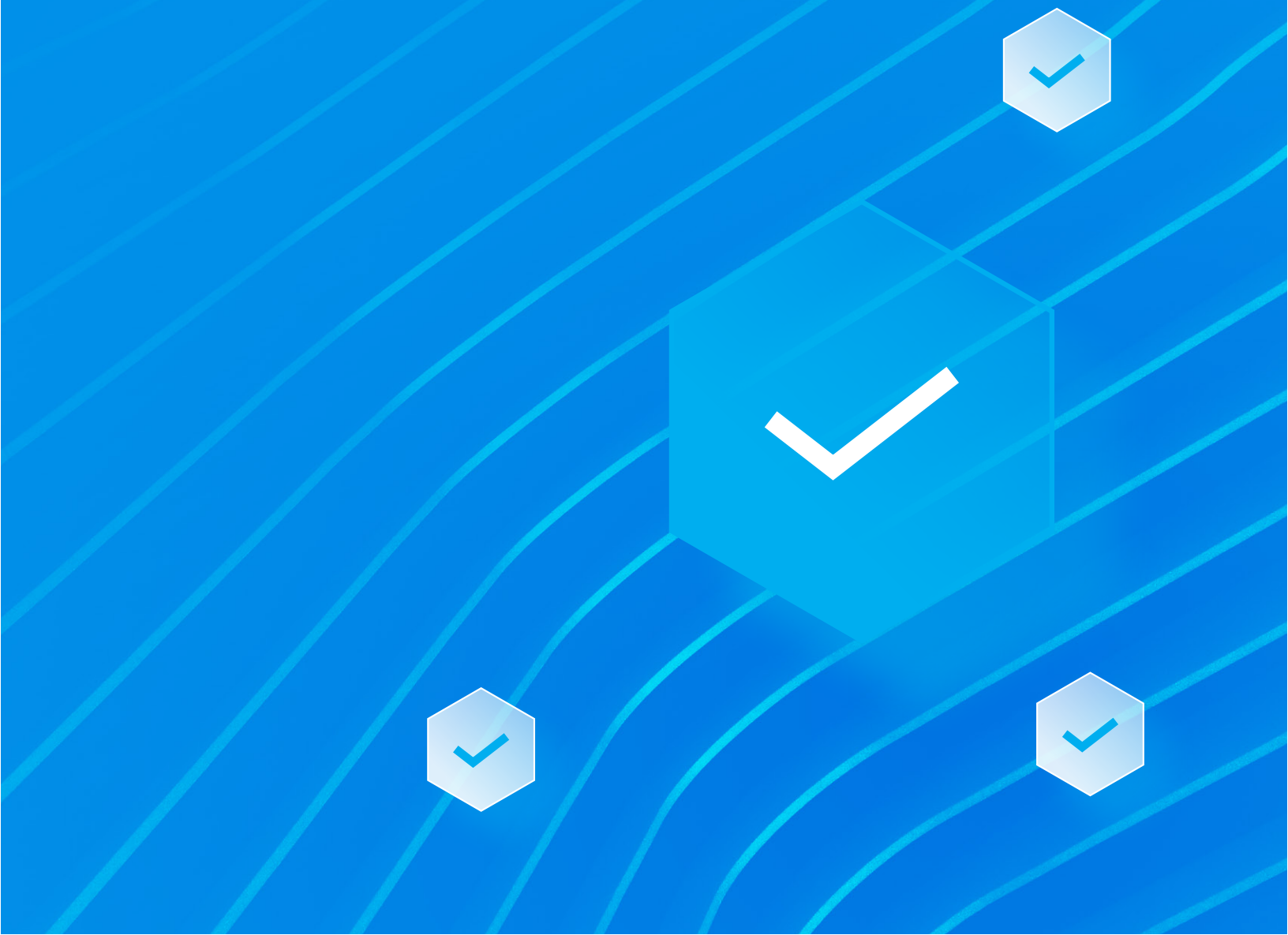
DuploCloud

WHITEPAPER

The Complete SOC 2 Compliance Checklist



CONTENTS

INTRODUCTION

Achieving SOC 2 compliance is critical for launching a world-class, consumer-facing product — especially if your business stores and manages customer data. SOC 2 compliance is a rigorous set of checks and controls that provides customers and future business partners with the peace of mind that your infrastructure has the necessary guardrails to keep data private and secure, with minimal downtime of critical systems.

Earning SOC 2 compliance can be a lengthy and complex process. We at DuploCloud have designed this checklist to guide you each step of the way, from determining which type of SOC 2 report you need and which criteria you need to audit to the best ways to ready your infrastructure for the final exam.

However, there is no one-size-fits-all solution for SOC 2 compliance, so organizations will need to adapt this checklist to meet their needs. However, we will paint a broad enough picture to ensure your enterprise has a solid foundation to begin its journey to achieving compliance.

Read on to get started.

WHAT IS SOC 2?

The **System and Organization Controls (SOC)** are compliance standards created by the **American Institute of Certified Public Accountants (AICPA)** to help organizations develop processes that keep customer and financial information private and secure.

SOC 2 is a specific form of compliance standards focused on customer data; while not required by law, achieving SOC 2 compliance lets the public and business partners know that your organization is taking customer data security seriously.

TRUST SERVICES CRITERIA

Organizations achieve SOC 2 compliance by adhering to one, several, or all of five designated **Trust Services Criteria** (TSC):

The only required TSC needed to achieve SOC 2 compliance, this criterion governs how businesses store information and protect systems against unauthorized users and malicious actors. Data breaches can lead to expensive lawsuits and a loss of customer and client trust, so achieving this criterion is paramount.

This criterion determines how readily available systems and information are for users. Unscheduled downtime can impact your organization's bottom line. It can also affect how customers perceive the reliability of your services, especially if customers need immediate access to sensitive data or critical infrastructure.

This criterion ensures that system processes are accurate, fast, and validated. For example, if a user submits an online form, that information should be accurately processed and stored with the exact information the user submits. Failing to maintain reliable processes can lead to administrative headaches among staff and a lack of trust from customers.

This criterion specifies how organizations protect sensitive information and ensure that only authorized users can access this information. For example, specific laws may govern how certain confidential documents are stored and accessed (e.g., HIPAA regulates patient health information).

This criterion governs how personal information is collected, stored, and used to protect it from malicious actors. The privacy criterion is broader than confidentiality, as it applies to all user data, not just designated confidential information.

ACHIEVING SOC 2 COMPLIANCE

To attain SOC 2 compliance, your organization must undergo an external audit from a licensed third-party CPA. The auditor will walk you through the entire process, which may include interviews with key staff, sitting in on meetings, and a review of internal systems.

It's important to note that the audit process has no rigid structure, as each organization will have its own internal procedures and security needs. This makes it challenging to provide a single path to achieving SOC 2 compliance, but it also provides freedom in getting there. Remember, Security is the only required TSC — your organization can determine which other TSCs apply and implement controls that satisfy those requirements.

BENEFITS OF SOC 2 COMPLIANCE

While U.S. law does not require SOC 2 compliance, organizations seek it out for several reasons, including:

Strengthening processes and shoring up deficiencies:

Every organization needs to address its weak points. Undergoing a SOC 2 audit is a fantastic way to analyze current processes and make adjustments to strengthen your business's security posture.

Prevent the loss of data, revenue, and reputation:

No business wants to find itself a victim of a data breach. SOC 2 compliance reduces the risk of unauthorized access and maximizes the privacy of sensitive information.

Make security a selling point:

Potential customers and business partners want to know that you take security seriously. With SOC 2 compliance under your belt, you can quickly inform your customers that your processes have undergone rigorous examination.

FAILING TO ACHIEVE COMPLIANCE — THE HIDDEN COSTS

While SOC 2 audits can be expensive and time-consuming, failing to achieve compliance can result in direct and indirect costs to your business. Being proactive and implementing automated compliance scanning tools like DuploCloud will ensure that your organization saves money in the long run and prevents adverse outcomes, such as:

- **Loss of opportunities:** Many businesses looking to partner with your organization will only do so if you've achieved SOC 2 compliance. Failing to do so will lock you out of these partnerships, leaving money on the table.
- **Fallout from data breaches:** SOC 2 compliance ensures that you've achieved a baseline of security when managing customer data. If you suffer a data breach, lawyers can likely use the lack of compliance against your organization during a class action lawsuit.
- **Reputational damage:** Being compromised will make customers and other businesses think twice about trusting your organization with sensitive information.

SOC 2 COMPLIANCE CHECKLIST

Step 1:

☐ **Determine the Scope of the Audit**

- ☐ SOC 2 Type 1 Report Requested
- ☐ SOC 2 Type 2 Report Requested

Step 2:

☐ **Determine Which Trust Services Criteria You Will Meet**

- ☐ Security (Required criterion)
- ☐ Availability
- ☐ Processing Integrity
- ☐ Confidentiality
- ☐ Privacy

Step 3:

☐ **Complete Readiness Assessment and Gap Analysis**

- ☐ Readiness Assessment Completed
- ☐ Gap Analysis Completed

Step 4:

☐ **Close Gaps**

Step 5:

☐ **Begin Audit**

- ☐ Find auditor
- ☐ Provide information on scope and TSCs
- ☐ Allow auditor to conduct fieldwork
- ☐ Receive report

STEP 1

DETERMINE THE SCOPE OF THE AUDIT

Before you begin the audit process, you need to determine which aspects of your organization's infrastructure, data, policies, tech stack, and other processes will undergo an audit, as well as the time you have available to handle the audit process.

This step is crucial because it will determine which type of SOC 2 report you need, which will determine your overall timeline and budgetary requirements to complete a SOC 2 audit.

There are two types of SOC 2 reports available:

	Type 1	Type 2
What it audits:	Processes and controls at a specific point in time	Processes and controls over an extended period
Purpose of report:	Determines process design quality at a conceptual level	Determines the effectiveness of controls during practical application
Timeframe needed:	A few weeks	Several months, usually six at minimum
Which report is right for you?	For start-ups who need to go to market quickly and prove compliance, or businesses that haven't started SOC 2 compliance process before.	For businesses and enterprises that have already received a Type I report, have clients or partners specifically requesting a Type II report, or have more time to go to market.

STEP 2

DETERMINE WHICH TRUST SERVICES CRITERIA YOU WILL MEET

Once you've determined which report you'll need to audit for, it's time to determine which Trust Services Criteria your audit will cover.

Your services and access to customer data will largely determine the TSCs you need to meet. Not all organizations need to (or likely should) meet all criteria, so examine your current processes and map them to their respective TSC.

Security is the only required criterion to achieve SOC 2 compliance. Still, your industry, customer location, as well as federal and local laws may necessitate specific requirements (such as HIPAA, GDPR, etc.), so be sure to keep these regulations in mind as you conduct your internal assessment.

Complete the following checklist to track the TSC you plan to audit:

- ☐ **Security (Required criterion):** How does your system protect your business and its customers against unauthorized access?
- ☐ **Availability:** Are services available when clients need them?
- ☐ **Processing Integrity:** Is service reliable and free of errors? How does the system handle failure? Can you repeat processes at scale with consistent results?
- ☐ **Confidentiality:** How does your system handle sensitive data?
- ☐ **Privacy:** How do you keep information protected and anonymous?

STEP 3

COMPLETE READINESS ASSESSMENT AND GAP ANALYSIS

Before beginning the official audit, you should perform an initial readiness assessment to determine your organization's current security posture. Not doing so can lead to wasted time and money on a failed audit.

Third-party auditors are responsible for performing the readiness assessment; they will examine how effective your current systems and policies are in regard to SOC 2 specifications. The readiness assessment will not be as thorough as a full audit but will provide you with areas that may crop up as potential failure points when you conduct a full audit.

Once you've completed a readiness assessment, it's time to conduct a gap analysis. This is where you will compare your assessment results to your current systems and lay out the steps you'll need to take to close any gaps. This may require adjusting configurations, redesigning internal processes or procedures, or implementing entirely new systems.

It may be difficult to track and monitor all aspects of your infrastructure, especially as systems are live and continuously updated. Implementing automated tools like DuploCloud will be invaluable in analyzing potential gaps and building remediation processes through continuous active monitoring and alerting to variances from SOC 2 standards, after-rules configuration, and reconciliation.

STEP 4

CLOSE GAPS

Once the gap analysis is complete, begin shoring up gaps to ready your organization for the official SOC 2 audit. Implement controls, update configurations and processes, and take other steps to remedy any lingering deficiencies. Also, be sure to revise affected training and documentation to reflect new, updated processes.

STEP 5

BEGIN AUDIT

Once your organization is confident it has completed the remediation of the readiness assessment and gap analysis, it is ready to begin the official SOC 2 audit.

First, you must select a SOC 2 auditor. They must be accredited by the AICPA, qualified and experienced with your organization's industry, and understand your tech stack. Interview auditors and ask questions about their background and experience before making a selection.

After selecting an auditor, you will provide them with the necessary information regarding your chosen scope and the TSCs you plan on auditing.

The auditor will then begin fieldwork, which may include:

- Facility walkthroughs
- Sitting in on internal meetings
- Interviews with employees
- Manual review of systems and processes
- Investigation of onboarding processes and security checks
- Code review
- And more.

Depending on the scope of your report, this process may take anywhere between a few weeks and several months. Once finished, you will receive a written report featuring your audit results. There are four types of opinions that you may receive:

Unqualified	Your organization's security controls are effective, and you have fully passed the audit.
Qualified	Some of your organization's controls are ineffective, though issues may not impact all users or processes. The audit is considered failed, though users can generally rely on the security of your system even with qualifications.
Adverse	Many of your organization's controls are ineffective, and users cannot rely on your system's security. The audit is considered failed.
Disclaimer	The auditor did not have access to the necessary information or systems to form an opinion. The audit is considered failed.

The best outcome is an unqualified opinion. If you receive any other opinion, you will receive additional information describing the reasoning behind the opinion, helping you make further adjustments before attempting another audit.

ABOUT DUPLOCLOUD

Manually achieving SOC 2 compliance is a monumental task, especially for organizations operating at the scale needed to compete in today's landscape.

That's why we developed DuploCloud: a DevOps-as-a-Service platform that automates the Infrastructure-as-Code framework construction, security protocol integration, and compliance enforcement necessary to build cloud-native applications at scale. DuploCloud's automated scanning tools will detect security or compliance issues against specifications mapped directly to SOC 2, PCI DSS, HIPAA, HITRUST, and GDPR's set of controls. When coupled with DuploCloud's powerful audit-ready reporting tools, you'll know what's working, what isn't, and how to fix it.

LEARN MORE

DuploCloud can help you get and stay SOC 2 compliant, and ensure your customers' data remains safe and secure.

Contact us today at sales@duplocloud.net for a personalized one-on-one walkthrough, and see DuploCloud in action for yourself.