Everything You Need to Know About SOC 2

From the SOC 2 experts at

ByteChek



Table of Contents

Chapter 1	**SOC 2 Overview**	**4**
	What is SOC 2 (and Why Does it Matter)?	6
	Why is SOC 2 Important?	7
	Real Examples of SOC 2	7
	When to Consider Pursuing a SOC 2 Examination	8
	Automating SOC 2 Readiness Assessments	8
	Tips and Reminders for SOC 2	9
	Key SOC 2 Terms to Know	9
	SOC 2 Report Use	10
	Types of SOC 2 Reports	11
	Sections of a SOC 2 Report	12
	SOC 2 Trust Services Categories	13
	Five Benefits of Earning a SOC 2 Report	13
Chapter 2	**What is an attestation report?**	**14**
	How Attestation Reports Apply to SOC 2 Reports	15
	Sections of the Attestation Report	15
Chapter 3	**SOC 1, SOC 2, & SOC 3 - What's the Difference?**	**17**
	Infographic	18
	What This Means for You	18
	SOC 1	19
	SOC 2	19
	SOC 3	19
	Which SOC report is right for you?	19
Chapter 4	**What are the different "types" of SOC 2 reports?**	**20**
	Introduction	21
Chapter 5	**What's in a System Description (SOC 2 - Section 3)**	**23**
	Introduction	24
	What is the system description and why is it important?	24
	OK, so what's in the system description?	25
Chapter 6	**AICPA SOC 2 Trust Services Criteria 101**	**27**
	What are the trust services criteria and why are they important?	28
	Tips and Reminders for the Trust Services Criteria	31
Chapter 7	**SOC 2 Information Flow-down**	**32**
	Introduction	33
	The Details	33
Chapter 8	**SOC 2 Report Opinions**	**36**
	The different opinions	37

Preface

Are we nerds? Maybe.

But at ByteChek, we love SOC 2. From getting started with readiness, to your end goal of SOC 2 Type 2, we have you covered. Our unparalleled experience in both automation and audit makes the SOC 2 lifecycle easier for you.





Chapter 1

SOC 2 Overview

Protecting customers' data is a concern for all organizations regardless of industry or size. Most organizations outsource key aspects of their business to third-party vendors such as Software-as-a-Service (SaaS) solutions or cloud hosting providers (i.e. Amazon Web Services or AWS). As companies continue to share the responsibility of protecting sensitive data, there is increased importance and scrutiny on the cybersecurity practices implemented at these organizations.

Third-party assessments are a common way in which organizations prove their cybersecurity practices to vendors, customers, and prospects. SOC 2 examinations have become one of the de facto standards for organizations to prove how they are securely managing their customers' data to protect their interests and privacy. For most organizations conducting business with a SaaS provider, a SOC 2 examination is a minimum requirement. SOC 2 reports are also common for other service organizations as well such as law firms, marketing agencies, accounting firms, healthcare organizations, and more. This guide will provide an overview of:

- What is SOC 2 (and Why Does it Matter)?
- When to Consider Pursuing a SOC 2 Examination
- Automating SOC 2 Readiness Assessments
- Tips and Reminders for SOC 2
- Key SOC 2 Terms to Know
- SOC 2 Report Use
- Types of SOC 2 Reports
- Sections of a SOC 2 Report
- SOC 2 Trust Services Categories
- Five Benefits of Earning a SOC 2 Report



What is SOC 2 (and Why Does it Matter)?

SOC 2 is a report on a service organization's controls relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy. SOC 2 reports are intended to inform users of detailed information and assurance about the controls at the service organization. These reports are provided by qualified CPAs, who form an opinion about the service organization's system and the control environment.

First and foremost, SOC 2 is a report, and therefore you should think of it as a reporting framework, rather than the common misconception of it as a compliance framework. I go into that in a lot more detail in this blog post. Think about it this way, SOC 2 is a way for a service organization to show its customers (through a system description) how they meet certain criteria prescribed from the AICPA that are relevant to the in-scope categories (security, availability, etc.).

The auditor's job is to verify the information in the description provided by the service organization, as well as identify the specific controls from the description that meet the criteria. In the case of a type 2 report (period of time), the auditor will also determine if those controls operate effectively during that period of time. More on the differences between report "types" in this post.

Let's use the security category as an example. The system description will describe the service organization's system in accordance with certain AICPA defined criteria. One of those criteria is the control environment of the organization, which, at a high level, will describe the security controls the organization has related to things like onboarding, risk management, system operations, change management, logical access, etc.

Those controls will then be shown in more detail in another section of the report (typically "section 4") according to how they meet each of the criteria related to the security category (for example, logical access criteria will have all of the controls related to logical access under it). In the case of a type 2 report, section 4 will also include the auditor's testing of those controls as well as the results of tests over a period of time.

Depending on if the controls are designed appropriately to meet the prescribed criteria, as well as (in type 2) if those controls operated effectively, the auditor then forms an opinion for the report on that design and operational effectiveness. Read more opinions in our report opinions article.

The report itself is provided by the service organization to its customers so that those customers can have comfort in knowing that the system and its controls are designed appropriately and operating as described.

Why is SOC 2 Important?

SOC 2 reports are becoming more prevalent in the market and more companies are asking for them in order to meet contractual obligations, supply chain management, due diligence, or other requirements. For the service organization, the report becomes not just a means to deliver on these obligations, but also a way of showcasing your security posture, as well as improving it through making sure your controls will operate properly.

Don't just take our word for it. According to the AICPA:

These reports can play an important role in:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

And because SOC 2 is more of a reporting framework as opposed to a compliance framework, it allows for more flexibility in how you can report on how you meet criteria, whereas in other frameworks, you're just showing yes or no when determining if you meet their requirements.

With the involvement of CPAs, SOC 2 has the element of trust, as CPAs are held to a high standard of quality and integrity in how they produce opinions and reports. You can be assured that a qualified, highly skilled CPA will not only make sure the appropriate person(s) are testing your environment but that the report itself is structured to meet all the AICPA requirements.

Real Examples of SOC 2

To see how SOC 2 is relevant for service organizations, look no further than the biggest cloud service providers. Microsoft, AWS, and Google Cloud all have SOC 2 for their offerings. The links below will bring you to their landing pages for their SOC 2 reports, but to obtain a copy, you will have to request it from your representative or through their respective sites.

https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc?view=o365-worldwide
https://aws.amazon.com/compliance/soc-faqs/
https://cloud.google.com/security/compliance/soc-2

NOTE - SOC 2 is not limited to cloud service providers but can be applied to many different types of organizations.

When To Consider Pursuing a SOC 2 Examination

The best day to consider pursuing a SOC 2 examination is when you started your company, the second-best day is today. In our experience, a SOC 2 examination is pursued as a reaction to a request from a customer or vendor. This reactionary response leads to the nightmare stories you have probably read regarding the SOC 2 process. Undergoing your first SOC 2 examination when you have a big deal or potential strategic partnership on the line can be a stressful and operationally draining experience.

Starting your SOC 2 journey prior to receiving a request from a customer or vendor is analogous to the famous quote by Benjamin Franklin, “An ounce of prevention is worth a pound of cure.” Preparing for your inevitable SOC 2 examination does not mean you have to undergo an audit by a third-party professional services auditing firm or pay exorbitant auditor fees. The Bytechek platform is designed for organizations that are taking a proactive approach to cybersecurity preparedness and readiness. Our fully integrated platform quickly assesses your technology stack against the SOC 2 criteria, providing detailed recommendations and implementation guidance in minutes.

Automating SOC 2 Readiness Assessments

It is possible to automate your readiness assessment using the fully integrated Bytechek platform. Our platform is built to quickly assess your organization’s gaps related to the Security, Availability, and Confidentiality Trust Services Categories. Instead of spending weeks working with a large auditing team, long arduous remote interviews, and archaic evidence collection procedures.

You can quickly integrate the cloud hosting, system information & event management, version control, human resources information system, and other relevant tools with the Bytechek SaaS platform. This eliminates the need for third-party auditors because our intelligent platform automatically provides recommendations for controls or security weaknesses identified. This frees up your team and resources to begin remediation efforts and ultimately earn your SOC 2 Type 1 report.

Tips and Reminders for SOC 2

Remember that SOC 2 is a reporting framework. As a service organization, you are showing (reporting) what you have in place to meet certain criteria, and a CPA is reporting on if what you have is adequate and operating effectively.

Always use a qualified, peer-reviewed CPA firm to assist with SOC 2 efforts. Determination of a CPA firm's peer review can be done through their home state's board of accountancy, or through the AICPA. Make sure they understand IT auditing and SOC 2!

Get to know the description criteria and (for your organization) relevant trust service category criteria as you are pursuing SOC 2. Understanding the criteria for both before you start will help with readiness assessments and overall development of your control environment.

Key SOC 2 Terms To Know

- **Applicable trust services criteria**
  The criteria codified in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy used to evaluate controls relevant to the trust services category or categories included within the scope of a particular examination.
- **AICPA**
  American Institute of Certified Public Accountants
- **Service Auditor**
  As used in this guide, a CPA who performs a SOC 2 examination of controls within a service organization's system relevant to security, availability, processing integrity, confidentiality, or privacy. **ByteChek Assurance is a Service Auditor**.
- **Service Organization**
  An organization, or segment of an organization that provides services to user entities (e.g. your company).
- **SSAE 18**
  Attestation standard for SOC Engagements. Relevant sections include AT-C Section 105 and AT-C Section 205
- **Subservice Organization**
  A vendor used by a service organization that performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved
- **Trust Services Categories**
  Five categories a service organization can be evaluated against including Security, Availability, Confidentiality, Privacy, and Processing Integrity

SOC 2 Report Use

SOC 2 report readers should understand who the service organization is, what services they provide, and how those services are delivered and managed. Without this knowledge, the report can be confusing and cause misunderstandings. Examples of intended users of a SOC 2 report are:

- Service organization internal personnel.
- Customers of the system.
- Business partners subject to risks from interactions with the service organization or system.
- Prospective customers going through vendor due diligence on the service organization.
- Regulatory agencies or authorities.

Because of the sensitive nature of the SOC 2 report and intended users of the report, a SOC 2 report is considered a restricted use report and should only be provided to readers under a non-disclosure agreement or other confidentiality agreements. In the event, your company needs or wants a report that is for general use, they can opt to undergo a SOC 3 examination. A SOC 3 report is a general use report that can be made publicly available. A SOC 3 report does not include the full system description (section 3) or the description of service auditors' tests of controls and the results thereof (section 4). Distribution of a SOC 2 report for marketing purposes is ill-advised as section 3 and section 4 contain sensitive information about the system and results of control design or operating effectiveness. This is why SOC 2 reports are considered restricted-use reports. SOC 3 reports can be posted on the company website and include limited information about the system and results of the examination. For example, AWS makes its SOC 3 report available for download as a PDF.

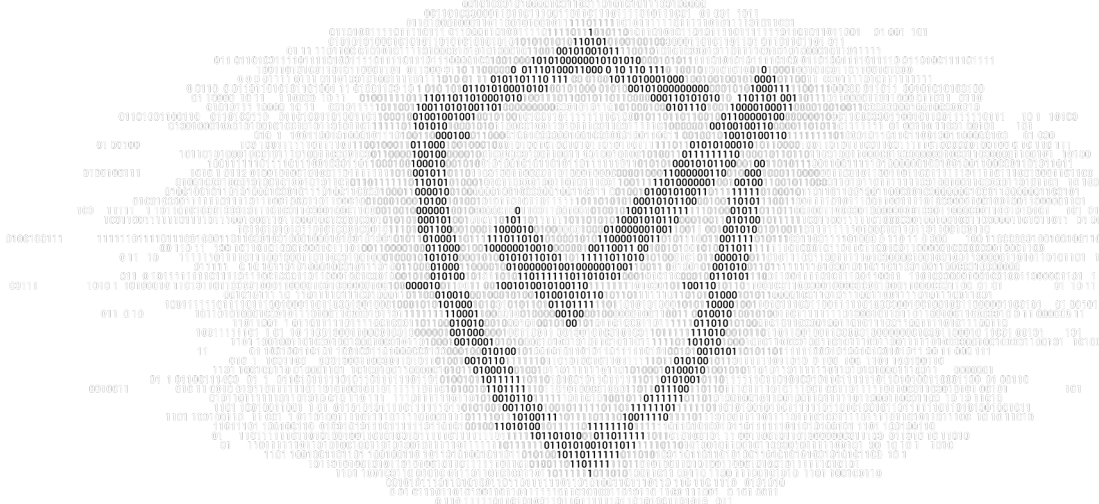
Types of SOC 2 Reports

In a SOC 2 examination, organizations can undergo a SOC 2 Type 1 or SOC 2 Type 2 examination. A Type 1 examination is a report on the controls at a service organization at a specific point in time, whereas, a Type 2 examination is a report on the controls at a service organization over a period of time. The period of time evaluated in a SOC 2 Type 2 examination is typically between 3-12 months.

A Type 1 examination is generally seen as the first stepping stone for an organization pursuing a SOC 2 examination. This report is a great way for companies to prove to their customers and vendors that they take security seriously and have partnered with a third-party auditing firm to prove their security. At ByteChek, we recommend that all companies pursue a SOC 2 Type 1 examination prior to beginning their SOC 2 Type 2. The level of effort and time it takes to earn a Type 1 examination is significantly lower than a Type 2 examination.

The level of effort decreases because your company is being evaluated at a point in time. This reduces evidence requirements and eliminates any requirement to sample test controls over a period of time. For example, in a Type 2 examination, your auditors may ask you to provide evidence of security awareness training for a sample of new hires over a three-month period. Whereas in a SOC 2 Type 1 examination, your auditors should only ask you for an example of a new hire's completion of security awareness training.

There is no AICPA requirement to undergo a Type 1 examination before a Type 2 but at ByteChek this is the recommended way to reduce the risk of exceptions or deviations in your first Type 2 report. Earning a Type 1 before your first Type 2 does not guarantee that your Type 2 report will not have exceptions or deviations, but it does mitigate the risk by providing clear and direct insight into the type of evidence and processes expected for every control that will be evaluated. Your customers can rest assured knowing that your Type 1 is a stepping stone to your Type 2. ByteChek provides every customer with a confirmation of engagement letter that can be provided to your customers outlining the scope and timeline of the Type 1 and Type 2 report.



Sections of a SOC 2 Report

In a SOC 2 report, there are five sections to be aware of.
Below is an overview of these sections and their components:

Section 1: Independent Service Auditor's Report:

- Scope
- Service Organization's Responsibilities
- Service Auditor's Responsibilities
- Inherent Limitations
- Description of Tests of Controls
- Opinion
- Restricted Use
- Service Auditor Signature (Bytechek Assurance), city and state, date of the report

Section 2: Management's Assertion

- Facts and assertions made by the management of the service organization
- A statement that management confirms, to their best knowledge and belief, that the description was presented in accordance and controls were suitability designed and, in type 2 examinations, operating effectively over a period of time
- The service organization is responsible for the completeness and accuracy of what is provided during the assessment

Section 3: System Description

- Overview of services provided
- Principal Service Commitments and System Requirements
- Components of the system (Infrastructure, software, data, people and procedures)
- System Incident Disclosures
- Applicable Trust Service Criteria
- Complementary User Entity Controls and Responsibilities
- Complementary Subservice Organization Controls
- Non-applicable TSCs
- Significant changes during the review period

Section 4: Trust Services Categories, Criteria, Related Controls and Tests of Controls Relevant to In-Scope TSCs

- Trust Services Criteria and Control Activities
- Bytechek Assurance Tests of the Controls (Type 1 reports do not include tests of controls or results of testing)
- Results of Tests

Optional Section 5: Other Information Provided by Management That Is Not Covered by the Service Auditor's Report

- This section is not audited by your service auditor, management has control over what is documented and presented in Section 5. In our experience, this section generally includes:
    - Management's responses to any deviations or exceptions. This section allows you to explain the circumstances surrounding the deviation and outline the remediation steps you have taken since the identification of the deviation. For example, if your service auditor found a deviation related to a new hire completing security awareness training. You could explain to the readers of your report that this new hire missed training because they were out of the office but have since completed the training.
    - A mapping of SOC 2 controls (from Section 4) to additional frameworks such as ISO 27001, HIPAA, HITRUST, CSA STAR, CMMC & more. Prior to investing the time and money into additional cybersecurity compliance frameworks or certifications, Bytechek recommends using Section 5 of your report to assess the business need or demand for additional certifications or frameworks. We have found that most customers will accept a mapping of your SOC 2 controls in Section 5 to answer any questions they may have about your compliance with other standards or frameworks.



SOC 2 Trust Services Categories

There are five Trust Services Categories (often mistakenly referred to as Trust Services Principles) that a client can choose to be evaluated against in a SOC 2 examination. The five Trust Services Categories and their definitions as defined by the AICPA are:

Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Availability: Information and systems are available for operation and use to meet the entity's objectives.

Processing integrity: System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Confidentiality: Information designated as confidential is protected to meet the entity's objectives.

Privacy: Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Five Benefits of Earning a SOC 2 Report

1. Enable Sales to unlock new markets and close deals faster
2. Prove security to customers and vendors with one report (audit once, use many)
3. Leverage the flexibility of the SOC 2 reporting framework to differentiate your company from its competitors
4. Demonstrate the maturity of your security program
5. Accelerate the customer onboarding and due diligence process, eliminating vendor security questionnaires



Chapter 2

What is an attestation report?

SOC 2 reports are, in official terms, attestation reports. So, what does that mean and why is it relevant when thinking about SOC 2 reports? First, the definition :

Noun. attestation report - a consulting service in which a CPA expresses a conclusion about the reliability of a written statement that is the responsibility of someone else.

How Attestation Reports Apply to SOC 2 Reports

When we break down that definition, we can apply it to SOC 2 reports.

- Consulting service - the examination engagement that the CPA will provide in order to deliver the SOC 2 report.
- Expresses a conclusion - this is the actual CPA's report (which includes their opinion), and often included as "section 1" of a complete SOC 2 report.
- Written statement - this is "management's assertion" in the SOC 2 report and often is included as "section 2". The management assertion will state that the company prepared the system description, as well as that the controls in that description were suitably designed as of a specific date (and operating effectively over a period of time if a type 2 report).

Sections of the Attestation Report

Putting that all together, in our SOC 2 attestation report, we have:

- Section 1 - CPA's report with an opinion on management's assertion
- Section 2 - Management's assertion that includes their statement about the system and its controls
- Section 3 - System description (as referenced in Section 2 from management)
- Section 4 - shows the criteria that the controls are measured against, the controls themselves, and in a type 2, the CPAs testing of those controls and results of tests

So why is all of this relevant for SOC 2? The boring answer is that attestations follow AICPA standards (in particular SSAE 18). But, when you break it down, it comes down to the assertion made by your company. In your assertion, you are going to state things like:

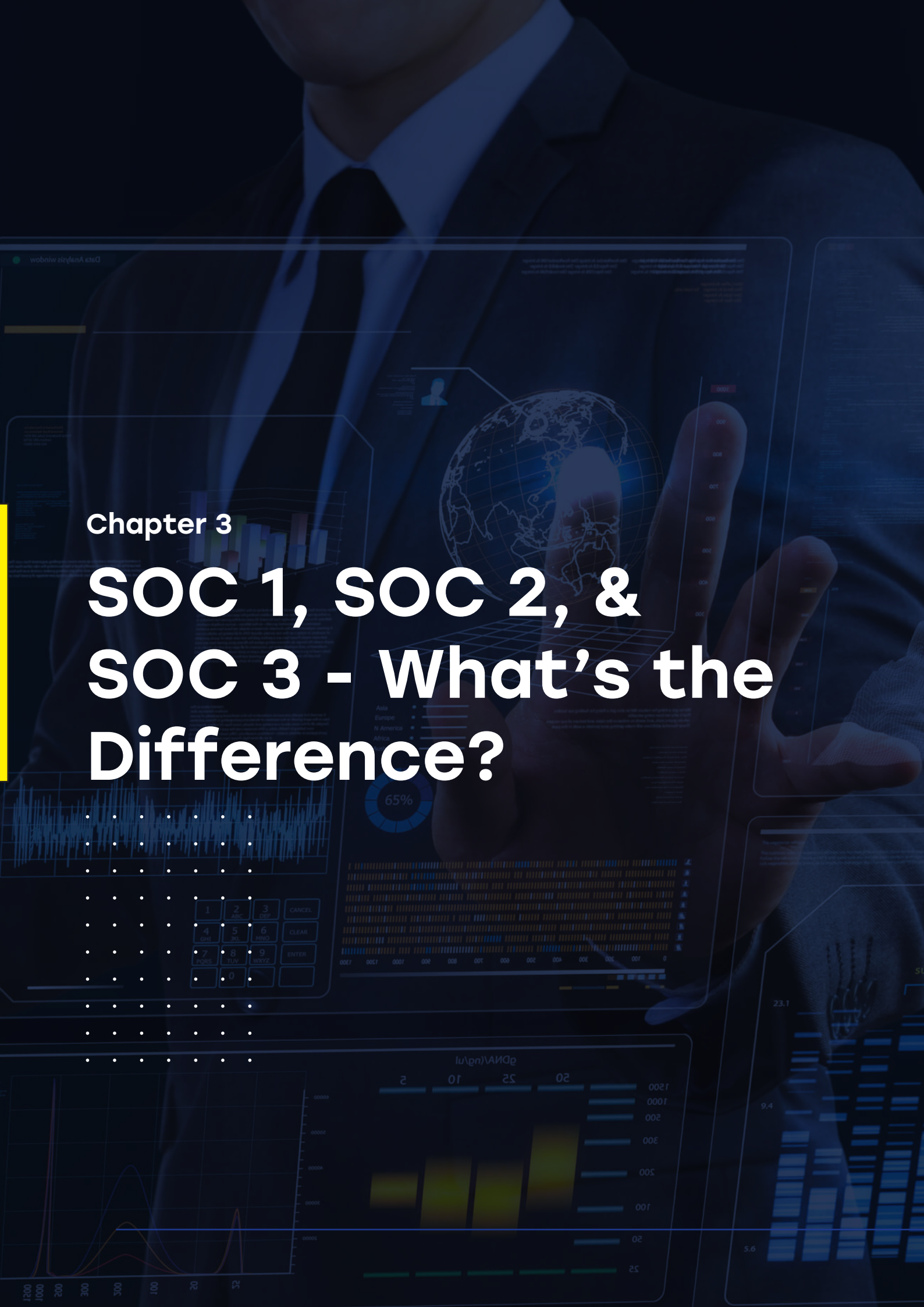
- The system description was prepared in accordance with the AICPA's description criteria

- The system can meet the commitments to your customers (for security, availability, etc.) and that the system has requirements in place to help meet those commitments. (NOTE - these are measured against the in-scope trust services criteria).

Your CPA then comes in and measures these assertions through inquiry, examination, testing, etc. Your CPA then forms the report based on these tests, and from there, you have your SOC 2 report.

"Attestation report - definition of attestation report by The Free ...."
https://www.thefreedictionary.com/attestation+report. Accessed 10 Aug. 2020.





Chapter 3

SOC 1, SOC 2, & SOC 3 - What's the Difference?

There are a variety of SOC reports that the AICPA has come up with, and each serves their own purposes. In this chapter, we will show you the differences between the three main SOC reports: SOC 1, SOC 2, and SOC 3.

SOC 1, 2, & 3 COMPARISON

AICPA SOC reports come in a variety of forms. The most common are SOC 1 SOC 2 and SOC 3. Whats the difference? See below for a summary. Keep in mind even though all of these reports serve different purposes, the common element is that even has an assertion and an auditor's opinion that go with them. To learn more about that, visit Bytecheck's SOC pillar page.

SOC 1	SOC 2	SOC 3
Internal controls for financial reporting	Controls related to security, availability, confidentiality, processing, integrity, or privacy	Redacted version of SOC 2
System impacts your customer's financial reporting	Based on your service commitments and system requirement	Only shows system description (no control testing shown)
Based on control objectives	Uses set criteria to measure against objectives	Can be provided publicly (most common on your website)
Some control objectives may be similar to SOC 2 (think security)	Most common of reporting of GRC programs	
Does not have preset criteria		

What This Means For You

SOC 1

When you think of SOC 1, you should be focusing on financial statements. SOC 1's are intended to discuss the internal controls for financial reporting (ICFR). Think about it this way, if your service has an impact on the financial statements of your customers, then you will likely be looking at a SOC 1. But those financial related controls aren't the only thing that might be in the report. You may find that you also need to report on some things you would find in a SOC 2, like security, confidentiality, etc. Those can be incorporated as well, because in SOC 1, you define the *Control Objectives*.

Let's use an example. Let's say you are a payroll processor service organization. You take your customer's raw data for payroll, run it through your systems, and produce payroll reports, tax filings, and employee pay stubs for those customers. Payroll is a significant part of your customer's income statement in their financial statements. So, you may have objectives around the accuracy of calculating those payroll items and how you file taxes with government entities. You may have objectives related to protecting your customer's data, which, for example, could be similar to logical access requirements from CC6 in SOC 2.

Because there are no prescribed objectives in SOC 1, you would have to determine what all of your objectives for customers are related to your service and include them in the report.

A SOC 1 does have a system description like SOC 2, but the criteria are less than what is required under SOC 2.

SOC 2

The difference between SOC 1 and SOC 2 is that SOC 2 will not cover those financial objectives because SOC 2 is focused on the Trust Services Categories as they relate to the service commitments you make to your customers. Let's go back to our example payroll processor again. They might also need a SOC 2 in addition to their SOC 1. In their agreements, they are making commitments to customers around the security and confidentiality of customer data, as well as being available 99.99% of every month. In this case, the security, availability, and confidentiality categories would be in scope for their SOC 2 and can be tested in conjunction with the SOC 1 testing, since both reports are going to share some similarities in objectives.

SOC 3

So, what is SOC 3 then? SOC 3 is simply a redacted version of a SOC 2 report. It is still based on the same trust services categories and criteria, but the only thing shown is a redacted version of the system description. There is no Section 4 in the report, which would show details of the controls, the auditor's testing of those controls, and the results of testing. SOC 3 reports are meant for public use, and many times companies will provide them via their website with no NDA required.

The common elements of all these SOC reports though is an assertion from company management, and an auditor's opinion. The language in those may be different between each of these reports, but the purpose of these sections remains the same.

So which SOC report is right for you?

- SOC 1 - does your service have an impact on the financial statements of your customers?
- SOC 2 - are you committing to anything related to the trust services categories (security, availability, confidentiality, processing integrity, privacy)?
- SOC 3 - do you need a public version of your SOC 2 to display to customers, potential customers, investors, or other interested parties?

Based on the answers to those questions, along with your objectives, you can find your way to the right path for SOC reporting.



Chapter 4

What are the different “types” of SOC 2 reports?

Introduction

SOC 2 reports come in two different “types.” Simply put, they are “Type 1” and “Type 2”. Each one serves a purpose and provides value to the report reader. Many organizations will use a Type 1 report as a means to get to Type 2, or some organizations will only use a Type 1 for specific purposes. So, what’s the difference? Let’s dive into the details of what these variations in SOC 2 reports entail.

A SOC 2 Type 1 report is as of a single point in time. The reason for that is because the report focuses on the suitability and design of the system and its controls to meet the criteria related to the categories in scope. This means that your path to earning your SOC 2 Type 1 is much shorter than achieving a SOC 2 Type 2 report. When it comes to providing evidence, you’re only providing example pieces of evidence from a specific point in time, not evidence showing controls operating over a period of time (i.e. 6-12 months). For example, in a SOC 2 Type 1, you may be asked to prove that your security awareness training control is suitably designed. You will be asked to provide evidence of a single new hire or employee that completed security awareness training. Whereas, in a SOC 2 Type 2, you will be asked to provide evidence for all or a sample (~25) of new employees that completed security awareness training during your reporting period.

This is why many organizations will use a Type 1 report as a “stepping stone” after a readiness assessment is done (and remediation is completed) to show that their controls are in place, suitably designed, and are ready for a Type 2 assessment. The reduced evidence requirements in a SOC 2 Type 1 make this the next logical step after your readiness assessment.

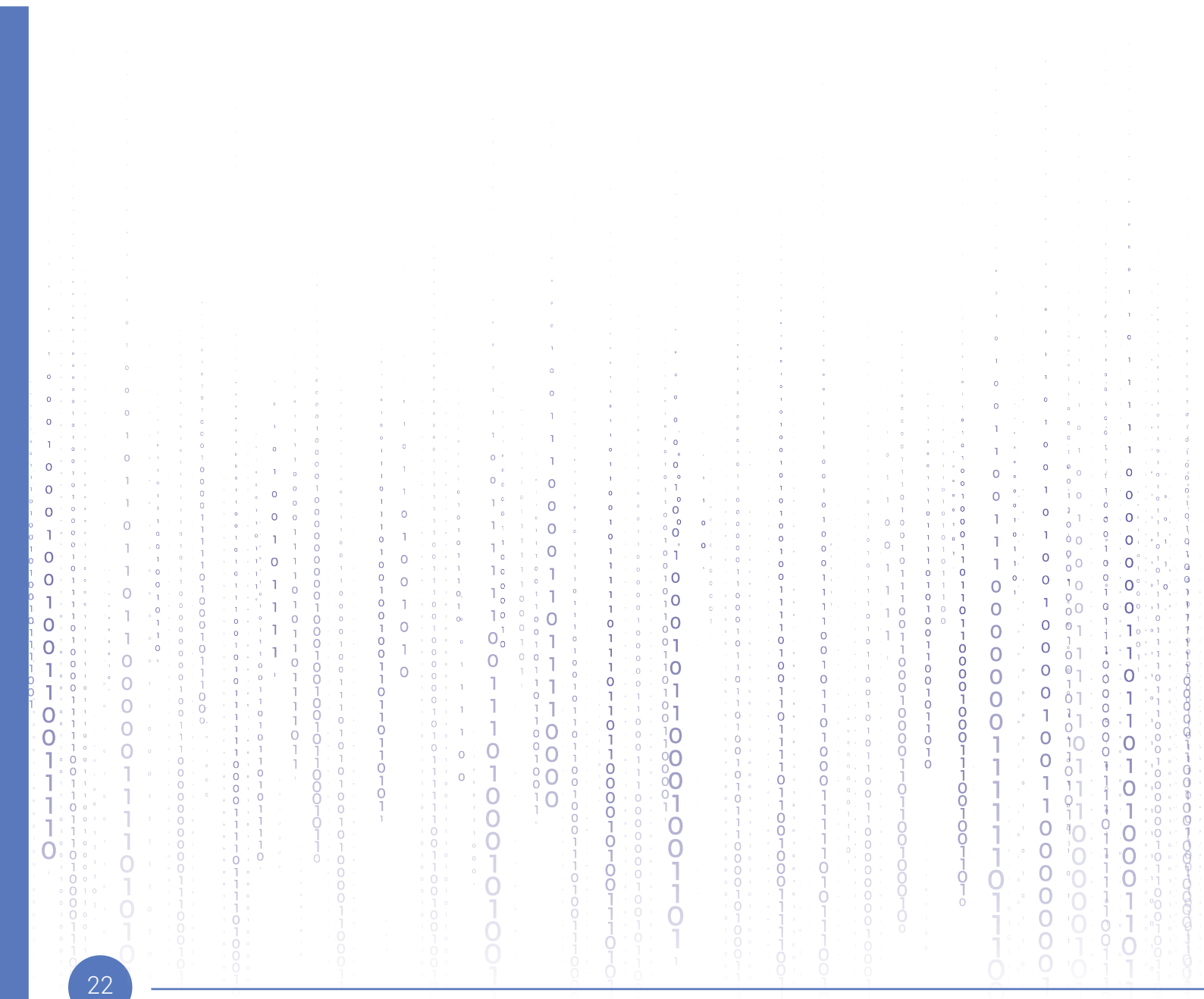
With ByteChek, our fully integrated platform streamlines and automates the SOC 2 readiness assessment process accelerating your organization towards a SOC 2 Type 1. Within minutes of onboarding, you will receive detailed recommendations for controls not suitable, and also have a clear understanding of which controls are already in place. Our platform is able to quickly identify controls that meet the criteria for your SOC 2 Type 1, and testing is complete in minutes, freeing up your team to focus on controls that need a little extra work.

Some companies may only do a Type 1 report year-over-year as a way to show their control environment to customers, but those customers do not have a need to see operational effectiveness. A SOC 2 Type 2 report includes everything from the Type 1 (suitability of design), but also will show the operational effectiveness of controls over a period of time. To be operating effectively, it has to show repeatable evidence that the control functioned as described. That’s why Type 1 covers “is it designed correctly?” and Type 2 covers “did it operate that way over this period of time?”.

Most companies end up on an annual SOC 2 Type 2 cycle where the prior 12 months are looked at for operational effectiveness. This report details the auditor's testing of the controls and the results of tests as well. Most of your customers or business partners will look for a Type 2 report as it is the highest level of scrutiny of the control environment. If you satisfy that, they are satisfied too.

Type 1 / Type 2 - similar reports, yet with different purposes. Are you looking to showcase your control environment and how it meets the criteria? Type 1 is for you. Are you looking for that, but also show how your controls operate? Type 2. In the end, you will have to determine which report is appropriate for the stage that your company and your control environment is in.

So which type of SOC 2 is right for you? It will depend on your situation, budget, and customer needs of course, and many companies will go the route of readiness > Type 1 > Type 2 for their SOC 2 journey.





Chapter 5

What's in a System Description (SOC 2 - Section 3)

Introduction

For most people, when they think of SOC 2 reports, they think about the auditor's opinion and the controls (in section 4). But there is another vitally important section of a SOC 2 report, and that is the System Description (section 3). The reason this is so important is that, ultimately, it is what your SOC 2 report opinion is on. Wait, what? The opinion isn't just about controls you say? That is absolutely the case and the system description is probably the biggest reason why it's vital for your SOC 2.

This chapter is going to let you know more about the SOC 2 system description, what it is, what needs to be included in it, and some tips on how to make it easier when developing your SOC 2 report.

What is the system description and why is it important?

The system description is exactly what it says. It's a description of the system that is being reported on in your SOC 2 report. It is important because it gives your report users an overall understanding of your service and the system that is supporting it.

In your management assertion, the very first statement is, "we have prepared the accompanying description of XYZ's _____ system…". That statement goes on to have language about the description being presented in accordance with the AICPA's description criteria (DC 200) and what the purpose of the description is (to inform report users about useful information related to assessing the risk of using your system - including the controls). There is also an explicit statement that the controls stated in the description were suitability designed (and operating effectively - Type 2) in order to achieve commitments and system requirements based on the applicable trust services criteria. So really, the controls are already in the description. Section 4 of the SOC 2 report is a means of displaying those controls, how they map to criteria, and (in Type 2) the auditor's tests of controls and results of tests.

That in turn means that the CPA's opinion, because it is essentially an opinion on the reasonableness of management's assertion, is really about the system description in addition to the testing of those controls for suitability and operational effectiveness. That's why the system description is so important. A poorly written description will not meet the requirements and therefore delay your SOC 2, or worse yet, result in a qualified opinion.

OK, so what's in the system description?

The AICPA has provided a benchmark of 9 criteria for system descriptions of SOC 2 reports. They are as follows:

1. **Types of services provided** - This is pretty straightforward. Here you will describe what services your company provides as it relates to the system in scope. There are a couple of key things to remember for this criterion. Some companies opt to describe their entire business in general, which is acceptable, but really this criterion should mostly focus on the system under examination. Another common theme we have seen in the past is companies using their marketing language in this section to describe the system (think "XYZ Corp., a world-leader in _____" or "providing the best service in the industry" and even "_____ system saves customers money by…". Think about what we discussed above. Management's assertion is about this description, and then the CPA's opinion is about the reasonableness of the assertion. These types of statements are not measurable and are really just "sales" language. Stick to the facts of what the system is and does.

2. **Principal service commitments and system requirements** – Commitments and system requirements are crucial for the entire SOC 2 report. This section lets the reader know what those commitments and system requirements are, and where they come from (SLAs, contracts, etc.). This helps give the reader context as to what trust services categories are in-scope and why.

3. **Components of the system** - This is where the description begins to get a little technical. The components described here include the infrastructure, software, people, procedures, and data that support and make up the system. For many Cloud Service Providers (CSP), the infrastructure section will include their hosting provider (such as Amazon Web Services). The Software section should list your software and applications that support service delivery1. The People section should include a high-level overview of the departments or key personnel that support the system and what they do. Procedures should also be high-level, stating what procedures are and their purpose, but we recommend leaving the details of controls for later in the description. Data should discuss what the data is that the system processes (what is your customer data), as well as any other data types that directly supports the system.

4. **System incidents** - This part of the description should discuss any security incidents that rose to the level where your company failed to either meet criteria, your commitments to customers, or your system requirements.

5. **Applicable trust services criteria and related controls** - This is probably the most "bulky" criterion of the system description. In this section, you will state the criteria that are in-scope so that the reader understands the criteria you are being measured against. That part is pretty standard. After that though, is where it gets super detailed. This is where you are going to discuss your control environment and describe the controls that support it. Things like logical access, change management, risk assessment and mitigation, communication, and other information are all included here, and essentially, this is where your auditor would find and pull your controls from that get tested in section 4. We recommend that you lay this section out similar to how the criteria are set up in section 4, which makes it easy for your report users to be able to understand your control environment as it relates to the criteria. Start with the control environment, information and communication, risk assessment, etc. See the link above to read in more detail about the criteria to help you develop this part of your system description.

6. **Complementary user entity controls (CUECs)** - A very important part of the description, CUECs are the controls that your customers need to have in place in order for the system and control environment to be complete and achieve its objectives. For example, maybe your customers need to have their own logical access controls in place so that only authorized users access your service, otherwise, unauthorized access may cause you to fail to meet your security commitments. The important thing to remember with this section is that it should not be a "laundry list" of things that you want customers to do in order for you to be covered in case something happens. That is what your contracts and agreements are for. This is purely just meant for controls they need to have in place otherwise your system doesn't work to meet its objectives.

7. **Complementary subservice organization controls (CSOCs)** - This criterion is where you will discuss the subservice organizations that support your system and control environment. Subservice organizations are a bit more involved than your vendors (or sometimes even critical vendors). Think of subservice organizations as a vendor that cannot meet your criteria, commitments, or system requirements. For most CSPs, that is going to be your cloud hosting provider (AWS, GCP, Azure, etc.). For example, you cannot meet the physical controls in CC6.4 or CC6.5 without them. So, you would list them here and what criteria they help you meet. Because you are only describing them in the system description, but not testing any of those controls (AWS isn't letting you visit their DCs), most subservice organizations are "carved out" of the opinion in a SOC 2 report.

8. **Specific trust services criteria not applicable to the system** - This is where you would describe any criterion that is not applicable to your system and why. An example could be where you have privacy in scope for your SOC 2, but you are not a data controller. Therefore, things like the notice, choice, and consent criteria in privacy would be not applicable.

9. **Significant changes to the system during the period (Type 2 reports only)** - In a Type 2 report, if you had any significant changes (how the control environment operates, control changes in how they meet criteria, key personnel changes, mergers/acquisitions, etc.) during the period, you would state those here and their effect on the report.

System descriptions contain a lot of important information for your users. That information has repercussions throughout the whole report, so making sure your description is well-done and accurate is crucial for your audit.

P.s. We are automating the system description in our product, send us an email to hear more



Chapter 6

AICPA SOC 2 Trust Services Criteria 101

Introduction

The AICPA Trust Services Criteria. It's what drives SOC 2 reports. That is because they were designed by the AICPA for use in attestation or consulting engagements. They are the primary means that you and your CPA use to measure and report on your controls for the trust service categories. You have probably heard of those categories: Security, Availability, Processing Integrity, Confidentiality, Privacy. In this chapter, we're going to dive into the details of the criteria including the why, how they are used, and what they mean for SOC 2.

What are the trust services criteria and why are they important?

The trust services criteria ("TSC") were developed by the AICPA as a means to measure the suitability of the design and operational effectiveness of controls relevant to how a system handles security, availability, or processing integrity of its information. The criteria cover how that system handles the privacy or confidentiality of that information as well. These criteria (and trust service categories) are what SOC 2 primarily is focused on.

The TSC were designed considering the risks that threaten a company's ability to meet its objectives for the internal control system. A company will address these risks through suitably designed controls that, if operating effectively, will help achieve the entity's objectives. The risks that were identified by the AICPA included:

- The nature of a company's operations and the environment in which it operates
- The types of information generated, used, or stored by the company
- The types of commitments made to customers and third parties
- Responsibilities entailed in operating and maintaining systems and processes
- The technologies, connection types, and delivery channels used
- The use of third parties (such as service providers and suppliers), who have access to the system, to provide the company with controls that are necessary, along with company controls, to achieve objectives
- System changes including:
  - Operations and related controls
  - Processing volume
  - Key management personnel
  - Legal and regulatory requirements
  - Introduction of new services, products, or technologies

How the TSC are structured

The TSC are organized in a way that aligns with those risks shown above. First, we begin with the "common criteria." These are applicable to any of the trust service categories. The common criteria were derived from the COSO 2013 framework and specifically address:

- The control environment (CC 1 series)
- Communication and information (CC 2 series)
- Risk assessment (CC 3 series)
- Monitoring of controls (CC 4 series)
- Control activities related to the design and implementation of controls (CC 5 series)

There are also supplemental criteria for any trust services engagement (think security). Those include:

- Logical and physical access (CC 6 series)
- System operations (CC 7 series)
- Change management (CC 8 series)
- Risk mitigation (CC 9 series)

For pretty much every SOC 2, you will have the CC 1 through CC 9 series included. When you add the other categories (availability, etc.) you have to add supplemental criteria that are specific to that category.

- Availability (A series)
- Confidentiality (C series)
- Processing integrity (PI series)
- Privacy (P series)



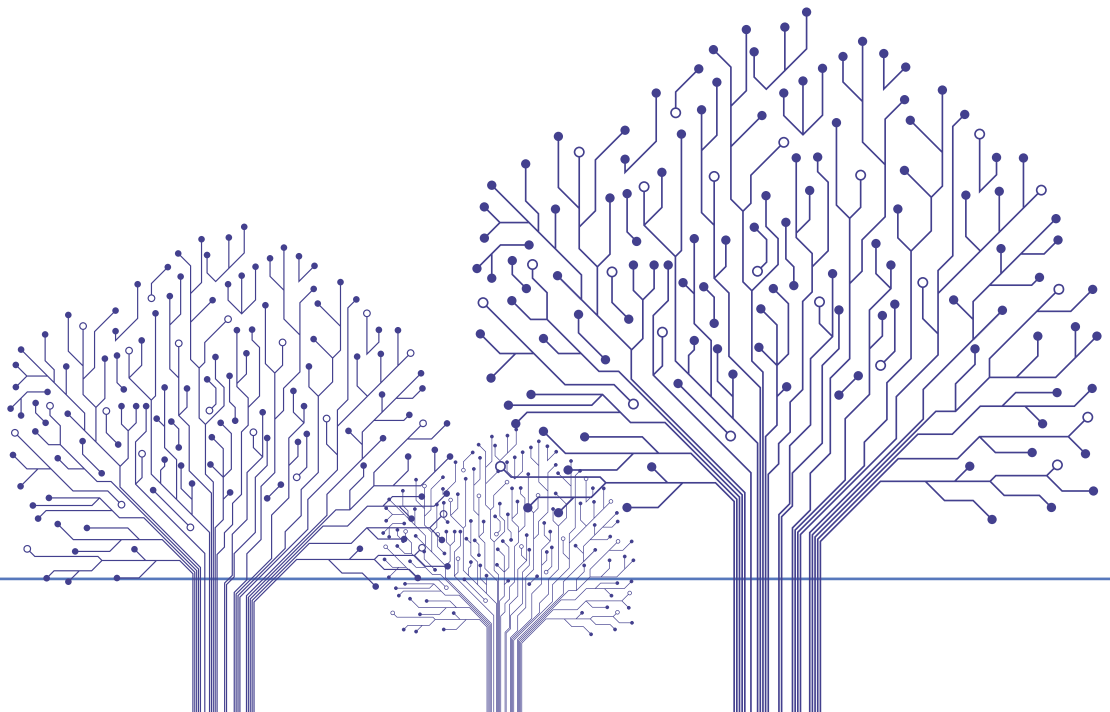
Each series above has a prescribed number of criteria that are intended to meet the objectives of the criteria (for example, objectives related to change management [CC 8]). That CC 8 series has only one criterion associated with it. That criterion for CC8.1, along with the criteria for any of the categories you have in scope, won't change in your SOC 2. Some of the criteria could be N/A for your company (for example, as a cloud provider, maybe you don't handle physical controls in CC6.4), but you would still show the criteria (like CC6.4), and explain why it's N/A to you.

For each of the criteria, you then would show your control(s) that help meet that criterion. There is no prescribed number of controls, or control wording on how to meet criteria. This is because SOC 2 is not a compliance framework, but a reporting framework. Your controls may be worded differently than other organizations. Or maybe you have 3 controls to meet a specific criterion whereas a similar organization has 5. As long as you are meeting the criteria with your 3, that's OK.

What are "Points of Focus" I hear about?

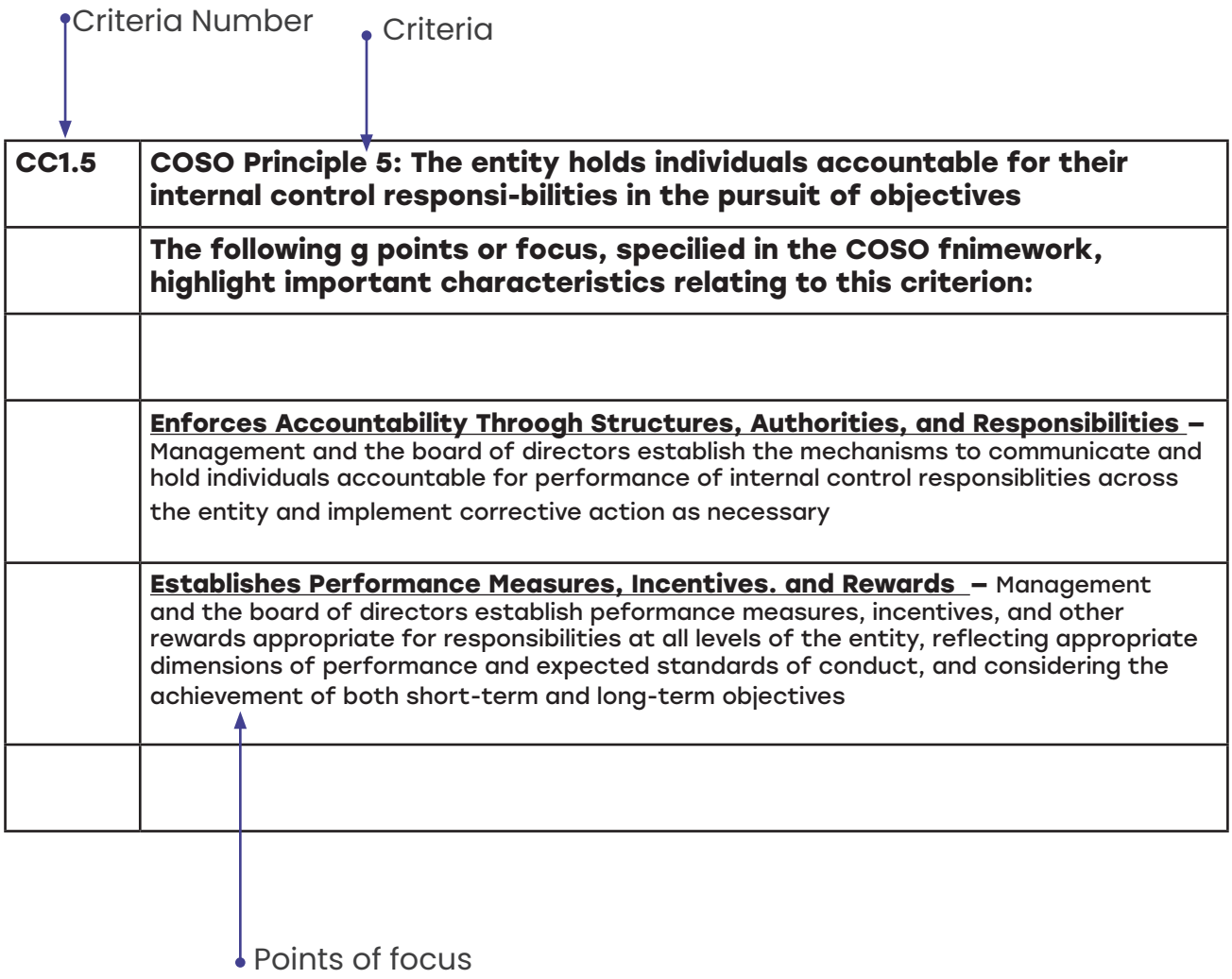
When the AICPA published the Trust Services Criteria, they adopted the COSO idea of having points of focus that relate to each of the criteria. They define it as, "important characteristics of the criteria." The way to think about these is that they are meant as a "guide" for meeting criteria. They are not required, you don't have to have controls that match their verbiage, and you likely won't need controls that relate to every point of focus in order to meet criteria.

If you are building your control environment, and getting ready for SOC 2 however, the points of focus can be great to use as an idea for controls and wording, as well as understanding what auditors and the AICPA are looking for when meeting criteria.

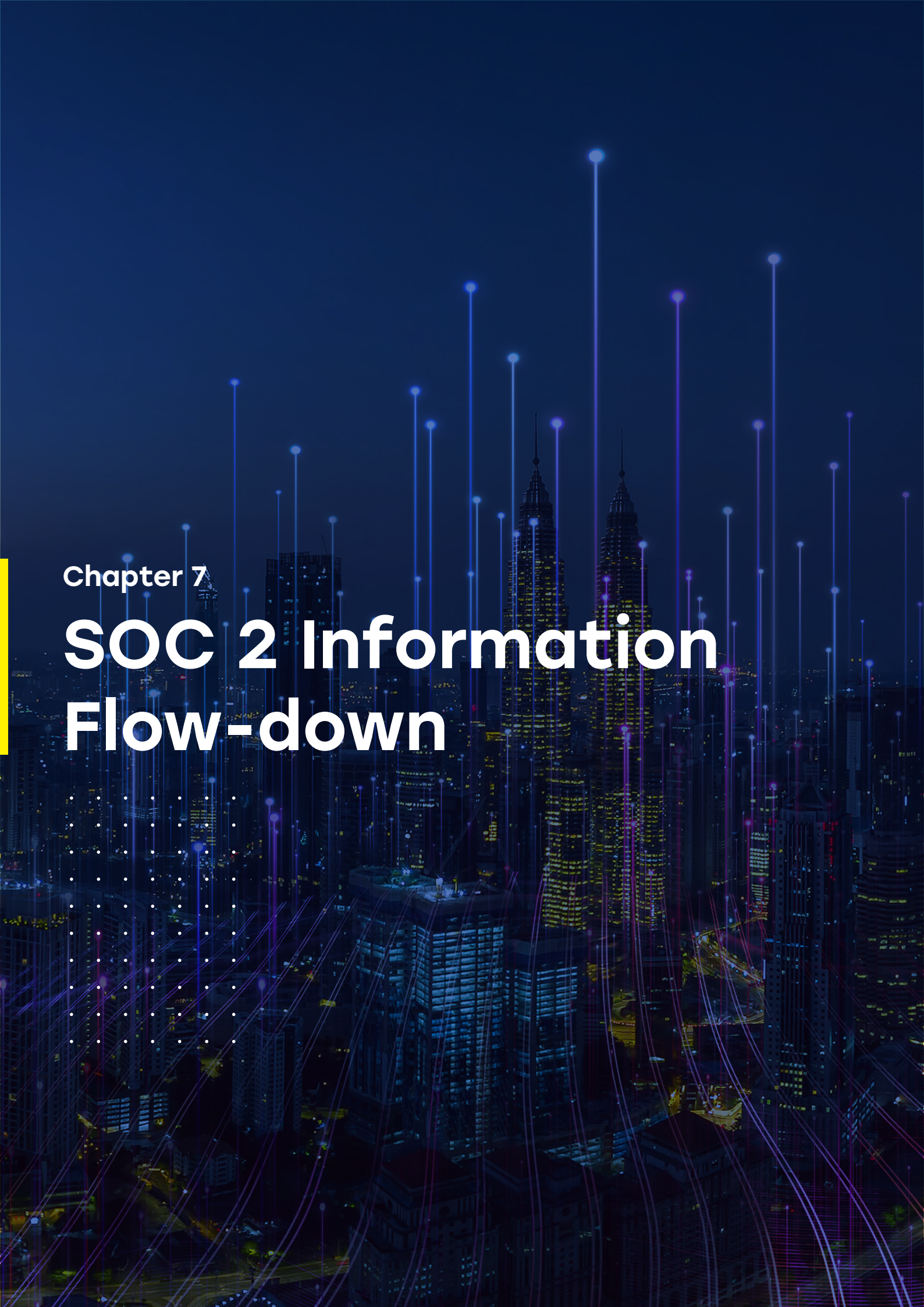


Tips and Reminders for the Trust Services Criteria

The best way to understand the criteria is to read what they are from the AICPA. The criteria listing starts on page 13. Read each one and think of what your company does to meet that criterion. Use the points of focus as a guide to further understand what the criteria is looking for as well. Here is a snapshot of how to read that document:



The trust services criteria are a very important aspect of SOC 2 and are critical to successfully prepare for and navigate through the SOC 2 process. They are also critical in having a "clean" SOC 2. If you fail to meet the criteria, which in turn means you fail to meet your objectives, then you may get a qualified opinion from your CPA in your SOC 2 report. Make sure you take the time to understand the trust service criteria before pursuing SOC 2!

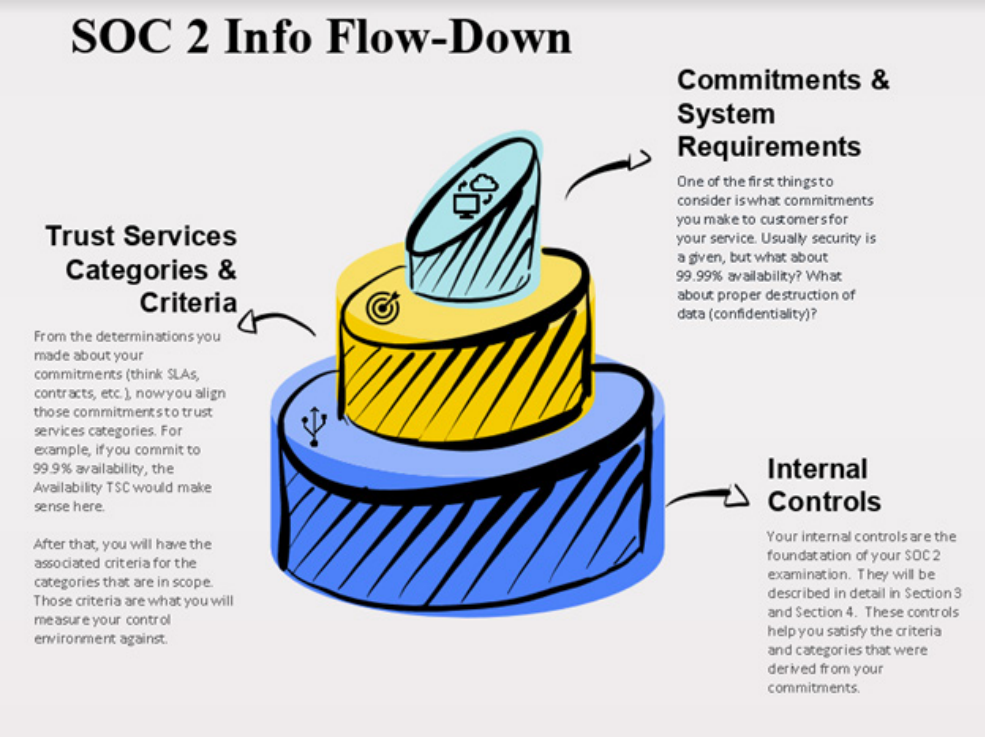


Chapter 7

SOC 2 Information Flow-down

Introduction

SOC 2 is more than just meeting a bunch of criteria with controls. Yes, that is an important part. But why? How does it get to that point? It is important to know the flow of information when it comes to SOC 2 because it will help you make better decisions for your SOC 2, understand how the report works, and know in greater depth the ins and outs of your report. In this infographic blog, we will show you that flow down and explain the details.



The Details

Your SOC 2 starts with understanding the promises or commitments your company makes to your customers. These commitments can be found in customer contracts, service-level agreements, master service agreements, terms and conditions, or other similar documents. From these commitments, you can determine which of the trust service categories should be in scope for your SOC 2. The trust service categories are ultimately what drives the criteria, but more on that in a bit.

The 5 trust service categories that relate to SOC 2 are:

- **Security** - Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the information or systems and affect a company's ability to meet its objectives (think commitments).
- **Availability** - Information and systems are available for operation to meet the company's objectives.
- **Confidentiality** - Information designated as confidential is protected to meet the company's objectives.
- **Processing Integrity** - System processing is complete, valid, accurate, timely, and authorized to meet the company's objectives.
- **Privacy** - Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

It's very likely that you have security included somewhere in your agreement documents with language discussing protection of data, unauthorized access, etc. So, that means for pretty much every SOC 2, security is an included category. It's also likely that you have some language in your agreements about the confidentiality of customer data. Confidentiality in that regard is closely tied to security, but when it comes to the trust services criteria, it has some slight differences. Read more about that here. For the availability category, think about if you are committing to uptime percentages, available hours, etc. In our experience, the Security, Availability, and Confidentiality categories are the most common for SOC 2.

With the processing integrity category, think about it if you are processing data on behalf of your customers. Are you committing to the accuracy, timeliness, completeness of those outputs? I always like to use the example of a payroll processor. They take the raw payroll data of their customers, then they are required to (and commit) to produce timely and accurate payroll reports in order for their customers to make payroll.

With privacy, you really have to think about it from the perspective of if you handle and interact with the information of data subjects. Many people think confidentiality and privacy are the same, but that is not correct for SOC 2. If you do think privacy is in scope, are you providing notice, choice, consent to the data subjects? The ability to opt-in/out? Do you provide them the ability to modify their personal data? It is important that this is applicable to the service in scope for your SOC 2 not just your public website.

Once you know your categories, the criteria are easy because they are already set by the AICPA. For each category, there are prescribed criteria that your organization has to meet. In the end you have your controls in place that satisfy those criteria, which in turn satisfy the in scope categories, which ultimately determines if your system is meeting its commitments and system requirements.

So, if you think about it, it really all comes down to your commitments to customers and what your system requirements are to meet those commitments. Determining those correctly flows down to everything in your SOC 2. It also determines what type of report opinion you'll get if you meet those commitments and system requirements or not.





Chapter 8

SOC 2 Report Opinions

Introduction

SOC 2 reports are attestation reports. With those types of reports, the Certified Public Accountant or CPA (i.e. service auditor) will have an opinion on management's assertion as it relates to the system and its ability to meet commitments, system requirements, and objectives. This short chapter will show you the various types of report opinions that SOC 2 can result in, and what each means.

The different opinions

The first and most common SOC 2 report opinion is **unqualified**. Basically, that means it's a "clean" opinion. No issues were noted in the description, controls, testing, etc. that would cause a modification of the opinion, and management's assertion is deemed reasonable. This is the type of opinion you should be striving for. When you hear people refer to "passing" a SOC 2 examination, they are more than likely referring to an unqualified opinion.

The two main factors that drive the other opinions are scope limitations and material misstatements. A scope limitation is when your company is not able to provide evidence for the auditor. Material misstatements can happen due to a system description being misstated, controls not designed appropriately, or controls not operating effectively (exceptions or deviations in the testing of controls). A control may have failed due to these exceptions, which in turn caused you to fail to meet criteria appropriately or fail to meet commitments or system requirements (this is the most common cause of opinions other than unqualified). For example, a common control in a SOC 2 report is a requirement to perform risk assessments on at least an annual basis. If you did not perform a risk assessment within your testing period, this would be a control failure and would be denoted as an exception or deviation in your report.

The next most common is a **qualified** opinion. This means that the report was mostly OK, but there was an issue somewhere. If there was a scope limitation and/or material misstatement, it might be material to the report (causing the qualification), but not pervasive enough to go any further. Should you panic if you have a qualified opinion? NO! Qualified opinions are more common than you think. Exceptions happen. It's not the end of the world. Especially if it was one control that had an exception and everything else was fine. Many firms opt to explain their exceptions and why it was a rare occurrence or how they fixed it in an optional "unaudited" section of the report for management to respond to exceptions in testing (section 5 of the report).

Less common is the disclaimer of opinion, which mostly results from if there was a severe inability for your company to produce evidence for the examination (the scope limitation was material and pervasive).

The least common is the adverse opinion. This rare report results from if there were material misstatements that were both material and pervasive to the point that the control environment is pretty much failing to meet either criteria, commitments, system requirements, or objectives.

Here is a graphic to help visualize how the opinions (other than unqualified) can happen:

SOC 2 Reports

Report opinions other than unqualified

Byte/Chek

What caused the modification of the opinion	Service Auditor's Professional Judgement About the pervasiveness of the effects on the Opinion of the Report	
	Material but Not Pervasive	**Material and Pervasive**
Scope limitation. An inability to obtain sufficient, appropriate evidence.	Qualified Opinion	Disclaimer of Opinion
Material Misstatements • Description misstated • Controls not suitably designed to provide reasonable assurance that the commitments or system requirements were achieved • Controls not operating effectively	Qualified Opinion	Adverse Opinion

You should always strive for an unqualified opinion for your SOC 2. The first step in that is to make sure you have a solid control environment that is designed appropriately. A ByteChek readiness assessment is a great way to get that started! Once suitability is determined to be OK (we recommend a Type 1 report), just to make sure you operate your controls as described. If you do, you will reduce your likelihood of exceptions in testing, paving the way for your unqualified SOC 2 Type 2 report.



ByteChek

About Us

OUR PHILOSOPHY

We found out first-hand how difficult, time-consuming, and expensive assessments can be – and we knew there had to be a better way. We asked ourselves, "What can we do to make this suck less?" We've taken our experience and built our philosophy around how to answer that question. That's why we built ByteChek.

With our extensive experience in SOC 2 and other cybersecurity assessments for SaaS, IaaS, and PaaS providers we have developed a platform to help our clients make their assessment process easier. We built our product, processes, and reports with that expertise in mind. In turn, we created a more integrated and secure product that provides minimal disruption to the everyday operations of our client's business.

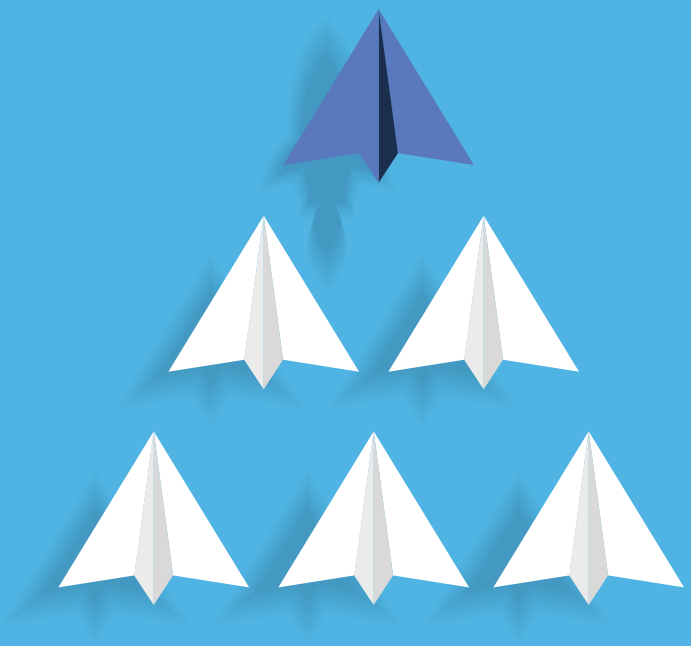
OUR LICENSES & CERTIFICATIONS

The team at ByteChek has various licenses and certifications relevant to our professional services, including the following:

- Certified Public Account (CPA)
- AWS Certified Solutions Architect-Professional
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- AWS Certified Security-Specialty
- AWS Certified Solutions Architect-Associate
- Certified Information Technology Professional (CITP)
- Certified Information Privacy Technologist (CIPT)
- ISO22301 Lead Auditor
- Certificate of Cloud Security Knowledge (CCSK)
- AWS Certified Sysops Administrator – Associate
- AWS Certified Developer Associate
- AWS Certified Cloud Practitioner

About Us

OUR LEADERSHIP



Our dedication to our philosophy stems from our experience as auditors, partners, and cloud security advisors. We've been through hundreds of cybersecurity assessments – responsible for consulting and assessing organizations of all sizes from startups to the Fortune 500. Our leadership team was also part of the working group that helped develop the 2018 version of the AICPA SOC 2 guide and has developed numerous trainings for the AICPA.



AJ Yawn
CEO



Jeff Cook
CFO

ByteChek

877-537-3734

info@bytechek.com

936 SW 1st Ave #376
Miami, FL 33130

