

eBook

# The ultimate SOC 2 guide for **startups**



# TABLE OF CONTENTS



<b>Introduction</b>	<b>03</b>
<hr/>	
Chapter 1 <b>Understanding SOC 2 compliance</b>	<b>04</b>
<hr/>	
Chapter 2 <b>Benefits of SOC 2 for startups</b>	<b>08</b>
<hr/>	
Chapter 3 <b>Preparing for SOC 2 compliance</b>	<b>10</b>
<hr/>	
Chapter 4 <b>Implementing SOC 2 controls</b>	<b>14</b>
<hr/>	
Chapter 5 <b>Conducting a SOC 2 audit</b>	<b>16</b>
<hr/>	
Chapter 6 <b>Post-audit actions</b>	<b>18</b>
<hr/>	
Chapter 7 <b>Different ways to achieve SOC 2 compliance</b>	<b>20</b>
<hr/>	
<b>Wrapping up</b>	<b>23</b>

# Introduction

---

System and Organization Controls 2, or SOC 2 compliance, is necessary for startups looking for meaningful growth. It has largely become a prerequisite to working with mid-market and enterprise-level customers, especially with the growing concerns around data security.



**60% of companies** prefer to work with a startup that has achieved SOC 2. Additionally, **70%** of venture capitalists prefer to invest in a startup that has achieved SOC 2.

In **2024**, the average cost of a data breach reached \$4.88 million—a 10% increase from the previous year and the highest on record. Breaches involving data stored in public cloud environments have exceeded \$5 million. Startups, especially those in sectors like healthcare and finance, face the highest costs due to their handling of sensitive data.

Unlike larger companies, startups and SMEs cannot easily absorb or pass on these costs. For tech startups and SaaS companies, preventing data breaches is vital. With limited resources and constrained pricing power, robust data security is essential.

SOC 2 compliance not only demonstrates your commitment to security and privacy but also builds trust with potential clients. SOC 2 compliance can be complex, but this guide simplifies the process for tech startups by providing a clear overview of the compliance process.

Now, let's get started!

# Understanding SOC 2 compliance

---

**SOC 2** (System and Organization Controls 2) is a framework designed to help organizations manage and protect sensitive information.

Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 is particularly relevant for technology and cloud-based service providers. It ensures that a company's information systems meet rigorous standards for security, availability, processing integrity, confidentiality, and privacy.

SOC 2 compliance is evaluated based on five Trust Service Criteria (TSC):

1. Security
2. Availability
3. Processing integrity
4. Confidentiality
5. Privacy

Each criterion helps ensure that a company's processes and systems are capable of handling data securely and effectively.

While Security is mandatory, the inclusion of other criteria like Availability, Processing Integrity, Confidentiality, and Privacy will depend on the nature of your services and the data you handle.

## Understanding the costs of SOC 2 compliance

---

Achieving SOC 2 compliance involves a range of costs that vary widely based on factors such as the organization's size, complexity, and the scope of the audit. On average, the total cost for a SOC 2 audit can range from **\$60,000 to \$220,000**. This broad estimate encompasses several key components, including pre-audit preparation, audit firm fees, remediation efforts, and ongoing compliance maintenance.

Pre-audit preparation typically costs between **\$15,000 and \$20,000**. This phase involves internal staff training, reviewing and enhancing internal controls, and developing or updating policies and procedures to meet SOC 2 standards. These preparatory steps are crucial for setting up the organization to pass the audit and may involve both internal and external resources.

The third-party audit firm fees, which can range from **\$5,000 to \$60,000**, cover the cost of the actual audit. These fees can vary based on the audit firm's reputation, the complexity of the organization, and whether a Type I or Type II SOC 2 report is required.

Following the audit, organizations may face additional costs ranging from **\$25,000 to \$80,000** for remediation, including addressing audit findings and system upgrades.

Ongoing compliance maintenance, which involves annual renewals and continuous monitoring, adds another **\$10,000 to \$60,000** to the total cost. Understanding these components helps organizations budget effectively and ensure they remain compliant over time.

## SOC 2 vs. other compliance standards

---

**SOC 1, SOC 3, ISO 27001, [GDPR](#)**—these standards often get compared with SOC 2. Here's a brief overview of their differences and similarities:

- **SOC 1:** Focuses on internal controls over financial reporting. Ideal for organizations handling financial data but not necessarily covering other aspects of security and data management.
- **SOC 3:** Similar to SOC 2 but designed for a general audience. SOC 3 reports are less detailed and intended for public distribution.
- **[ISO 27001](#):** An international standard for information security management systems (ISMS). It covers a broader scope of information security than SOC 2 but does not include the same level of operational detail.
- **GDPR (General Data Protection Regulation):** A regulation in EU law on data protection and privacy. GDPR is broader in scope, focusing on data protection and privacy rights for individuals, while SOC 2 is more about establishing and maintaining controls for managing data securely.

While SOC 2, ISO 27001, and GDPR all aim to ensure data security and privacy, **SOC 2 specifically addresses service organizations' controls and processes**. SOC 1 is more focused on financial reporting, and SOC 3 provides a high-level summary suitable for public sharing.

## SOC 2 Type I vs. Type II – Which do startups need?

There are two types of SOC 2 reports, and each serves different purposes

REPORT TYPE	DESCRIPTION	BEST FOR
 SOC 2 Type I	Evaluates whether an organization's systems and controls are suitably designed at a specific point in time.	Early-stage startups as it provides a snapshot of controls in place.
 SOC 2 Type II	Assesses whether the systems and controls operate effectively over a period (usually 6-12 months).	Established companies seeking long-term contracts with large enterprises. Shows higher maturity and operational effectiveness.

While Type I may be sufficient for early engagements, most startups **should aim for Type II as it's becoming a common requirement for doing business with larger organizations and is often seen as a sign of robust operational security**. Achieving Type II can significantly boost credibility, increase customer confidence, and create more revenue opportunities.

## SOC 2 for different types of startups

SOC 2 compliance requirements can vary depending on the nature of your startup. This chapter addresses the unique considerations for different types of startups.

## SaaS startups

SaaS companies often handle large volumes of data and provide critical software services.

Key considerations include:

- **Data Security:** Implement robust security measures to protect customer data from breaches and unauthorized access.
- **Service Availability:** Ensure that your service level agreements (SLAs) and disaster recovery plans are well-defined to meet availability requirements.
- **Access Controls:** Implement strict access controls to manage who can access sensitive customer data and system configurations.

## Fintech startups

Fintech startups operate in a highly regulated environment with stringent compliance requirements.

Key considerations include:

- **Data Protection:** Implement measures to protect sensitive financial data, including encryption and secure transaction processing.
- **Regulatory Compliance:** Align your SOC 2 controls with financial regulations such as PCI DSS (Payment Card Industry Data Security Standard) and AML (Anti-Money Laundering) requirements.
- **Audit Trails:** Maintain detailed audit trails for financial transactions and system access to meet regulatory scrutiny.

## Healthcare startups

Healthcare startups must comply with both SOC 2 and HIPAA (Health Insurance Portability and Accountability Act) regulations.

Key considerations include:

- **Data Privacy:** Ensure that your SOC 2 controls align with HIPAA's privacy and security rules for handling protected health information.
- **Risk Management:** Implement risk management practices to address the specific privacy and security needs of healthcare data.
- **Compliance Integration:** Coordinate your SOC 2 efforts with HIPAA compliance requirements to create a unified approach to data security and privacy.

# Benefits of SOC 2 for startups



### Benefit 1

Building trust and credibility with clients and investors



### Benefit 2

Market differentiation



### Benefit 3

Establishes strong policies and procedures for data protection



### Benefit 4

Prepares for growth

## 1. Building trust and credibility with clients and investors

Achieving SOC 2 compliance early gives startups a competitive edge by showcasing a commitment to high security and privacy standards. It helps differentiate your startup, attract and retain clients, and secure funding.

SOC 2 certification reassures clients and investors of your dedication to data security and operational excellence, enhancing trust and making your startup more appealing for investment.

## 2. Market differentiation

Being one of the few startups to achieve SOC 2 early can set you apart from competitors who may not yet be compliant, giving you an edge in attracting clients who require stringent security measures.

## 3. Establishes strong policies and procedures for data protection

SOC 2 compliance aligns with various industry standards for data protection, helping your startup navigate complex regulatory landscapes.

SOC 2 compliance requires implementing robust policies and procedures for managing data security and privacy. Establishing these policies helps you meet regulatory requirements and fosters a culture of accountability and vigilance within your organization.



*Scrut gave us added confidence in managing documentation for ensuring continuous compliance across 3 standards, and now we're in the process of getting our HIPAA certification as well!*

**Satish G**

Chief Evangelist, [Cogniquest](#)



## 4. Prepares for growth

Early SOC 2 compliance positions your startup for future growth by establishing a strong security framework. As your startup scales, having these controls and policies in place ensures that you are prepared to handle increased data volumes and more complex regulatory requirements, facilitating smoother expansion.

### Startups that benefit most from SOC 2 compliance are typically

Entering the growth stage or beyond



Planning significant expansion



Operating in data-sensitive industries like healthcare, finance, pharmaceuticals, or technology



Offering e-commerce services or dealing with big data, where clients may request SOC 2 reports



# Preparing for SOC 2 compliance

Achieving SOC 2 compliance requires careful preparation and a strategic approach. This chapter will guide you through the essential steps to prepare your startup for SOC 2 certification, from initial assessment to building a strong security culture. There are 9 crucial steps to follow to prepare for SOC 2 compliance.



Conduct an initial assessment



Conduct a gap analysis



Identify key stakeholders



Develop a compliance plan



Set goals and timelines



Effectively allocate resources



Build a security culture



Impart training and awareness



Define roles and responsibilities

## How to prepare for SOC 2 Compliance:

### 1. Conduct an initial assessment

Before diving into SOC 2 compliance, it's crucial to understand your current state and identify what needs to be addressed. The initial assessment involves a comprehensive review of your existing policies, procedures, and controls related to security, availability, processing integrity, confidentiality, and privacy. This step helps to establish a baseline for your compliance efforts and highlights areas that need improvement.

## 2. Conduct a gap analysis

A gap analysis is a critical component of the initial assessment. It involves comparing your current practices against the SOC 2 Trust Service Criteria (TSC) to identify discrepancies. This process helps pinpoint specific areas where your controls or procedures fall short of SOC 2 requirements. The results of the gap analysis will guide your subsequent efforts in developing and implementing necessary changes to meet SOC 2 standards.

## 3. Identify key stakeholders

Successful SOC 2 compliance requires the involvement of key stakeholders across your organization. Identify individuals who play a crucial role in managing and overseeing compliance efforts. This typically includes:

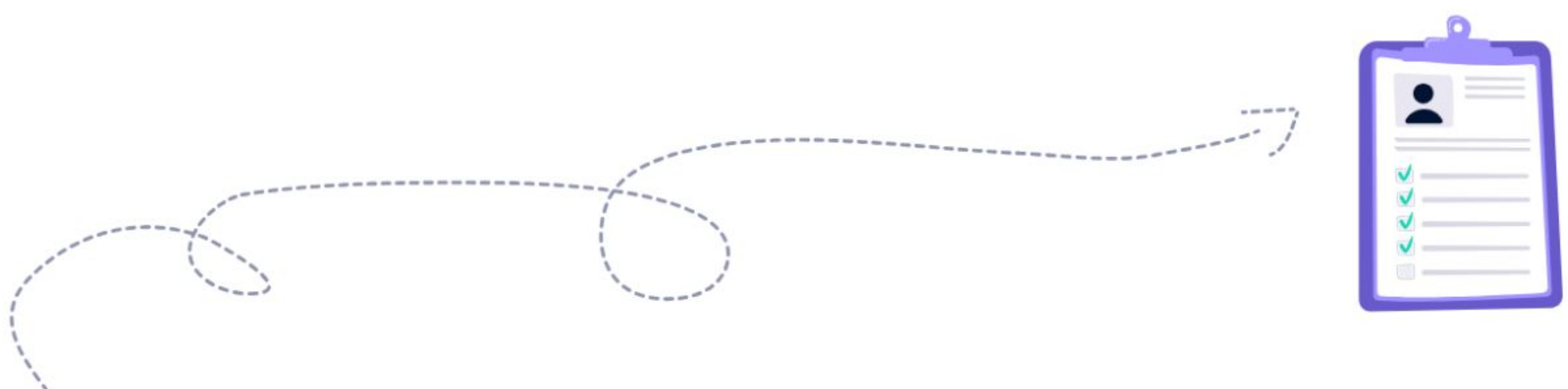
- **Executive Leadership:** For strategic direction and support.
- **IT and Security Teams:** For implementing and managing controls.
- **Compliance Officers:** For overseeing adherence to SOC 2 requirements.
- **Legal and HR Departments:** For policy development and training.

Engaging these stakeholders early ensures alignment and facilitates a smoother compliance process.

## 4. Develop a compliance plan

A well-structured compliance plan outlines the steps and strategies required to achieve SOC 2 certification. It should include:

- **Objectives:** Define clear compliance goals aligned with SOC 2 criteria.
- **Action Items:** List specific tasks and responsibilities for implementing controls.
- **Timeline:** Establish deadlines for each phase of the compliance process.
- **Milestones:** Identify key checkpoints to track progress and make adjustments as needed.



## 5. Set goals and timelines

Setting realistic goals and timelines is essential for effective SOC 2 preparation.

- Break down the compliance process into manageable phases, each with specific objectives and deadlines.
- Ensure your goals are SMART (Specific, Measurable, Achievable, Relevant, Time-bound) to maintain focus and track progress.
- Regularly review and adjust timelines as necessary to address any challenges or delays.

## 6. Effectively allocate resources

Effective resource allocation involves assigning the right people, budget, and tools to support SOC 2 compliance efforts. This includes:

- **Human Resources:** Allocate staff with the necessary skills and experience to manage compliance tasks.
- **Financial Resources:** Budget for costs related to audits, technology upgrades, and potential consulting fees.
- **Technological Resources:** Invest in tools and systems that facilitate compliance, such as security monitoring solutions and documentation management software.

## 7. Build a security culture

Creating a strong security culture is vital for maintaining SOC 2 compliance and ensuring ongoing data protection. This involves:

- **Training and Awareness:** Regularly educate employees about security best practices, policies, and their role in maintaining compliance.
- **Regular communication:** Foster open dialogue about security concerns and encourage reporting of potential issues. Have periodic reminders about the importance of maintaining best infosec practices in the workplace.



## 8. Impart training and awareness

Implement a comprehensive training program to ensure all employees understand SOC 2 requirements and their responsibilities. Training should cover:

- **SOC 2 Criteria:** Overview of the Trust Service Criteria and their implications.
- **Security Policies:** Detailed explanation of your company's security policies and procedures.
- **Best Practices:** Practical tips for safeguarding sensitive information and responding to security incidents.

## 9. Define roles and responsibilities





Clearly define and communicate roles and responsibilities related to SOC 2 compliance. This helps ensure accountability and effective management of compliance activities. Key roles typically include:

- **Compliance Manager:** Oversees the overall compliance effort and liaises with auditors.
- **IT Security Lead:** Implements and monitors technical controls and security measures.
- **Policy Owner:** Develops and maintains relevant policies and procedures.
- **Employee:** Adheres to security practices and reports any concerns.

Establishing clear responsibilities and expectations helps streamline the compliance process and fosters a collaborative approach to achieving SOC 2 certification.



# Implementing SOC 2 controls

Criteria	Focus	Controls
 Security	Protecting systems against unauthorized access.	Network security measures, firewalls, intrusion detection systems, access controls, vulnerability monitoring.
 Availability	Ensuring systems are available for operation and use.	Disaster recovery plans, backup procedures, redundant systems.
 Processing Integrity	Ensuring system processing is complete, valid, accurate, timely, and authorized.	Data processing validation, error prevention, adherence to processing requirements.
 Confidentiality	Protecting information designated as confidential.	Data classification policies, encryption, secure data storage.
 Privacy	Handling personal information in compliance with privacy policies and regulations.	Data collection, storage, and processing in line with privacy laws and policies.

## Documenting policies and procedures

Effective documentation is essential for demonstrating compliance and guiding operational practices. This involves:

- 1. Creating and maintaining documentation:** Develop comprehensive policies and procedures that address each of the Trust Service Criteria. Ensure that documentation is detailed, up-to-date, and reflects current practices. This includes writing clear procedures for managing security, availability, processing integrity, confidentiality, and privacy.
- 2. Essential policies:** Key policies to document include:
  - **Information security policy:** Outlines security measures, risk management practices, and employee responsibilities.
  - **Incident response policy:** Details procedures for responding to and managing security incidents.
  - **Data retention policy:** Specifies how long different types of data will be retained and the procedures for securely disposing of data.
  - **Access control policy:** Defines how access to systems and data is managed and monitored.

## Implementing technical controls

Technical controls are the technological measures put in place to enforce SOC 2 requirements.

**Key areas include:**

- 1. Access controls:** Implement mechanisms to manage user access to systems and data. This includes setting up role-based access controls (RBAC) to ensure that users only have access to information necessary for their roles. Regularly review and update access permissions to maintain security.
- 2. Data encryption:** Use encryption to protect data both at rest and in transit. Encrypt sensitive data to ensure that it is unreadable to unauthorized users, which helps maintain confidentiality and integrity. Ensure that encryption protocols are updated to reflect current best practices.
- 3. Incident response:** Develop and implement technical measures for detecting, managing, and responding to security incidents. This includes setting up systems for monitoring, logging, and alerting on potential security breaches. Ensure that your incident response plan includes technical steps for containment and mitigation.

# Conducting a SOC 2 audit

---

Achieving SOC 2 compliance requires careful preparation and a strategic approach. This chapter will guide you through the essential steps to prepare your startup for SOC 2 certification, from initial assessment to building a strong security culture.

## Choosing an auditor

---

Selecting the right auditor is critical in the SOC 2 compliance journey. Here's how to make an informed choice:

### 1. Select a qualified CPA firm:

- i. Choose a CPA firm that specializes in SOC 2 audits and has a strong track record in the field.
- ii. Verify that the firm is licensed and has experience with companies of your size and industry.
- iii. Look for a firm with a deep understanding of SOC 2 requirements and a reputation for thoroughness and professionalism.

### 2. What to look for in an auditor:

- **Expertise:** Ensure the auditor has specific experience in SOC 2 audits and is familiar with the Trust Service Criteria relevant to your business.
- **Reputation:** Look for reviews, references, and past client feedback to gauge the auditor's reliability and effectiveness.
- **Approach:** Assess the auditor's methodology and approach to ensure it aligns with your needs and expectations. An auditor who communicates clearly and provides valuable insights will be an asset throughout the process.

## Audit preparation

---

Preparation is key to a smooth and successful SOC 2 audit. This involves:

1. **Preparing documentation:** Gather and organize all necessary documentation related to your SOC 2 controls. This includes policies, procedures, and evidence of control implementation. Ensure that all documents are up-to-date and reflect current practices.

**2. Internal reviews and pre-audit checklists:** Conduct internal reviews to identify any gaps or issues before the formal audit begins. Use pre-audit checklists to ensure that all required documentation and controls are in place. This proactive approach helps address potential issues early and ensures a more efficient audit process.

## The audit process

Understanding what to expect during the SOC 2 audit helps in managing the process effectively:

- **What to expect during the audit:** The audit will involve an examination of your documentation, interviews with key personnel, and testing of controls. The auditor will review your policies and procedures, assess the effectiveness of your controls, and verify compliance with the SOC 2 Trust Service Criteria. Be prepared to provide access to systems, data, and personnel as requested.

## Common challenges and solutions

Challenge	Solution
1. Incomplete or outdated documentation	Stresses the importance of being open and accountable, making it necessary for companies to check their algorithms for any biases or discrimination.
2. Inconsistent implementation of controls	Conduct internal audits and reviews to verify that controls are consistently applied and effective.
3. Difficulty in demonstrating compliance	Maintain detailed records of control operations and provide clear evidence of compliance. Prepare your team for interviews and provide them with the necessary information and training.

By thoroughly preparing and understanding the audit process, you can navigate the SOC 2 audit with confidence and increase your chances of a successful outcome.

# Post-audit actions

---

After the SOC 2 audit, several critical steps ensure that you address any findings, maintain compliance, and leverage your SOC 2 certification for business growth.

## Receiving and reviewing the audit report

---

Selecting the right auditor is critical in the SOC 2 compliance journey. Here's how to make an informed choice:

- **Receiving the report:** Once the audit is completed, the auditor will provide you with a detailed audit report. This document includes an evaluation of your controls, any identified deficiencies, and an overall assessment of your compliance with SOC 2 criteria.
- **Reviewing the Report:** Carefully review the audit report to understand the findings and recommendations. Pay close attention to any areas of non-compliance or improvement suggested by the auditor. This review is crucial for addressing issues and strengthening your controls.

## Understanding the audit findings

---

- **Interpreting findings:** Audit findings will highlight areas where your controls may not fully meet SOC 2 requirements. Understanding these findings involves interpreting the auditor's observations and recommendations.
- **Discussing with the auditor:** Engage with the auditor to clarify any ambiguities and get a deeper understanding of the findings. This discussion can provide insights into how to effectively address the issues raised.

## Addressing findings and recommendations

---

- **Action plan:** Develop an action plan to address any identified deficiencies or areas for improvement. Prioritize actions based on their impact and the auditor's recommendations.

- **Implementation:** Implement the necessary changes to your policies, procedures, and controls. Ensure that these changes are well-documented and communicated to relevant stakeholders.
- **Follow-up:** Schedule follow-up reviews to verify that the issues have been resolved and that the new measures are effective.

## Maintaining compliance

- **Continuous monitoring:** Regularly monitor your controls to ensure ongoing compliance with SOC 2 criteria. Implement systems for continuous tracking and assessment of your controls.
- **Regular reviews:** Conduct periodic internal audits to assess the effectiveness of your controls and ensure they remain aligned with SOC 2 requirements.

## Preparing for future audits

- **Documentation:** Keep your documentation and evidence up-to-date to facilitate future audits. Maintain a comprehensive record of your controls, procedures, and any changes made.
- **Continuous improvement:** Regularly review and refine your controls based on audit feedback and changes in SOC 2 standards or your business operations.

## Leveraging SOC 2 for business growth

- **Using SOC 2 as a marketing tool:** Highlight your SOC 2 certification in marketing materials, on your website, and in client communications to showcase your commitment to security and compliance. This can differentiate your business from competitors and attract new clients.
- **Enhancing trust with clients and partners:** Use your SOC 2 certification to build trust with existing and potential clients and partners. Demonstrating compliance with industry standards can strengthen relationships and provide reassurance regarding data security and privacy.

# Different ways to achieve SOC 2 compliance

Achieving SOC 2 compliance can be approached in several ways, each with its own implications.

Managing the process in-house demands extensive time and expertise, which can be overwhelming for startups with limited resources.

Engaging a consultant provides professional guidance but involves high fees and varying costs based on the consultant's expertise and the organization's size.

Alternatively, using a GRC (Governance, Risk, and Compliance) platform like Scrut offers a cost-effective and efficient solution. These platform automates many compliance tasks and streamlines the process, making it an affordable option for startups while minimizing the burden on internal resources.

The logo for Xeno, featuring the word "xeno" in white lowercase letters on a blue square background.

**Xeno**, an AI-driven CRM platform, helps major retail and D2C brands like Levi's and Taco Bell, boosts customer loyalty and repeat sales through personalized multichannel campaigns. Handling over 100 million customer profiles and 1 billion data points, Xeno requires robust cloud risk monitoring and stringent infosec measures.

To manage this, Xeno implemented Scrut to automate cloud risk monitoring, streamline information security processes, and maintain compliance with ISO 27001 and SOC 2. Scrut's platform provides a centralized hub for infosec artifacts, automates vendor risk assessments, and ensures continuous employee security training, thereby optimizing security and compliance efficiently.



**Orca**, a leading freight audit and analytics provider in Canada, previously achieved SOC 2 certification through Vanta. To enhance security and meet multiple compliance needs, Orca sought a GRC solution that matched their SaaS platform's focus on efficiency and user-friendliness. After evaluating options, they decided to transition to Scrut smartGRC™ for their renewal.

With Scrut, Orca achieved the following:

- SOC 2 compliance in 8 weeks
- Experienced 85% reduction in security questionnaire response time
- 50% time savings

## How Scrut helps startups become SOC 2 compliant?

Scrut is designed to address the unique challenges that startups face when pursuing SOC 2 compliance. With its comprehensive platform and tailored solutions, Scrut offers several key benefits to startups



1

### Streamlined compliance processes

Scrut simplifies the SOC 2 compliance journey with its automated compliance management system. Startups can benefit from streamlined processes that cover everything from documentation to risk management, reducing the complexity and effort required to achieve compliance.

### Automated evidence collection

One of the most time-consuming aspects of SOC 2 compliance is gathering and managing evidence. Scrut automates evidence collection from various integrations, which helps startups maintain accurate records without the need for manual data collection. This automation not only saves time but also minimizes the risk of errors.

2



3

### Centralized documentation management

Scrut provides a centralized platform for managing all SOC 2-related documentation. Startups can easily store, organize, and access policies, procedures, and audit trails from one place, ensuring that all required documentation is readily available and up-to-date.

## Real-time monitoring and alerts

With Scrut's real-time monitoring capabilities, startups can continuously track their compliance status. The platform offers alerts and notifications for any compliance gaps or issues, allowing startups to address potential problems before they escalate.

4



**iMocha**, a skills intelligence and assessment platform, utilizes Scrut Automation to enhance its compliance and security across its complex multi-region Azure cloud infrastructure.

By automating scans and monitoring over 200 controls, Scrut helps iMocha identify and address misconfigurations, ensuring continuous SOC 2 compliance.

Scrut provides a unified platform for managing security risks, controls, and evidence, streamlining iMocha's SOC 2 Type II audit and maintaining a robust cloud security posture.



5

## Pre-built templates and frameworks

Scrut offers pre-built templates and frameworks tailored to SOC 2 requirements. These resources help startups quickly implement necessary controls and policies, reducing the time needed to create documentation from scratch.

## Expert guidance and support

Scrut's platform includes access to expert resources and support. Startups can benefit from guidance on compliance best practices, ensuring that they meet SOC 2 requirements effectively. This support is crucial for startups with limited in-house compliance expertise.

6



7

## Integration with existing systems

Scrut integrates seamlessly with a wide range of tools and platforms that startups may already be using. This integration simplifies the process of aligning existing systems with SOC 2 requirements, reducing the need for extensive modifications.

## Wrapping up: The path to secure growth

---

SOC 2 compliance is a powerful growth driver for startups, enhancing trust and credibility with clients and partners. It signals a strong commitment to security and privacy, which can attract new customers and facilitate valuable partnerships.

By following the steps outlined in this ebook, startups can navigate the SOC 2 certification process more efficiently and effectively, ultimately achieving compliance and enhancing their security posture.

Ready to take the next step toward achieving SOC 2 compliance and driving secure growth for your startup?

[Take the next step towards secure growth with Scrut](#), and let our tools simplify your [SOC 2](#) journey and help your startup thrive.

Usher in a new era of  
**frictionless** GRC programs

Request a demo