controlmap

Getting started: SOC 2 Compliance Guide

Get answers to your SOC 2 compliance questions.

Foreword

As data breaches, malicious attacks, and ransomware continue to rise, every business is diligently evaluating with whom they do business. Every company has the same questions on its mind with regards to its data's confidentiality, integrity, and availability.

- Whom can I trust with my data?
- What security assurance does my vendor provide?
- Is the vendor doing enough to secure my company's data?

Pallav Tandon
CEO, ControlMap
pallav@controlmap.io

Every day it’s becoming more evident that business growth depends on how much trust your business can garner in its industry, customer base, and partner ecosystem.

In this ever-changing and evolving security ecosystem, businesses and service providers are looking for a common language to discuss trust, security assurance, and data protection. Various industry cybersecurity compliance standards such as SOC 2, ISO 27001, HIPAA, and NIST have become this language in the last couple of years. Demonstrating compliance to these standards communicate a great deal about a company’s cybersecurity practices and procedures, helping stakeholders and customers make well-informed decisions with confidence and trust.

This eBook is about the steps a company can take to achieve SOC 2 Compliance. I hope you find this eBook helpful and that it becomes a valuable source of information for your SOC 2 compliance journey.

Contents

SOC 2 Compliance Guide

1. Introduction

1.1 What is Cybersecurity Compliance

Cybersecurity compliance is a measure of cybersecurity maturity that an organization demonstrates by the polices, procedures and standards it has established for its employees, partners, systems and other assets.

Due to ever-increasing threats and cyber attacks, cybersecurity is no more just a best practice. It's a requirement, regulation, and a mandate in many industries, primarily financial, healthcare, and industrial sectors.

There are many standards, old and new which a company can align to demonstrate compliance and cybersecurity maturity. The choice of a framework to which a company aligns to, is driven by its industry, type of data and risk to that data.

Standards, such as ISO -27001, HIPAA, SOC 2, CMMC, FFIEC and FedRAMP, all cater to different scenarios and industries but all of them define requirements that, when successfully met, provide a way for the company to confidently claim a level of process and security maturity. Each standard lays emphasis on different areas of cybersecurity but all of them in one way or another address the CIA (Confidentiality, Integrity and Availability) triad goal of cybersecurity.

C: Confidentiality - Make sure only the people who require access to data have access, also make sure that everyone who needs the data can access it.

I: Integrity - Is this data the correct data? Make sure no bits were lost, making sure no web address was changed, and even making sure that unauthorized people cannot change your data.

A: Availability - Make sure your data is available for critical processes in time.

In this paper we focus on Service Organization Control (SOC) 2, a compliance standard defined and developed by the American Institute of Certified Public Accountants (AICPA) for service organizations

2. SOC 2 Overview

2.1 What is a SOC 2 audit

According to AICPA (the governing body that develops, and maintains guidance on SOC 2 reports), a SOC 2 report is a "Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy."

Simply put, SOC 2 is an audit of your company's cybersecurity controls that is performed by an AICPA-certified third-party Certified Public Accountant (CPA).

Being SOC 2 compliant means that your company fulfills all AICPA requirements for a SOC 2 audit and there are no negative findings during the audit.

The SOC 2 report itself is an outcome of the examination of the company's cybersecurity controls in the areas of **Security, Availability, Processing Integrity, Confidentiality, and Privacy**.

The examination of these controls is broadly aligned to the four areas of

- Policies
- Communications
- Procedures
- Monitoring

SOC 2 Trust Services Criteria

Security
Evaluates the protection of Information Security Systems from unauthorized access and other threats that could impact the security.

Confidentiality
Ensures that all customer data by a service provider is kept confidential and protected from unauthorized access.

Processing Integrity
This trust principle requires that a company processing data ensures to maintain the input and output integrity of the data being processed.

Availability
Ensures that the processing and storage facilities of a company are available to fulfil the objectives of the company and its customers.

Privacy
Ensures that all personal data of customers are kept private and proper consent and data deletion processes are in place.

2.2 Who must be SOC 2 compliant?

SOC 2 compliance requirements are primarily designed for service organizations and generally apply to any firm or a company offering services to a customer and are responsible for handling its customer's data with confidentiality, integrity, and privacy.
An annual SOC 2 audit has recently become table stakes for software vendors, software as services companies, and software services providers to do business. Every business must have one to grow, close deals, and keep growing.
A successful and clean SOC 2 Audit report is a strong statement made by your company that you take the Confidentiality, Integrity, and Availability of your and your customer's data very seriously. It helps your company garner more trust from your stakeholders, partners, and customers.

So yes, if you are a services organization handling customer data, it's imperative that you plan for a SOC 2 audit if already not done so.

A SOC 2 audit has many other benefits in addition to business growth and a shorter sales cycle.

1. **Lower risk of data theft or loss:** A SOC 2 audit significantly reduces the risk of harm and loss of reputation due to information theft or loss.
2. **Continuous improvement:** An annual SOC 2 audit enforces a year-over-year improvement in the security of the organization's information assets and processes.
3. **More aware employees and partners:** With each audit, the employees and vendors of the company become more aware of information security policies and procedures.
4. **Peace of mind:** A clean audit outcome provides peace of mind to customers, staff, board members, suppliers, and other interested parties that their information is secure.

2.3 ROI of SOC 2 compliance?

Continuous SOC 2 compliance requires significant investment, management buy-in, and time commitment from resources across various departments in your company regularly. Even if you automate most of the processes around evidence collection and compliance monitoring, there is still a cost of automation tools, third-party audits, external consultants, etc.

Like every other project, your SOC 2 project must demonstrate a significant ROI to justify the ongoing costs.

But how do you measure the ROI of a cybersecurity compliance project such as a SOC 2? After all, compliance projects usually bring qualitative gains and returns, which are hard to measure in precise numbers. Although sometimes this is possible if factors such as the cost of past information security breaches can be estimated.

The sidebar on this page will give you a few tangible and intangible ways to measure the ROI of a cybersecurity compliance project such as SOC 2. (Yes, you can use the same measures for other compliance projects such as an ISO-27001 or HIPAA)

Cost of no compliance

1. Cost of lost or stolen data due to past breaches
2. Ransoms / penalties and fines due to malicious attacks
3. Loss of reputation and business
4. Cost of responding to a security incident

Project Costs

1. Audit / Auditor / CPA fees
2. Vulnerability testing
3. Compliance & Risk management platform
4. Security software costs
5. External consultants
6. Internal security resources
7. Internal IT team resources
8. HR and resource

Benefits

1. Reduced risk of data breaches
2. Streamlined cost effective response to incidents
3. Faster sales cycle
4. More closed business in regulated industries
5. Competitive edge over uncompliant competition

3. SOC 2 Requirements

3.1 SOC 2 trust principles

SOC 2 requirements are categorized into 5 groups called Trust services criteria. These criteria are Security, Availability, Processing Integrity, Confidentiality, and Privacy.
For a service organization to successfully complete a SOC 2 audit, the organization must fulfill all requirements for Security trust services criteria and optionally choose one or all other trust criteria. Below is a high-level overview of the various TSCs and the overarching requirements included for each.

Trust Services: Requirements	Areas covered
Security: This TSC covers 33 requirements with more than 120 points of focus implemented as controls.	It covers Personal Conduct, Corporate governance, Awareness training, Code of Conduct, Access Control, Asset Management, Data Protection, Change Management, Hiring & Termination workflows.
Availability: It has about 15 points of focus typically implemented as controls.	These additional requirements cover current capacity, forecasting system usage demand, data backup, and alternate processing infrastructure.
Processing Integrity: The additional criteria for Processing Integrity have five additional requirements and about 14 points of focus.	Processing integrity covers data related to processing inputs, detection and correction of production errors, and other system processing specifications.
Confidentiality: The additional criteria for Confidentiality specify requirements for an entity to identify and maintain confidential information to meet its objectives related to confidentiality.	This area's controls and requirements deal with protecting, identifying, and maintaining sensitive information.
Privacy: It deals with the additional requirement for handling your customers' and users' private and personal data. There are eight additional requirements to be implemented and 50 points of focus.	The additional requirements for Privacy cover criteria related to choose, consent, and collection of private information, access, disclosure, and monitoring

3.2 Types of SOC 2 Reports

A SOC 2 audit can be conducted in one of two ways, and they are conveniently called Type 1 and Type 2.

- **SOC 2 Type 1**
- **SOC 2 Type 2**

The approach, scope, and time needed for a Type 1 and a Type 2 audit are very different from one another and the effort required will depend on the company's situation, how quickly the report is needed, and how ready and mature a company is with its cybersecurity practices.

SOC 2 Type 1 Report

What is a Type 1 Report?

Type 1 report evaluates the suitability of the design of the controls at a point in time. The auditor assesses the effectiveness of control design and implementation

When to get a Type 1 Report

The company should get a Type 1 report when a report is required on its current design, and they do not have a history of operations and evidence collection. None or very little evidence is required to be presented for a Type 1 audit.

How long does it take?

A SOC 2 Type 1 audit can be completed as little as 3 weeks, but 6- 8 weeks is more common

SOC 2 Type 2 Report

What is a Type 2 Report?

A type 2 report evaluates the design of controls and their operating effectiveness of the controls for a period. This period must be at least six months and no more than 12 months before the Type 2 audit

When to get a Type 2 Report

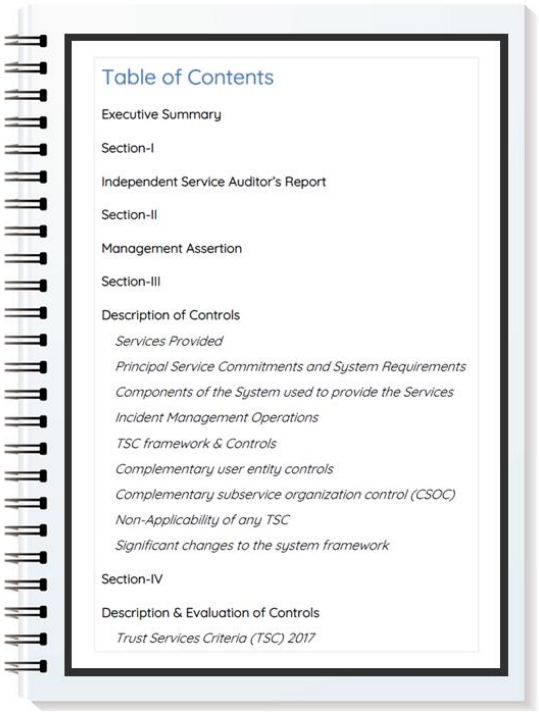
A Type 1 audit must be followed up with a Type 2 report within at least 12 months. Also, if you have demonstrated operating effectiveness for at least 6 months, a type 2 report is desired.

How long does it take?

A SOC 2 Type 2 audit can be completed in 3- 4 weeks, but readiness could take longer as evidence for controls have to be collected for at least 6 months.

3.3 What's in a SOC 2 Report

A SOC 2 report is produced by an AICPA accredited auditor and may vary based on the company's needs, scope, and environment. However, AICPA defines the high-level areas which the report must include



Section-I: Independent Service Auditor's Opinion
This section contains an auditor's opinion after examining the controls of the company information systems in-scope evaluated against the Trust Services Criteria.

Section-II: Management Assertion
An assertion and representation letter provided by the company's management to the auditor in writing asserting that the information provided by the company to the auditor is accurate and current as per their knowledge

Section-III: System description
A section describing the company's in-scope environment, including products and services provided. A description of system boundaries, infrastructure, integrations, software/tools, people, processes and procedures, information/data, data security and encryption, and incident management.

Section-IV : Description & Evaluation of Controls
This section contains description of applicable Trust Services Criteria framework & controls and related Trust Services Principles in the organization. The section also contains description of control objectives, control activities, and control tests and results.

4. SOC 2 Engagement

4.1 Legwork involved in starting a SOC 2 engagement

1

Management commitment

Management sponsorship goes a long way in securing resources, designing and building controls, policies, processes, and procedures.

2

Identify your internal team

Identify a single point of contact for the project and for each department involved in the SOC 2 initiative and ongoing compliance.

3

Recruit external resources

Connect with external resources and service providers to augment your internal team in the areas of tech implementation, process knowledge or project management.

4

Pick software platform

A platform such as ControlMap brings all your compliance work into a single platform and is much more efficient than doing it manually or a spreadsheet.

5

Select a CPA / Auditor

Auditors can help with the right plan, approach, and gap assessments for you to get started. Interview a few auditors to find the right technology and cultural fit for your organization.

6

Finalize internal scope

Identify the application and services which will be examined by the auditor as part of the SOC 2 audit.

7

Report & trust criteria

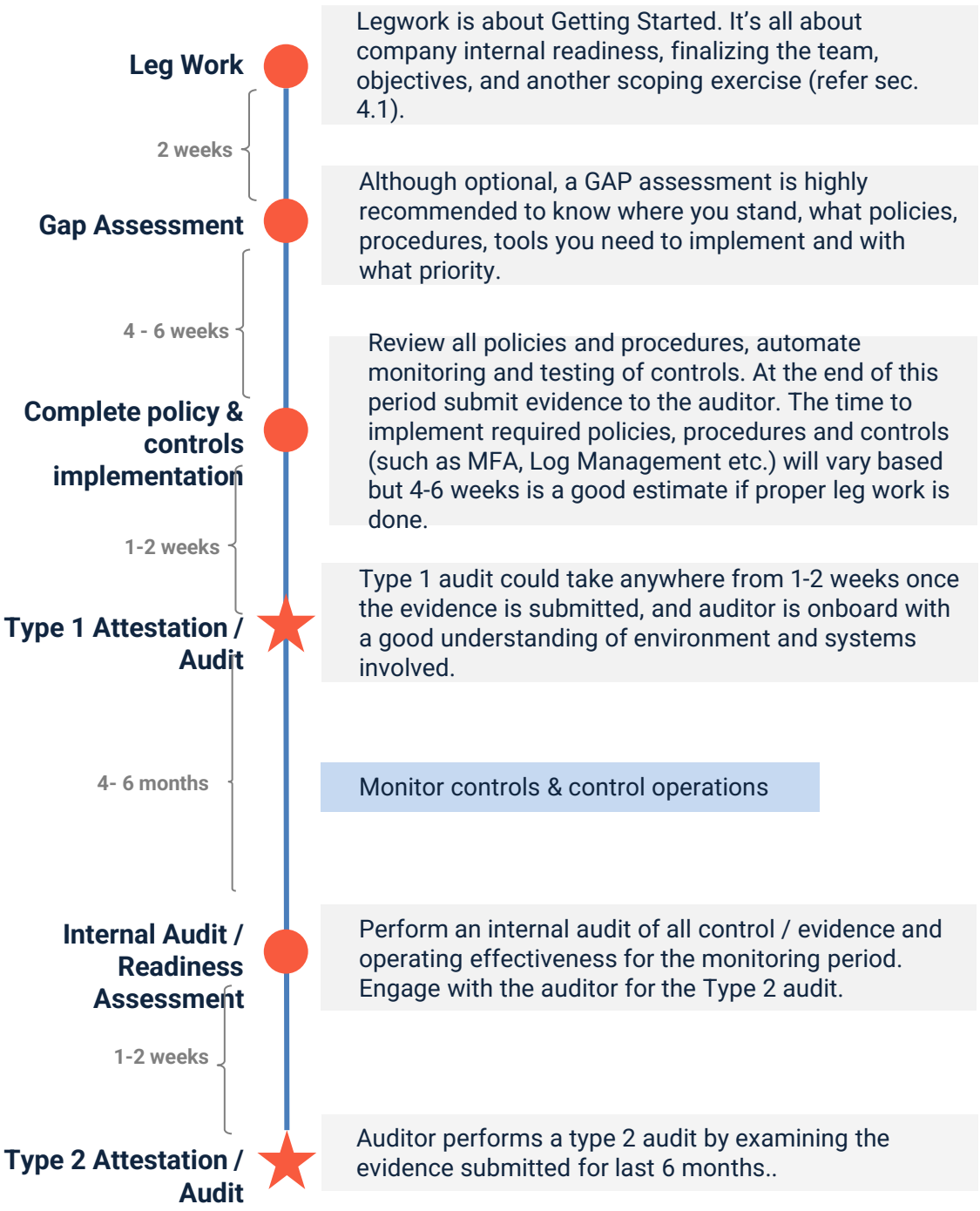
Chose if you want to get a Type 1 or a Type 2 report. Also finalize the trust principles you want to be audited for. Security trust criteria is mandatory.

8

Internal onboarding

Identify a business process owner (BPO) within your company who will oversee the entire SOC 2 initiative and ongoing compliance.

4.2 Plan and timelines



5. The Work Involved

5.1 Documentation

Within each Trust Services Principle, there are four main categories of documented activities that must be performed during the examination/audit period.

1. **Policies**: Company has defined and documented its policies relevant to the principle.

2. **Communications**: Company has communicated its defined policies to responsible parties and authorized users of the system.

3. **Procedures**: Company placed in operation procedures to achieve its objectives in accordance with its defined policies.

4. **Management & Monitoring**: Company monitors the system and takes action to maintain compliance with its defined policies.

Below s a list of documentation that you can expect to submit during the SOC 2 Type 1 and Type 2 audit All documentation should be recently reviewed and updated by appropriate parties.

- Information Security Policy
- Security Awareness Policy
- Code of Conduct Policy
- Change Management Policy
- Encryption Policy
- Access Control Policy
- Remote Work policy
- Risk Assessment Policy
- Vendor Management Policy
- VPN Policy
- Logging & Monitoring Policy
- Incident Management Policy
- Wireless Access Policy
- Asset Policy

5.2 Risk Assessment

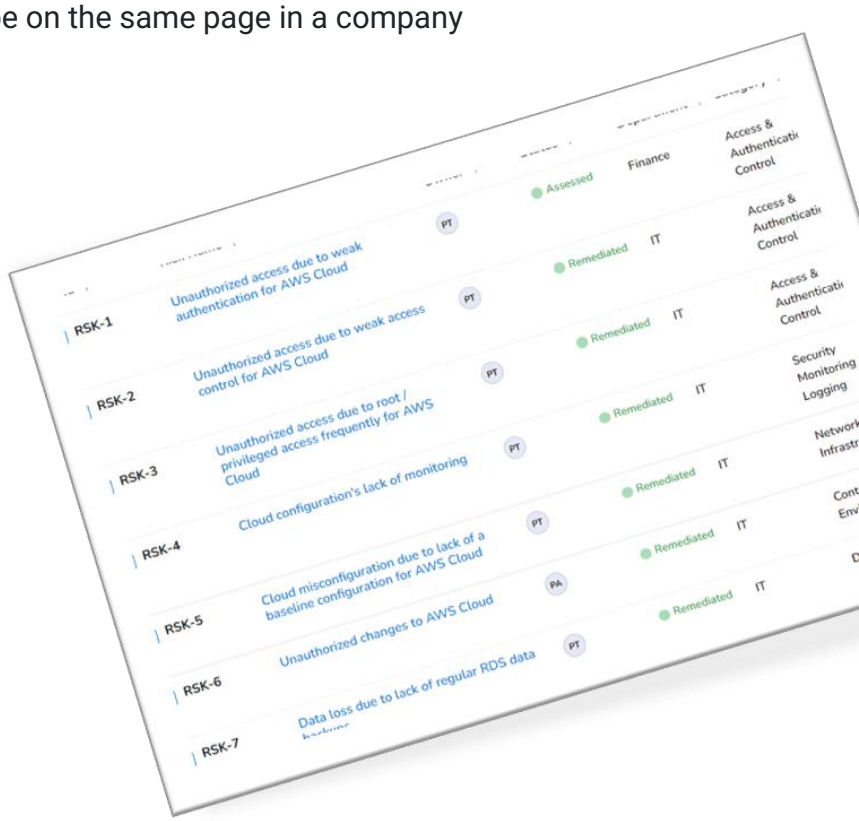
A risk assessment aims to identify all risks your business faces , prioritize those risks based on likelihood and impact and then create controls to mitigate those risks.

The risks faced by each business vary based on the business environment, industry, and size of the business but there are common risks for cloud businesses, software products, and service providers that every business must mitigate.

Periodic risk assessments are one of the most critical activities for being SOC 2 compliant. It can

- Identify the riskiest assets in the organization
- Help in Identifying opportunities for improvement in critical infrastructure
- Assign proper priority to improvement initiatives
- Get executive and management buy-in for change initiatives
- Get everyone involved and be on the same page in a company

Risk assessment activity generally results in a risk register that captures the risks, risk ratings, assets to which the risk applies, and a list of controls that mitigate the risks.



Most recent Risk Assessment report is required to be submitted to the auditor for a Type 1 or a Type 2 audit.

5.3 Implementing controls

Controls implementation as per your policy and risk assessment is the most critical and time-consuming step towards cybersecurity compliance. SOC 2 compliance does not prescribe which controls you implement and how you implement them, if you address all risks and policy requirements. Generally, we have seen that all business minimally implement controls in the following areas

Key control areas

Human Resources

Controls for hiring, onboarding, offboarding, awareness and training, job descriptions are generally the responsibility of the human resources team.

Data Protection & Backup

Controls for protecting data from malicious attacks, unauthorized access , unintentional loss or intentional theft are part of this category.

Logging & Monitoring

Security controls for creating, managing, storing and securely archiving logs for all important functions such as user access. Alerting on logs for unusual activity

Application Development

The objective of this control area is to define & maintain secure application development policies and procedures for the application development team.

Cryptographic Protection

Controls to ensure all data in transit and data at rest are encrypted by using latest and strongest encryption algorithms which can be supported by the company.

Access Control

Establish controls to restrict user access to sensitive information and document policies and procedures for granting and revoking access to information systems.

Incident Management

Controls to monitor, track, respond , and communicate security incidents. This area includes controls for effectively handling any security incidents.

Vendor Management

Establish, document, approve, apply, communicate, evaluate & maintain policies and procedures to assess all vendors which the company decides to do business with.

6. Automating Evidence Collection

Continuously maintaining SOC 2, can be an uphill task. Maintaining compliance across assets, vendors, employees and their devices can be very challenging if you take a completely manual approach of assigning tasks and following up.

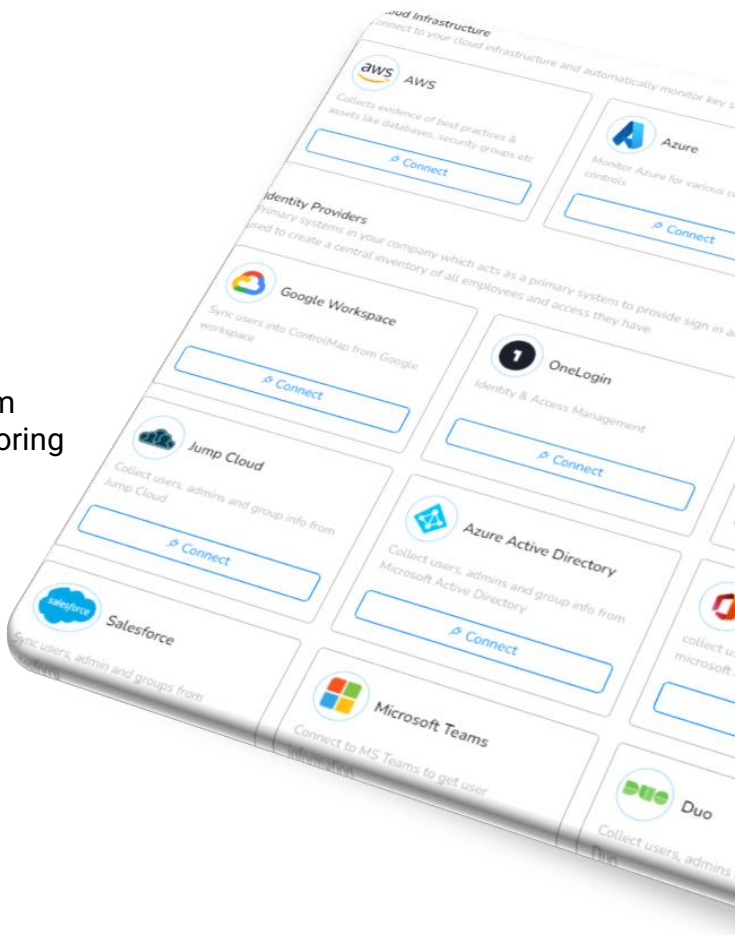
A little bit of automation can save you 100s of hours spent by your IT, HR, and other operations resources collecting and collating evidence.

How do you start automating your evidence ?

The first step to start your cybersecurity compliance automation is to procure or subscribe to a specialized compliance automation software such as ControlMap which connects to your tools and services to collect the right evidence required for a SOC 2 audit from different systems.

Some of the key systems to connect to for automatic evidence collection are

- Identity Management system
- Human Resources System
- Cloud infrastructure systems
- Ticketing systems
- Source code control systems



What does automation do?

An automated evidence collection system continuously keeps collecting and monitoring the end systems for compliance signals such as

- IS MFA enabled
- Are all databases backed up
- Are all accounts current
- Are all databases encrypted
- Are users being offboarded correctly
- Is firewall enabled on endpoints
- etc.

7. Conclusion

Maintaining SOC 2 compliance can be challenging, and the audit procedures can be daunting, especially for the first-timers. However, it could be a fascinating journey with a bit of preparation, readiness, and knowledge.

The benefits of a successful audit are many starting from business growth, more significant deals, and peace of mind. However, the biggest win is the TRUST you gain in your business community by undergoing this exercise.

Hopefully, you find **the overview and description of the SOC 2 audit and compliance provided in this eBook useful**. If you want to add, comment, or learn more, feel free to reach out to us.

8. About ControlMap

Call Us

+1- (502) 430-2668

Visit Us

2018 156th Ave
Bellevue, WA, 98007

Write to us

hello@controlmap.io

controlmap

ControlMap is the only Cybersecurity Compliance Automation platform that brings together all aspects of cybersecurity compliance operations in a single system. ControlMap provides support for more than 25 cybersecurity frameworks and integrates with more than 30 systems to automate compliance

www.controlmap.io