letsbloom

SOC 2 FAQs Playbook

Everything you need to know to leverage SOC 2 for your business!

JANUARY 2025

1. Who does SOC 2 compliance apply to?

If you're a service organization providing Information System Services to customers, you'll likely need to be SOC 2 compliant. Especially, IT service providers, SaaS businesses, and cloud computing companies who provide Infra / application services, store or transmit and process customer data need SOC 2 to demonstrate robust Internal controls and data security practices to their clients.

2. How does a company get SOC 2 certified?

SOC 2 is not a certification but rather a third-party attestation of the controls implemented within your organization. When addressing this topic, the process generally begins with defining your scope, which includes identifying the system and relevant SOC 2 categories (trust services). Next, you conduct a readiness assessment to prepare for the evaluation. Following this, a licensed CPA firm or an agency accredited by AICPA conducts either a Type 1 or Type 2 assessment. The result is a comprehensive report that outlines the effectiveness of your controls, which is often informally referred to as achieving SOC 2 compliance.

3. What is the difference between SOC 2 Type 1 & SOC 2 Type 2?

The primary distinction lies in the focus and timeframe of the reports. A SOC 2 Type 1 report evaluates the design of your systems and controls at a single point in time. In contrast, a SOC 2 Type 2 report assesses both the design and the operational effectiveness of those systems and controls over an extended period, usually ranging from 4 to 12 months.

4. How often does a SOC 2 compliance audit need to be performed?

It is industry standard to conduct the SOC 2 Type II compliance audit annually, or when significant changes are made, however, there are times you may choose to perform them twice a year. Additionally, if recently completing a SOC 2 Type I, performing a SOC 2 Type II a few months later is also very common.

5. Is it mandatory to get both SOC 2 Type 1 and SOC 2 Type 2 compliant simultaneously?

No. If you are starting your SOC 2 compliance journey from scratch, you should aim to get SOC 2 Type II compliant as that will demonstrate the comprehensive design and operational effectiveness of the controls implemented in an organization. However, Type II attestation requires demonstration of control operation effectiveness for a minimum period (3 to 4 months), if your organization needs to quickly demonstrate control design then Type I assessment would provide a point in time attestation. However, this needs to be followed up by a Type II assessment for an organization to effectively demonstrate SOC 2 compliance.

6. What are the 5 SOC 2 service criteria?

SOC 2 is based on five principles, called the Trust Services Criteria (formerly called the Trust Service Principles).

1. **Security**: Protecting systems and data from unauthorized access.
2. **Availability**: Making sure services and data are available as agreed.
3. **Processing Integrity**: Ensuring the processing of data is complete, valid, accurate, timely, and authorized.
4. **Confidentiality**: Keeping sensitive information safe and sound.
5. **Privacy**: Protecting personal information as agreed or as required by law.

7. What is the purpose of SOC 1, SOC 2, and SOC 3?

SOC 1, SOC 2, and SOC 3 each serve distinct purposes related to different aspects of service organization controls.

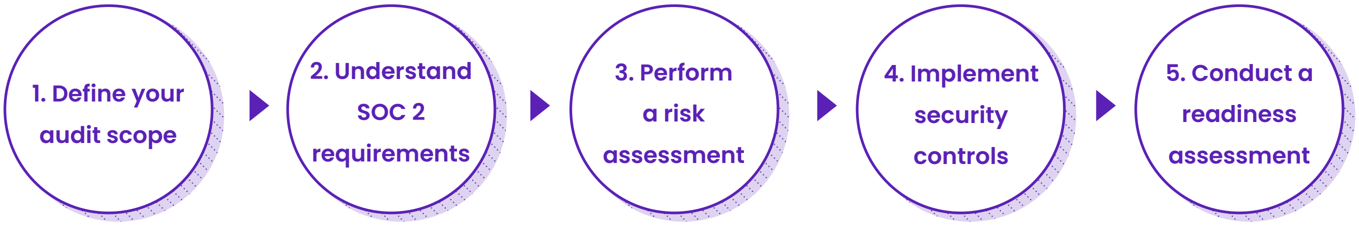
SOC 1 focuses on providing auditors and customers attestation on financial reporting control effectiveness. This helps customers get assurance that company is sensitive financial data of its customers with requisite protections and accuracy. It includes an auditor's opinion to help assess the effectiveness of these controls.

SOC 2 is aimed at management, customers, partners, and other stakeholders, offering insights into the service organization’s controls related to security, availability, processing integrity, confidentiality, and privacy. This attestation helps customers get assurance on the effectiveness of companies internal control systems to protect their data from cyber threats.

SOC 3, on the other hand, is designed for the general public. It provides a summary of the same types of controls covered in SOC 2 (security, availability, processing integrity, confidentiality, and privacy) but in a more accessible format for broader evaluation purposes.

8. How do I prepare for SOC 2 audit?

Here are the key steps:



1. Define your audit scope

2. Understand SOC 2 requirements

3. Perform a risk assessment

4. Implement security controls

5. Conduct a readiness assessment

Collaborate with stakeholders to identify the Trust Services Criteria relevant to your organization and decide whether to pursue a SOC 2 Type I or Type II report.

Know all about the five Trust Services Criteria and their implications for your organization. Find the complete SOC 2 compliance checklist for seamless audit.

Evaluate potential threats to sensitive data and determine appropriate mitigation strategies.

Establish measures to address identified risks and ensure they are prioritized effectively.

Review your current systems, processes, and controls to confirm they align with SOC 2 requirements before initiating the formal audit process.

9. How do I determine the scope of my SOC 2 audit?

The scope depends on:

- **Services offered.**
- **Applicable Trust Service Criteria.**
- **Customer requirements.**
- **Most organisations focus initially on Security (mandatory) and then expand to others as needed.**

10. What happens if the company fails the SOC 2 audit?

You can’t technically "fail" a SOC 2 audit, as there’s no pass or fail system. But if you still get an objective report for not meeting the relevant Trust Service Criteria, it may result in a failed SOC 2 audit, requiring gap remediation. This is called “Qualified opinion”, signalling areas that need improvement.

11. What are the biggest challenges in achieving SOC 2?

Achieving a SOC 2 audit can be challenging due to several factors, including the need for extensive documentation, incomplete or ineffective risk assessments, weak change management practices, and difficulties in defining the audit scope. Additional challenges include managing complex system environments, maintaining consistent control effectiveness, and meeting strict deadlines. For teams unfamiliar with the process, thoroughly documenting policies and procedures can create a significant workload, adding to the overall complexity.

12. What is SOC 2 automation?

SOC 2 automation simplifies achieving and maintaining compliance by using technology to streamline routine tasks. Instead of manually tracking compliance, automation tools continuously monitor systems, alerting you to issues like unauthorized access or policy violations. They also automate evidence collection for audits. In short, SOC 2 automation reduces the burden of compliance, allowing your team to focus on more critical tasks.

13. What tasks can be automated with Letsbloom's compliance automation platform?

Letsbloom's compliance automation platform can help you navigate SOC 2 compliance complexities by automating a range of tasks:

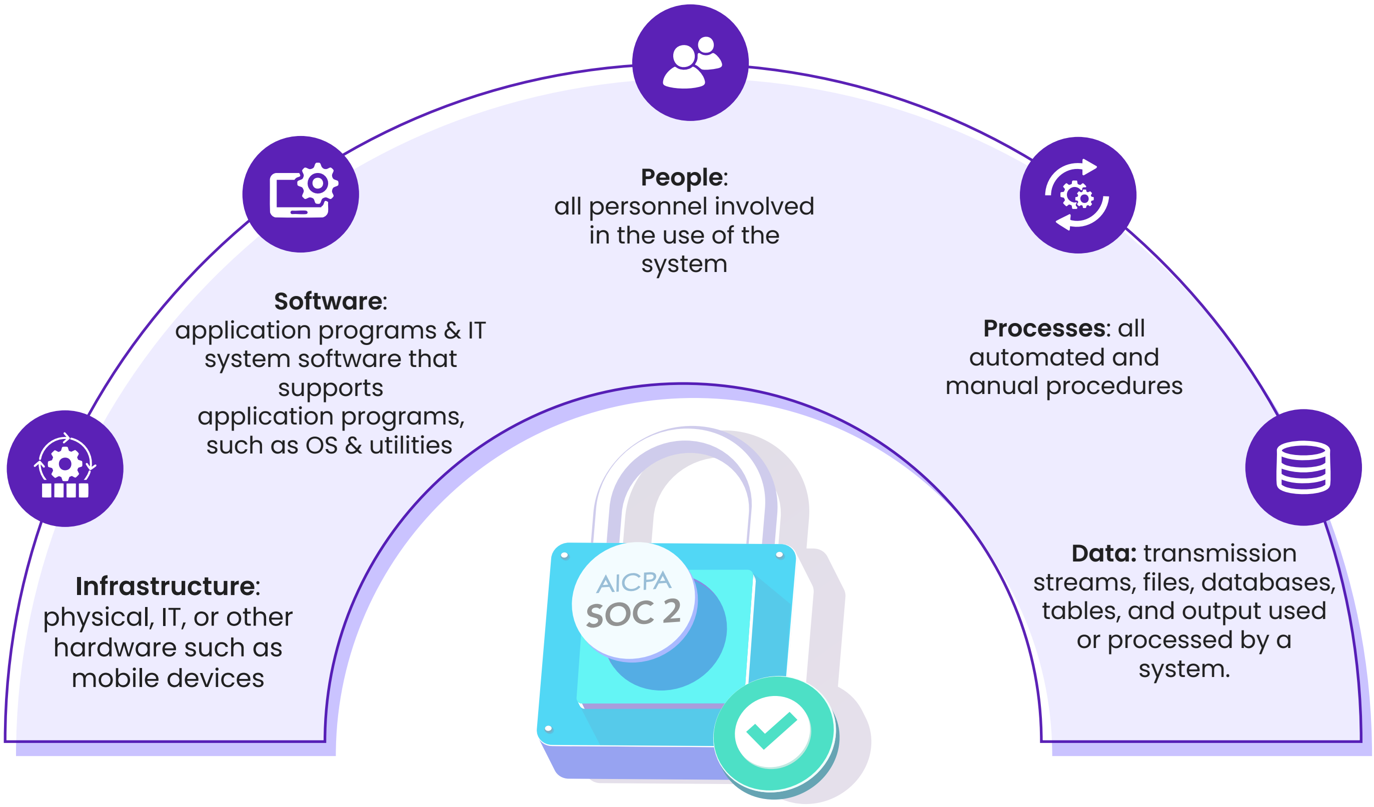
- Automated mapping of all 5 Trust Service Criteria to relevant controls
- Automated evidence collection and mapping to controls
- SOC-2 ready pre-built policy templates and instant gap assessment reports
- Continuous monitoring of controls for nonconformities or any failures
- AI-enabled risk identification, prioritization, and remediation guidance
- Vendor risk management and policy management

Letsbloom's platform ensures proof for every implemented SOC 2 control, reducing the back-and-forth with the CPA. When done manually, these tasks could take hundreds of hours!

14. How long does a SOC 2 attestation take?

1. **Pre-audit phase** - This phase can take 2 weeks to 3 months. The length of the preparation phase depends on how many controls are already in place and how many need to be added.
2. **Assessment window** - This phase can be anywhere from 3 months to one year. The auditor will validate the security controls and test their effectiveness during the designated Audit period. The organization needs to implement designed controls throughout this period and show evidence as required by auditors.
3. **Audit phase** - This phase can take 2 - 4 weeks. The auditor will review the documentation and implemented controls to determine if the organization meets the requirements for SOC 2 compliance.
4. **Report creation and delivery** - This phase can take 2-4 weeks. The auditor will compile their findings into a SOC 2 report.

15. What system components are evaluated during a SOC 2 audit?



People: all personnel involved in the use of the system

Software: application programs & IT system software that supports application programs, such as OS & utilities

Processes: all automated and manual procedures

Infrastructure: physical, IT, or other hardware such as mobile devices

Data: transmission streams, files, databases, tables, and output used or processed by a system.

16. Can we implement two compliance frameworks simultaneously?

Letsbloom not only delivers a seamless compliance experience but also offers straightforward, centralized, and scalable solution that can help you get compliant with multiple frameworks effortlessly.

Many frameworks share common controls and requirements, and Letsbloom is designed to leverage your existing compliance efforts to reduce redundancy. For example, if you're already SOC 2 compliant and aim to incorporate ISO 27001, Letsbloom minimizes the additional work needed, making the process highly efficient.

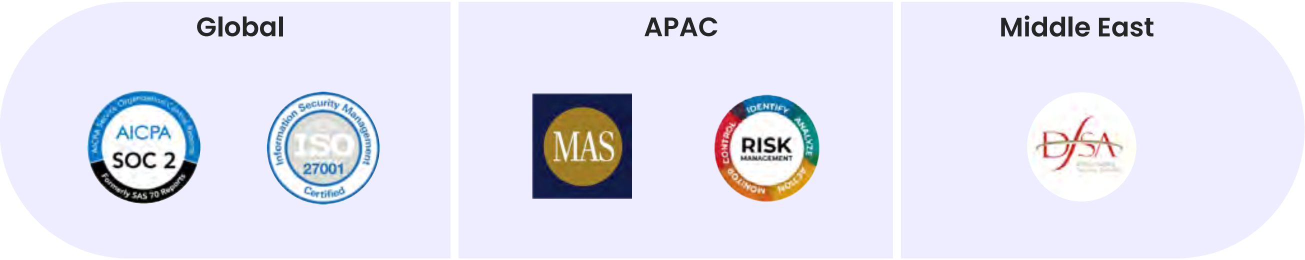
17. Is Letsbloom a SOC 2 or an ISO auditor? What type of audit partners do you work with?

Letsbloom isn't an auditor. We are a compliance automation platform. We work closely with independent, certified auditors to support our customers with their audit requirements. As a Letsbloom customer, you can collaborate with our affiliated auditor network or select one outside of it. Either way, Letsbloom's compliance experts will work with you to keep your compliance program running smoothly.

18. How does Letsbloom meet the compliance requirements of different countries?

Letsbloom maintains a comprehensive library of common control objectives, encompassing the requirements of major global regulators and industry benchmarks. This allows us to:

- **Adapt to diverse regulatory landscapes:** Quickly configure reports for new regulatory frameworks, typically within 6-8 weeks.
- **Support a wide range of compliance initiatives:** Currently, the platform supports key frameworks such as:



19. Who are Letsbloom's customers?

Letsbloom serves a diverse global client base, including organizations in the US, Singapore, and the Middle East. We also have strong partnerships with leading global System Integrators (SIs) and Big 4 consulting firms across key regions such as the US, UK, Southeast Asia (SEA), Australia and New Zealand (ANZ), and Japan.

20. What are the costs involved in getting compliant?

Cost Comparison: Traditional vs. Letsbloom

Traditional Approach:

- Significant upfront costs:
- Employee time for implementation
- Consultant fees for assessments
- Audit expenses
- Separate software purchases (vulnerability scanners, MDM, etc.)
- Ongoing costs for security training

VS

Letsbloom

- **All-in-one solution:** Includes automated platform, expert support, built-in MDM, training, and more.
- **Reduced costs:** Eliminates many of the individual expenses associated with traditional compliance.
- **Transparent pricing:** Primarily based on the platform cost, with additional fees for VAPT (Vulnerability Assessment and Penetration Testing).

21. What is the scope of activities that Letsbloom will support us with?

Letsbloom provides comprehensive support across three key phases:

- **Implementation:** Our platform guides you in personalizing your framework implementation, integrating with your systems, and mapping controls within the Letsbloom platform.
- **Monitoring:** You actively run, operate, and monitor all implemented controls within the Letsbloom platform.
- **Audit:** Our affiliated auditors assists throughout the audit process, collaborating with your chosen auditor (from our network or external) to ensure a smooth audit experience.

Key Benefits

Proven Success

100% of our customers have achieved successful audits.

Streamlined Audits

80% of our customers experience significantly reduced auditor interactions due to Letsbloom's automation capabilities.

22. Does Letsbloom help identify and address compliance gaps?

Yes, Letsbloom includes an in-app gap assessment feature. This tool helps you:

- **Pinpoint areas of non-compliance:** Identify specific processes or infrastructure components that do not meet compliance requirements.
- **Prioritize remediation efforts:** Understand the severity of each gap and prioritize remediation actions accordingly.
- **Drive continuous improvement:** Use the assessment results to continuously improve your compliance posture and reduce risk.

23. How much time does it take to maintain Letsbloom's compliance automation after an audit?

Letsbloom's compliance automation solution is designed for efficiency. Following a successful audit, our customers typically spend approximately one hour per week maintaining and managing their compliance program within the platform.

24. I already do a pen test, why do I need SOC 2?

Penetration testing and SOC 2 serve distinct purposes within cybersecurity.

- Penetration testing is a focused assessment designed to actively probe an organization's security defences to uncover vulnerabilities that could be exploited by malicious actors.
- SOC 2 is a voluntary compliance framework that allows organizations to demonstrate their commitment to data security and privacy. It focuses on establishing and maintaining controls around five key trust service principles: security, availability, processing integrity, confidentiality, and privacy.

25. Do Pen Test, VA Scans, and other audit services come as a part of your offering bundle?

Yes, we offer bundled packages for customers who require them. Our VAPT partners assist customers by delivering tailored solutions at highly competitive rates.

26. What is the penalty for non-compliance with SOC 2?

Failure to comply with SOC 2 does not result in legal penalties, but it can lead to significant indirect costs, such as lost revenue and prolonged sales cycles. Additionally, without SOC 2 certification, an organization may face heightened risks of data breaches due to insufficient security controls, potentially resulting in financial losses amounting to millions. Non-compliance can also lead to civil lawsuits from unhappy customers, damaging both the company's reputation and its business prospects.

27. Does SOC 2 certification mean a company is completely secure?

Emphatically no. SOC 2 isn't a pass/fail test where you're trying to prove you have zero vulnerabilities. If it were, we'd live in a world with no data breaches. What SOC 2 certification proves is that you have processes in place to mitigate potential risks, and that you consider the security ramifications of every decision.

28. Do I still need to use Letsbloom after I receive my audit?

While you can stop using Letsbloom after your audit, we don't recommend it. Continuous compliance is crucial for several reasons.

- Firstly, compliance yesterday doesn't guarantee compliance today, and your customers know this. They want to ensure their data is safe today, so a report from last quarter won't cut it.
- Secondly, maintaining daily compliance through continuous monitoring helps improve overall security by identifying risks and failing controls promptly.
- Lastly, staying compliant year-round reduces the time and effort required for your next audit.

By maintaining compliance (with minimal effort thanks to automation) throughout the year, you can avoid last-minute stress and make your next audit much smoother and more efficient.