Service Organization Control (SOC) Compliance Guide

Technology Risk Services
Table of Contents

- About SOC Reports
- Why obtain a SOC Report?
- What are the different types of SOC Reports?
- Which one to choose?
- What is the difference between the SOC Reports?
- When is a SOC Report not applicable?
- What is the Aronson Methodology?
- Why choose Aronson as the attestation provider?
- Case studies
About SOC Reports

“Service Organization Controls 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?

<table>
<thead>
<tr>
<th>Why do Service Organizations obtain a SOC Audit?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over time, companies have increased their <strong>reliance</strong> on third-party service providers to conduct business functions</td>
</tr>
<tr>
<td>Service providers can maintain stakeholder <strong>trust</strong> and provide <strong>transparency</strong> through an independent auditor’s report conducted using AICPA guidance and standards</td>
</tr>
<tr>
<td>It helps Service Organizations <strong>differentiate</strong> themselves from their competition</td>
</tr>
<tr>
<td>SOC audits can <strong>reduce</strong> or <strong>eliminate</strong> other customer audits and vendor risk management questionnaires</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What are the benefits of obtaining a SOC Audit?</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Ability to obtain a greater market share and competitive advantage through increased customer confidence</td>
</tr>
<tr>
<td>✓ Independent assessment of the control environment including people, process and technology</td>
</tr>
<tr>
<td>✓ One audit can satisfy multiple customers and various audit requirements</td>
</tr>
<tr>
<td>✓ Reduce third-party vendor risk management questionnaires</td>
</tr>
<tr>
<td>✓ Decrease client costs for other audits/compliance projects by relying on SOC reports</td>
</tr>
</tbody>
</table>
# What is SSAE 16 or SOC 1?

## 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).

## What is the scope?

Based on the internal controls over financial reporting of the service provider. 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
What is AT 101 or SOC 2?

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

What is it?

What is the scope?

What are the different types?

Based on the five trust principles of:

- Security
- Confidentiality
- Availability
- Processing Integrity
- Privacy

- Type I report covers the design and implementation of the controls
- Type II report covers the design, implementation and operating effectiveness of the controls
What is SOC 3?

**What is it?**

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

**What is the scope?**

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

**What are the different types?**

Based on the five trust principles of:
- Security
- Confidentiality
- Availability
- Processing Integrity
- Privacy

- Limited environment details
- Limited description of controls and systems
- Short report
Which one to choose?

<table>
<thead>
<tr>
<th>HOW TO IDENTIFY THE SOC REPORT THAT IS RIGHT FOR YOU?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>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?</strong></td>
</tr>
<tr>
<td><strong>Will the report be used by your customers as part of their compliance with the Sarbanes-Oxley Act or similar law or regulation?</strong></td>
</tr>
<tr>
<td><strong>Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization’s systems?</strong></td>
</tr>
<tr>
<td><strong>Do you need to make the report generally available or seal?</strong></td>
</tr>
<tr>
<td><strong>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?</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
# Focus & Distribution

<table>
<thead>
<tr>
<th>Report</th>
<th>Report’s Focus</th>
<th>Format</th>
<th>Intended Users</th>
<th>Distribution</th>
</tr>
</thead>
</table>
| 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 provider | 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 provider  
✓ Other relevant parties e.g., regulators, business parties | Restricted use to “customers with sufficient knowledge” e.g., current and 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 |
What is the difference between SOC 1 vs. SOC 2?

**Similarities**
- Contain an opinion and an assertion
- Contain Management Representation Letter from provider
- Contain processing environment description
- Contain control objectives, activities, and test results

**Differences**
- SOC 2 does not address ICFR and isn’t expected to support the financial reporting process for customers
- SOC 2 has a wider distribution to include “specified parties,” which includes anyone who understands the providers’ operations, internal controls, or services
- SOC 2 can offer more technical information through descriptions and control details
When is a SOC Report not applicable?

SOC Reports are not applicable for the following circumstances:

- Service organization is 100% professional services and doesn’t have systems or platforms that store, process, or transmit customer data
- Customers of the service organization are not relying upon services to support their financial reporting process
What is the Aronson Methodology?

<table>
<thead>
<tr>
<th>Planning</th>
<th>Assessment</th>
<th>Remediation</th>
<th>Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Develop project plan</td>
<td>1. Conduct interviews and walkthroughs to assess the current control environment</td>
<td>1. Develop Remediation Roadmap</td>
<td>1. Develop audit plan</td>
</tr>
<tr>
<td>2. Confirm system boundary</td>
<td>2. Review existing documents &amp; conduct control analysis</td>
<td>2. Develop or update policies and procedures</td>
<td>2. Conduct controls testing for design and operational effectiveness using AICPA SOC Report Audit Protocol</td>
</tr>
<tr>
<td>3. Confirm in-scope ICFR objectives or Trust Principles</td>
<td>3. Develop Gap Analysis &amp; Recommendations Report</td>
<td>3. Develop or revise processes and controls depending on the areas of deficiency</td>
<td>3. Develop audit report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Conduct trainings for new or revised processes</td>
<td>5. Perform continuous control improvement</td>
</tr>
</tbody>
</table>

Key Activities
Why choose Aronson as the attestation provider?

- Leading provider of assurance services in the Mid-Atlantic region (peer reviewed, nationally ranked CPA firm) that provides assurance services across a broad range of industries
- Collaborative teaming approach to drive better context and value of audit and knowledge transfer
- View of wider business implications and not just the immediate effect
- Tailored practical approach focused on the client’s unique environment
- Proven technical skills and understanding of emerging risks in key audit areas
- Focused on importance of knowledge transfer and alignment of cultures
- Relevant technical skills, practical knowledge and thought leadership
# Case Study 1 – SSAE 16

## Client Issue
ABC Company requires a third-party report on ICFR for services/products provided to private/public companies. ABC Company recognizes that an SSAE 16 report will provide assurance over in-scope controls to foster confidence in its control environment and enhance marketability. Without a favorable SSAE 16 report business opportunities will be limited.

## TRS Delivery
- Conduct SSAE 16 audit readiness assessment
- Conduct SSAE 16 audit

## TRS Value
- Understood and clearly articulated emerging risks in key areas
- Provide guidance on their remediation activities that helped them become ‘audit ready’ in a short period of time
- Focused on wider business implication
# Case Study 2 – SOC 2

## Client Issue
ABC Company is a pioneer in political technology, servicing many of the largest grassroots organizations, PACs, 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 2 audit for the following Trust Principles – Security, Confidentiality, Integrity, and Availability.

## TRS Delivery
- Conduct SOC 2 audit readiness assessment
- Conduct SOC 2 audit

## TRS Value
- Deep technical skills and use of accelerators that helped jump start the engagement
- Provided guidance on their remediation activities that helped them become ‘audit ready’ in a short period of time
- Provided guidance on how to reduce time spent on responding to multiple customer vendor management questionnaires