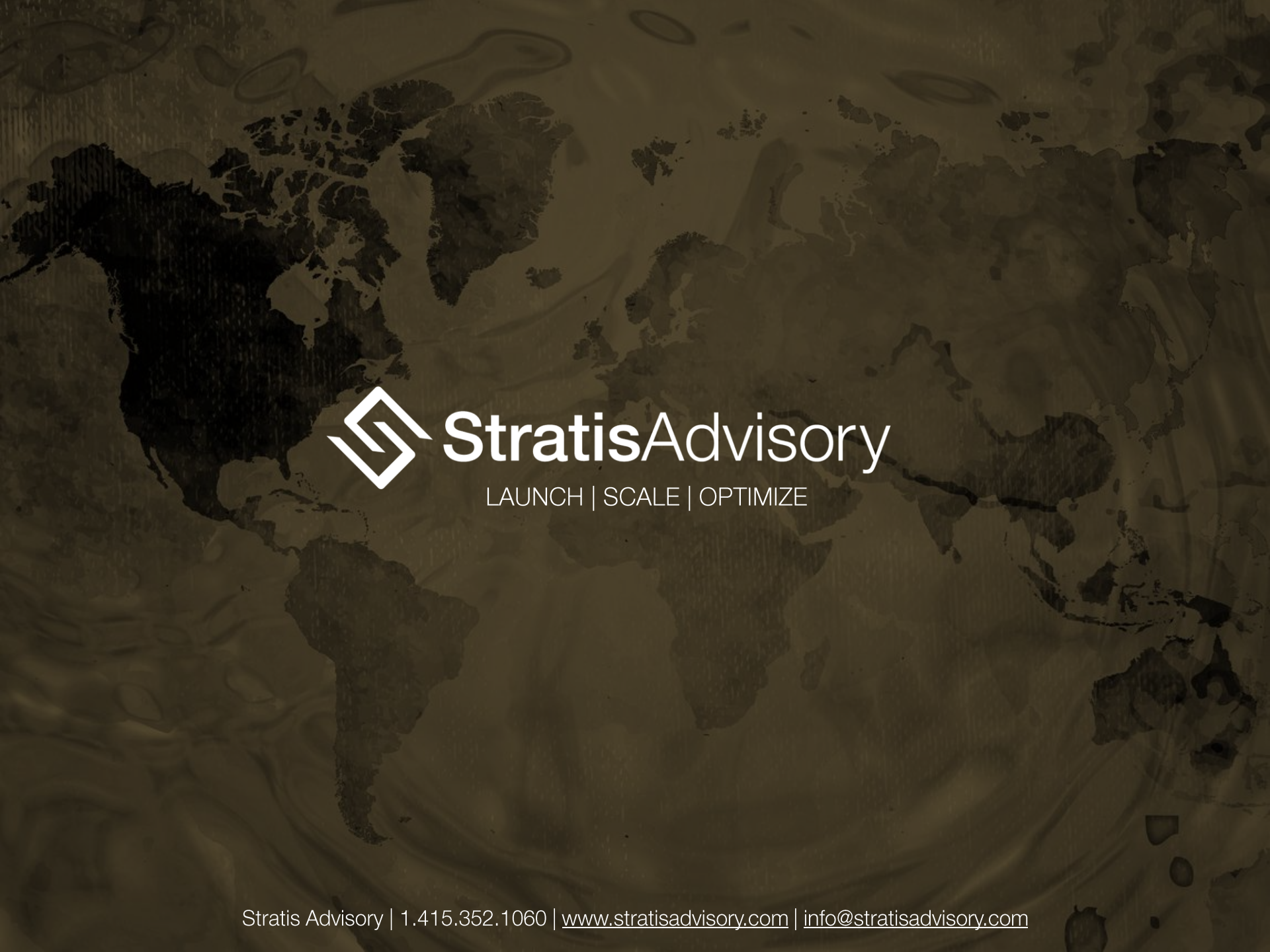
Whether you are a service organization or a company utilizing a service organization, it is crucial to understand the effectiveness of controls implemented within your operations to protect assets and intellectual property. A SOC 2® examination is intended to assess a service organization's system relevant to availability, confidentiality, processing integrity and privacy, which may be useful to overall risk management. Stratis can evaluate the readiness of your service organization to ensure proper and compliant controls are in place and are working effectively, not only for SOC 2® compliance, but also for you to be able to protect your customers and to demonstrate a strong security position within the service industry.

Cybersecurity Risk Assessment

Beyond Service and Organization Controls (SOC) audit(s), penetration testing, and PCI Security Standard assessments, dedicated risk assessments help you understand the inherent risks in information technology systems, processes, and programs. Stratis can execute your cybersecurity risk assessment to identify broader risk identification and control mitigation across key information systems.

Vendor Management Risk Assessment

A vendor management risk assessment is an evaluation used by organizations to assess risks and benefits associated with outsourcing to external entities. Regular risk assessments for each vendor relationship can help determine whether risks have evolved and are sufficiently mitigated. Stratis can perform your vendor management risk assessment for broader risk identification and control mitigation across key activities that may impact your organization, agreements, customers, and operations.



Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com