SOC 1, SOC 2 AND SOC 3 REPORTS: UNDERSTANDING THE DIFFERENCES

NCONTRACTS
The Upside of Risk

SOC 1

WHAT IS IT?

A SOC 1 report is **designed to review** internal controls at a service organization relevant to the user entities' **internal controls over financial reporting**. A SOC 1 report is best for your non-information technology-based products or services.

TWO TYPES

SOC 1: TYPE I
Reports on controls as of a specific date. A Type I report typically does not test the operational effectiveness of controls and only confirms that control activities exist and are appropriately designed.

SOC 1: TYPE II
Reports on controls throughout a period of time. A Type II audit is more rigorous as it includes an assessment of the operational effectiveness of controls over a period of time. In addition, a Type II report is more comprehensive and includes testing details and results.

WHEN IS IT RELEVANT?

A SOC 1 is relevant when the product or service used doesn't have consumer personally identifiable information being stored or hosted at the vendor. In addition, request and review this report when the product or service used may impact the financial reporting of your organization.

Example vendors include:

- Accounting software
- Investments/Securities/Funds Management
- Financial Planning and Wealth Management

SOC 2

WHAT IS IT?

A SOC 2 report is based upon the Trust Services Criteria (TSC) as issued by the AICPA. A SOC 2 report **focuses on a business's non-financial reporting controls** as they relate to security, availability, processing integrity, confidentiality, and/or privacy of a system.

This is typically the preferred SOC Report to utilize for Due Diligence.

TRUST SERVICES CRITERIA[1] *(please note, a SOC 2 report may cover one or all TSC)*

SECURITY
Systems at a service organization are protected against unauthorized access, modification, or use.

AVAILABILITY
Systems are available for operations and utilization as they were committed to.

PROCESSING INTEGRITY
System processing is complete, valid, accurate, timely, and authorized.

CONFIDENTIALITY
Information classified as confidential is protected as committed to.

PRIVACY
Personal information is collected, used, retained, disclosed, and disposed of as committed to and with adherence to criteria set forth in the Generally Accepted Privacy Principles (GAPP) issued by the AICPA and CICA.

TWO TYPES

SOC 2: TYPE I
Reports on controls as of a specific date. A Type I report typically does not test the operational effectiveness of controls and only confirms that control activities exist and are appropriately designed.

SOC 2: TYPE II
Reports on controls throughout a period of time. A Type II audit is more rigorous as it includes an assessment of the operational effectiveness of controls over a period of time. In addition, a Type II report is more comprehensive and includes testing details and results.

WHEN IS IT RELEVANT?

A SOC 2 focuses on the controls in place to protect private information that is either stored or transmitted by the vendor. Most of the TSC are related to technology-based services and therefore are beneficial in allowing the user entity to determine if proper controls are in place to protect their information.

Example vendors include:

- Core Banking
- Item Processing
- Online Banking
- Bill Payment
- Cloud Provider
- Managed Services

SOC 2 +
Although not a separate type, a SOC 2+ report, includes auditor opinions on additional criteria or subject matter. Examples of additional criteria include the Cloud Security Alliance, HITRUST, NIST 800-53, and ISO 27001. Although a SOC2+ is not defined within the attestation standard, this type of report is becoming more common.

SOC 3

WHAT IS IT?

A SOC 3 report enables a service organization to share a **general-use report** that is relevant to current and prospective customers.

KEY THINGS TO NOTE

A SOC 3 can also serve as a marketing tool to demonstrate that appropriate controls are in place to mitigate risks related to security, availability, processing integrity, confidentiality, and/or privacy of a system. As general-use reports, SOC 3 reports can be freely distributed.

- ✓ Based on Trust Services Criteria
- ✓ Less detailed than a SOC 1 or SOC 2
- ✓ Does not test the operational effectiveness of controls

WHEN IS IT RELEVANT?

A SOC 3 is best used as a tool in the initial vetting of a new vendor. In general, a SOC 3 Report should not be used in place of the more detailed SOC 1 and SOC 2 Reports.

[1] New Terminology: The COSO framework refers to "principles" that must be in place and working for an organization's internal control environment to be considered effective. To avoid confusion between the term "principle" as used in the COSO framework and in the trust services principles and criteria, the latter has been renamed "trust services criteria," although the acronym TSP is still used within the codification of guidance.