aronson LLC
ASSURANCE | TAX | CONSULTING
Expanding What's Possible

Service Organization Control (SOC) Reports Overview

Technology Risk Services

Table of Contents

SOC Reports Overview & Benefits

About SOC Reports

"Service Organization Control reports are designed to help service organizations, organizations that operate information systems and provide information system services to other entities, build **trust** and **confidence** in their service delivery processes and controls through a report by an independent certified public accountant."

– American Institute of Certified Public Accountants (AICPA)

Why obtain a SOC Report?

Why do Service Organizations obtain a SOC Audit?

Over time, companies have increased their **reliance** on third-party service organizations to conduct business functions

Service organizations can maintain stakeholder **trust** & provide **transparency** through an independent auditor's report conducted using AICPA guidance and standards

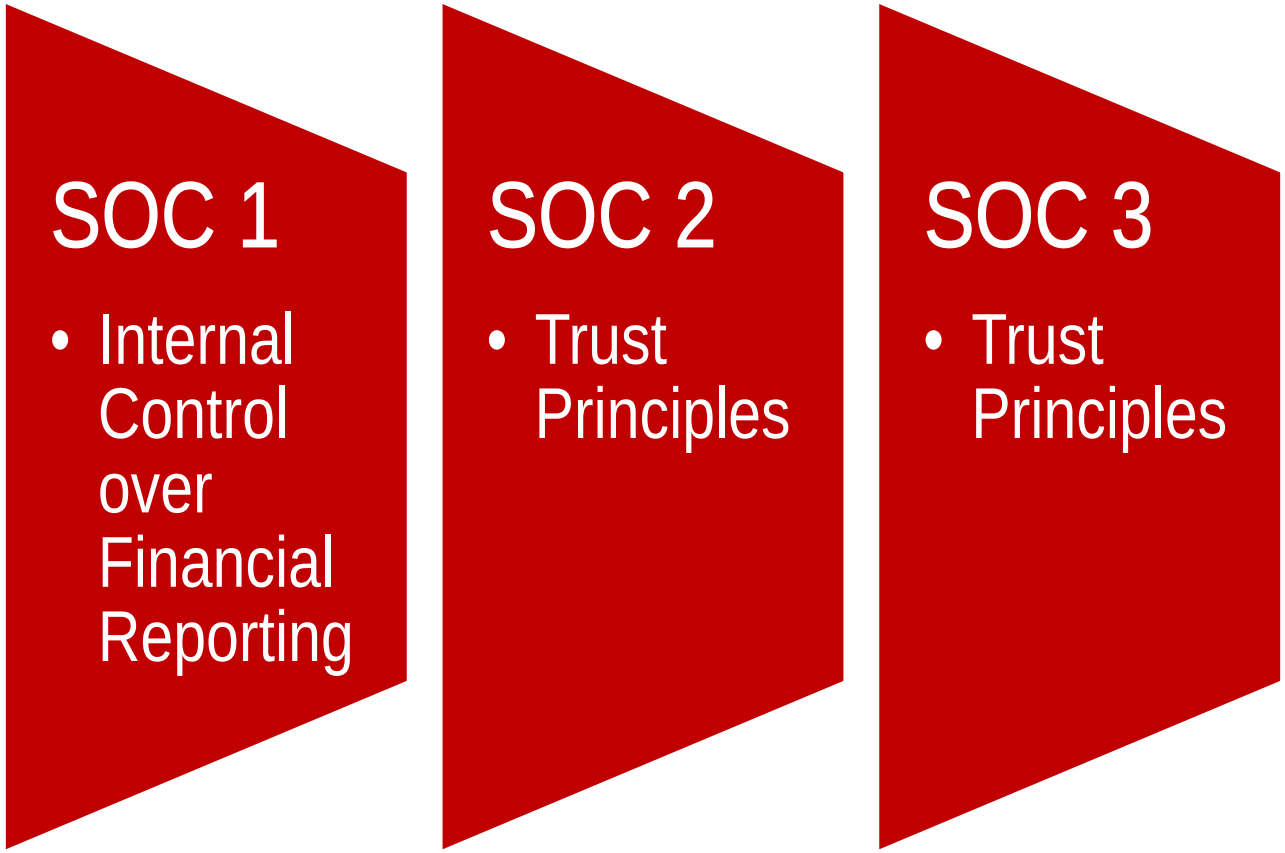
It helps Service Organizations **differentiate** themselves from their competition

SOC audits can **reduce** or **eliminate** other customer audits and vendor risk management questionnaires

What are the benefits of obtaining a SOC Audit?

- ✓ Ability to obtain a greater market share & competitive advantage through increased customer confidence
- ✓ Independent assessment of the control environment including people, processes, and technology
- ✓ One audit can satisfy multiple customers and various audit requirements
- ✓ Reduce third-party vendor risk management questionnaires
- ✓ Decrease client costs for other audits/compliance projects by relying on SOC reports

Types of SOC Reports



SOC 1 Overview

What is it?

Statement on Standards for Attestation Engagements (SSAE) No. 16 is an attestation standard put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) that addresses engagements undertaken by a service auditor for reporting on controls at organizations (i.e., service organizations) that provide services to user entities, for which a service organization's controls are likely to be relevant to user entities' internal control over financial reporting (ICFR). SOC 1 uses the SSAE 16 framework.

What is the scope?

Based on the internal controls over financial reporting of the service organization. This includes control objectives and activities that have been defined by the organization.

- ✓ Services, systems and locations covered
- ✓ Control objectives and activities

What are the different types?

- ✓ Type I report covers the design and implementation of the controls
- ✓ Type II report covers the design, implementation and operating effectiveness of the controls

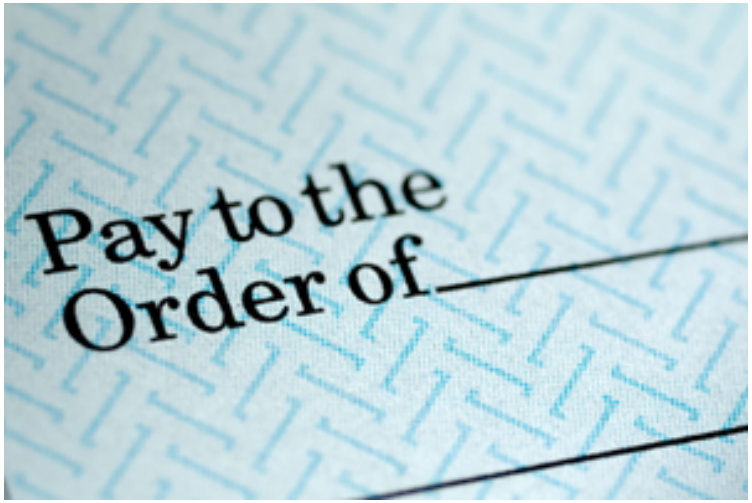
Examples of organizations that may need a SOC 1

Organizations that provide services that are being relied upon to store files being relied upon for financial reporting.

- Online document management repositories

Organizations that provide services to facilitate financial transactions.

- Payment Card Processors
- Payroll Processors



AT 101 or SOC 2 Overview

What is it?

A SOC 2 report is designed to provide various users with assurances regarding internal controls related to the Trust Principles of a service organization. The report can apply to an application, platform, hosting services, data center infrastructure, and related areas. The service organization determines the areas that will be evaluated based on the determined in-scope Trust Principles.

What is the scope?

Based on the five trust principles of:

- ✓ Security
- ✓ Confidentiality
- ✓ Availability
- ✓ Processing Integrity
- ✓ Privacy

What are the different types?

- ✓ Type I report covers the design and implementation of the controls
- ✓ Type II report covers the design, implementation and operating effectiveness of the controls

Trust Principles In-Depth: Security

Security	
CC1.0 Common Criteria Related to Organization & Management	Organizational structures responsible for ensuring Trust Principle commitments are met
CC2.0 Common Criteria Related to Communications	Service narratives, responsibility delegation, & stakeholder notifications
CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls	Risk Management policy, procedures, risk mitigation strategy, & risk assessments
CC4.0 Common Criteria Related to Monitoring of Controls	Monitoring policy, procedures, assessment results, & remediation plans
CC5.0 Common Criteria Related to Logical and Physical Access Controls	Access Management policy & procedures
CC6.0 Common Criteria Related to System Operations	Vulnerability Management and Incident & Breach Management policies & procedures
CC7.0 Common Criteria Related to Change Management	System Development Lifecycle (SDLC), Change & Configuration Management policies & procedures

Trust Principles In-Depth: Availability

Availability	
A1.1	Capacity & Usage Management
A1.2	Environmental Protections, Backup Processes & Recovery Infrastructure
A1.3	Recovery Procedures & Periodic Testing

Trust Principles In-Depth: Processing Integrity

Processing Integrity	
PI1.1	Processing Integrity Procedures to Prevent & Detect Errors
PI1.2	System Input
PI1.3	Data Processing
PI1.4	Storage
PI1.5	Output
PI1.6	Modification

Trust Principles In-Depth: Confidentiality

Confidentiality	
C1.1	SDLC Safeguards
C1.2	Unauthorized Access Safeguards - Internal
C1.3	Unauthorized Access Safeguards - External
C1.4	Obtain Third-Parties Confidentiality Commitments
C1.5	Ensure Compliance of Third-Party Confidentiality Commitments
C1.6	Proper Management & Notification of Confidentiality Commitment Changes

Trust Principles In-Depth: Privacy

Privacy	
1.0 Management	Defines documents, communicates, and assigns accountability for its privacy policies and procedures
2.0 Notice	Provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed
3.0 Choice & Consent	Describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information
4.0 Collection	Collects personal information only for the purposes identified in the notice
5.0 Use & Retention	Limits the use of personal information to the purposes identified in the notice and intended purposes
6.0 Access	Provides individuals with access to their personal information for review and update
7.0 Disclosure to Third-Parties	Discloses personal information to third-parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual
8.0 Security for Privacy	Protects personal information against unauthorized access (both physical and logical)
9.0 Quality	Maintains accurate, complete, and relevant personal information for the purposes identified in the notice
10.0 Monitoring & Enforcement	Monitors compliance with its privacy policies and procedures & has a plan to manage complaints/disputes

SOC 3 Overview

What is it?

SOC 3 report is a general-use report that provides information on whether the system achieved the trust principles criteria (no description of tests and results or opinion on the description of the system are provided).

What is the scope?

Based on the five trust principles of:

- ✓ Security
- ✓ Confidentiality
- ✓ Availability
- ✓ Processing Integrity
- ✓ Privacy

What are the different types?

- ✓ Limited environment details
- ✓ Limited description of controls and systems
- ✓ Short report

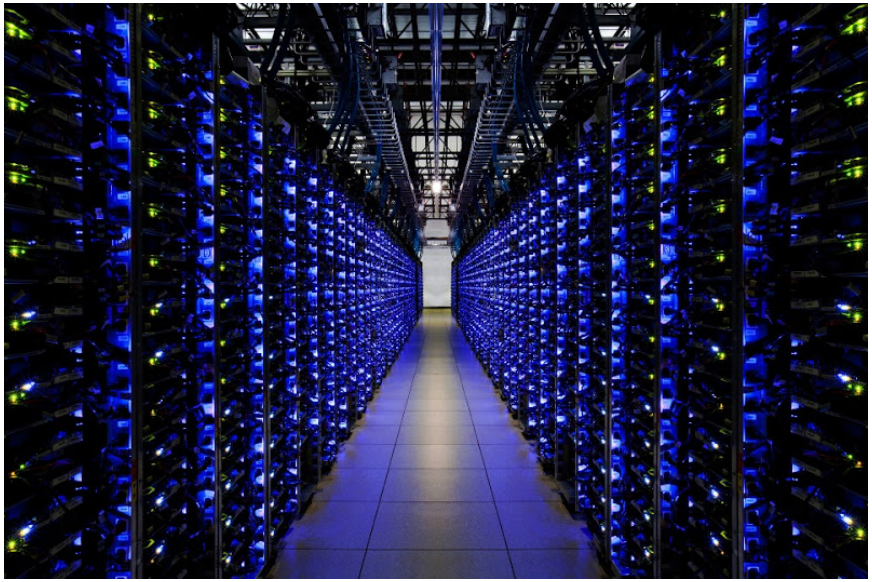
Examples of organizations that may need a SOC 2 or 3

Organizations that provide services for co-locating or hosting infrastructure.

- Data Centers

Organizations that provide applications for various purposes to facilitate business activities.

- Cloud Solutions (PaaS, SaaS, & IaaS)
- Campaign Management Software
- Health IT Applications



Selecting Trust Principles

- The Service Organization selects Trust Principles to include in its scope. Factors to consider include:
  - Short-term goals and initiatives
  - Types of services provided
  - Agreements & commitments included in contracts
- The Trust Principles in-scope can be changed in subsequent audits as determined by the Service Organization.

Report Contents

Standard

Across SOC 1, 2 & 3, there are standard components that are typically included.

1. Assertion of Service Organization's Services
   - The summary of services and background information provided by the Service Organization
2. Independent Service Auditor's Assurance Report
   - Auditor's opinion on whether the Service Organization's Assertions were fairly and accurately stated based on the audit work
3. Service Organization's Description of Services
   - Narrative includes details of the IT environment including the infrastructure and services provided
   - Also includes Complementary User Entity Controls (UECs): these are the controls required to be managed by the customer
     - *Note: the list of controls provided may not be comprehensive

User Entity Controls (UECs)

To facilitate the business relationship effectively, the Service Organization details examples of controls the customer should have in place. Some examples include the following:

1. Information security policies, procedures, standards, & guidelines
2. Access Management
   - Typically, customers are responsible for access management activities for the service organization's solution(s)
3. Network Security
   - Standard network access (e.g., Internet) and security safeguards are typically expected to be in place
4. Other areas may be included depending on the nature of services provided

Note: Customers should perform an analysis to fully inventory all UECs they are responsible for to ensure coverage & accountability

Differences in SOC Reports

SOC 1 & 2 reports have options to cover Type I (design only) or Type II (design + operating effectiveness). These reports will include the following:

Description of Control Objectives, Control Activities, Tests Performed, and Test Results

- SOC 1: The control objectives are provided by Management to cover standard aspects of ICFR.
- SOC 2: The control objectives are provided from the Trust Principles.
- Control Activities: These are the controls as they're designed / implemented in the environment.
- Test Results: Either deviations/exceptions will be noted or they won't.

SOC 3

- SOC 3 reports don't include the above control & test details as they are intended for general/public distribution. Such details may be irrelevant or unnecessary for certain audiences.

SOC 1 Control Categories

SOC 1 is based on assessing ICFR controls provided by Management. Typical subjects can include the following:

- Organizational Structure (can include Personnel Management e.g., background checks)
- Access Management (logical & physical)
- Risk Management
- Data Management (integrity, transmissions, storage, etc.)
- Backup & Recovery (environmental controls)
- Configuration & Change Management (includes Patch Management)
- Commitment Validation (governance documents and structures to ensure commitments to customers are met)

Report Selection & Applicability

Report Selection

AICPA GUIDANCE: HOW TO IDENTIFY THE SOC REPORT THAT IS RIGHT FOR YOU?		
Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer's financial statements?	Yes	SOC 1 Report
Will the report be used by your customers as part of their compliance with the Sarbanes-Oxley Act or similar law or regulation?	Yes	SOC 1 Report
Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization's systems?	Yes	SOC 2 or 3 Report
Do you need to make the report generally available or seal?	Yes	SOC 3 Report
Do your customers have the need for and ability to understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests?	Yes	SOC 2 Report
	No	SOC 3 Report

Focus & Distribution

Report	Report's Focus	Format	Intended Users	Distribution
SOC 1	Report on a service organization's internal control over financial reporting	✓ Type I ✓ Type II ✓ Control Descriptions ✓ Tests Performed & Results	✓ Financial Statement Auditors of the user entity (UE) ✓ Management of the UE ✓ Management of the service organization	Restricted use to current customers; can be shared with prospective customers if a third-party access letter is obtained
SOC 2	Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (Trust Principles)	✓ Type I ✓ Type II ✓ Trust Principle Controls ✓ Tests Performed & Results	✓ Management of the UE ✓ Management of the service organization ✓ Other relevant parties e.g., regulators & business parties	Restricted use to "customers with sufficient knowledge" e.g., current & prospective customers, regulators, business partners
SOC 3	Report on Trust Principles but does not contain all of the details of a SOC 2 report because users do not have the required knowledge/need for a SOC 2; processing details and control test results are omitted	✓ Brief Report ✓ Limited Details on Tests Performed & Results	✓ Same as SOC 2	✓ Can be freely distributed

When is a SOC Report Not Applicable?

SOC Reports are **not** applicable for Service Organizations that don't have systems or platforms that store, process, or transmit customer data.

Should Service Organizations pursue multiple SOC audits?

In some cases it may make sense for a service organization to have multiple SOC reports.

- SOC 1: services are relied upon for customers' financial reporting
- SOC 2: services are relied upon by customers to meet Trust Principle criteria

Discussions should be held with the audit team to determine cost-saving efficiencies if multiple SOC audits will be conducted.

Roadmap

SOC Roadmap

Gap Assessment

- Select Report & Type
- Perform gap assessment and determine any discrepancies in the design or operating effectiveness of controls
- Obtain/develop remediation recommendations
- Develop remediation plan and set priorities

Remediation

- Implement recommendations to enhance/establish controls to address deficiencies
- Train personnel on control changes

Audit

- Contract an independent auditor to conduct the SOC audit

Notes

- After remediation, controls must be operating for a specific time period before the audit can occur
- SOC reports cover a time period set by the Service Organization usually for about 3, 6, 9 or 12 months

Report Coverage & Promotion

SOC Report Coverage & Promotion

- SOC Reports must be continually renewed
- AICPA SOC Badges can be displayed publically
- Bridge Letters
  - A letter can be obtained from the service organization to understand if there have been any material changes within the control environment in between SOC audits

SSAE 18

Overview

SSAE 18 will replace SSAE 16 and will be effective on or after May 1, 2017.

SSAE 18 expands on the SSAE 16 to focus on the controls of sub-service organizations (SSO), which are “service organizations used by another service organization (SO) to perform some of the services provided to user entities’ internal control over financial reporting (SSAE 16/SOC 1) (AICPA).”

Source: SSAE-18 – An Update to SSAE 16 [Coming 2017] by SSAE16.com

Additional Requirements

- Compliance with certain laws, regulations, contractual agreements, or Agreed-Upon Procedures
- SSO services description and relationship to SO
- Focus on conducting annual risk assessments
- Additional guidance provided for assessing the risk of material misstatement
- Understand the SO's monitoring controls over SSO's relevant controls:
  - Reviewing and reconciling output reports
  - Periodic discussions with the SSO personnel
  - Regular site visits
  - Testing controls at the SSO
  - Monitoring external communications
  - Reviewing SOC reports of the SSO's system

Source: AccountingToday, Recodifying SOC Reports: What SSAE No.18 means for SOC 1s by Ryan Buckner

Additional Requirements

- Evaluate the reliability of evidence provided by the SO:
  - Population lists used for sample tests
  - Exception reports
  - Lists of data with specific characteristics
  - Transaction reconciliations
  - System-generated reports
  - Other system-generated data (e.g., configurations, parameters, etc.)
  - Documentation that provides evidence of the operating effectiveness of controls, such as user access listings

Source: AccountingToday, Recodifying SOC Reports: What SSAE No.18 means for SOC 1s by Ryan Buckner

Case Studies

Case Studies

SOC 1	ABC Company requires a third-party report on ICFR for services provided to its customers. Specifically, ABC is a payment card processor and its services are factored into financial reporting activities. ABC Company recognizes that a SOC 1 report will provide assurance over in-scope controls to foster confidence in its control environment and enhance marketability. Without a favorable SOC 1 report business opportunities will be limited as other competitors have obtained such reports.
SOC 2	XYZ Company is a pioneer in political technology, servicing many of the largest grassroots organizations and political campaigns in the U.S. and abroad. Their technology processes and stores sensitive client data. Many of their clients (especially large financial institutions) require them to fill out a detailed security questionnaire around the confidentiality, security, integrity and availability of the data. This is a time consuming exercise which has to be done annually for many of their clients. Instead of repeating this process for each client, they decided to get a SOC 2 Type II audit for the following Trust Principles – Security, Confidentiality, Integrity, and Availability.

Case Studies

SOC 3	PQR Company provides online document management services. The organization obtains a SOC 1 Type II report to provide customers and stakeholders with detailed information about the design and operating effectiveness of controls. PQR also receives outreach from prospects seeking to vet the adequacy of their services prior to engaging in a contractual agreement. PQR leadership recognized the value in providing some insight into their environment and services to help promote their brand and support prospect vetting of their business. Considering the sensitive nature of a SOC 1 Type II report, a SOC 3 report provides details without disclosing such sensitive content.


Questions?
aronson LLC
ASSURANCE | TAX | CONSULTING
Expanding What's Possible

Presenter Contact Information

Payal Vadhani, Partner

Technology Risk Services

pvadhani@aronsonllc.com

Natasha Barnes, Manager

Technology Risk Services

nbarnes@aronsonllc.com