Demystifying the SOC 2 Report

The SOC 2 report is mysterious to many, but once you learn how to navigate the contents and where to find the bits of information you are looking for, it is a little less intimidating. Whether you are close to receiving your first SOC 2 report, OR you are reviewing the reports of other organizations as part of your organization's vendor management process, it is helpful to know the lay of the land.

What is a SOC 2 report?

A System and Organization Controls 2, or SOC 2, report is an independent attestation that evaluates the controls a company has identified to secure the security, availability, confidentiality, processing integrity, and or privacy of any outsourced operations. A certified public accountant (CPA) performs the audit. When it's completed you'll receive the SOC 2 report.

Before diving in...

The AICPA (the governing body for all things SOC) provides an illustrative SOC Report layout. Refer to this document as you read through the explanations below. However before opening the link, a word of caution: The AICPA example report contains Trust Service Criteria (TSC) *and* the Cloud Controls Matrix (CCM). Most SOC 2 reports only contain TSCs, which are Security (aka the Common Criteria), Availability, Confidentiality, Processing Integrity, and Privacy. For purposes of this exercise, ignore the CCM sections. Also, the AICPA report is only an example. Service organizations and service auditors do present the contents differently. But no matter the layout, all content must be there.

There are always four and sometimes five sections in a SOC 2 report. There will be a cover page that calls out which TSCs are in scope (this is important info!) and a table of contents. The table of contents will always include reference to each Section, but may also contain more detailed reference to the subsections of Section 3.

Section 1: Assertion of Management (aka Management's Assertion)

This section is simply a letter from management of your organization to the reader that includes a summary of the product, services, structure and torches on the IT systems, teams, and controls. It provides the reader with a list of facts and assertions, or statements, made by the service organization's management related to the system(s) in

scope for the audit. The service auditor will provide this letter for an executive at the organization to sign. If you are the subject of the SOC 2 audit, before signing, read this document carefully to ensure that all statements are true.

Section 2: Independent Service Auditor's Report

For this section, auditors will generally follow the format found in the AICPA example. No need to deep dive into this section (a quick skim is ok), because the meat is in the section where the auditor states their opinion. This is where you find out if you 'passed' or 'failed' the audit. Technically one doesn't pass or fail a SOC 2 audit, rather, you are looking for a clean opinion.

There are four possible opinions:

- **Unqualified** - The audit is clean. This is what you want.
  - Look at from Page 7, AICPA Illustrative Report. Ignore the bit about the CCM, but note that it is an unqualified opinion.

- **Qualified** - The audit is clean but there were a few hiccups. This opinion will occur when the auditor found a control that was not working as intended - aka a test failure or exception. The auditor will provide a high level statement as to why they qualify their opinion, such as:
  - The description does not fairly present the system that was designed and implemented throughout the period.
  - The controls related to the control objectives stated in the description were **not suitably designed** to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period [date] to [date].
  - The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, **did not operate effectively** throughout the period from [date] to [date].

    [**SOURCE**: Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting Guide]

- **Adverse** - The system can't be trusted. The auditor will include similar language as the qualified opinion, above.

- **Disclaimer of Opinion** - Not enough information was provided for the auditor to form an opinion.

Section 3: Description of the System

The contents of this section are written by management and reviewed by the auditor. It is used to describe, to an audience of end users of the system, what is in scope, the people, processes and technology used to support the system, narrative of the supporting controls, description of any sub-services to support the system, and any controls that the end user will need to implement to ensure that the system will perform as intended.

Preparing this section can be a nightmare for management because let's face it, they are not in the business of writing IT compliance missives. The good news is that the AICPA example report provides an outline on how this section flows as well as required content. However, unless you have someone with loads of time who is well versed in drafting a system description, it is a beast.

This is where Strike Graph comes in! After years of drafting system descriptions, our team created a semi-automated and highly efficient way for someone who's not well versed in SOC 2s to complete this document. Our System Description Builder solution cuts the time to prepare this document by 75%. We also provide a dedicated Customer Success Manager to guide creation of this document because, at the end of the day, *anything* included in this section is audited.

Section 4: Applicable Trust Service Categories, Criteria, Related Controls, Tests of Controls and Results of Tests

Section 4 is prepared by the auditor and is used to support their opinion. Every control identified by management will be tested. Section 4 will always include a few paragraphs on how testing is performed and a test results table. Auditors all have their own way of presenting results, but it is typically presented in a table with the following:

- Control objectives related to the applicable trust service criteria
- Controls in place at the service organization to meet the objectives
- Auditor's test procedures for each control
- Test result for each control

Section 5: Other Information Provided by Organization Not Covered by the Service Auditor's Report

Section 5 is optional and the contents will not be tested by the auditor. Management can include this section to provide additional information, such as:

- The organization's future plans for new systems
- Key aspects of the control environment not covered by Section 3 but the organization wishes to communicate to its customers
- Detailed explanation of their response to a qualified opinion

Strike Graph can help

To remain competitive in today's environment, more organizations are requiring third-party security attestations like the SOC 2. Proving to vendors that you're a trusted business partner matters. Sometimes, the difference between passing and failing a SOC 2 audit depends entirely on who you've got in your corner. If you're ever worried about preparing for, or maintaining SOC 2, don't hesitate to get in touch with us. We're here to help!

If would like a sneak peek of the many ways that Strike Graph can make the SOC 2 process easier, reach out for a Free Trial of our product. We'll show you how our solution points you to the controls you need to implement and the right evidence to gather so you can eventually snag that unqualified report.