SOC 2 Readiness Checklist

A practical pre-audit checklist for startups and scale-ups

Preparing for SOC 2 does not start with the auditor. It starts with understanding your systems, defining your scope, identifying control gaps, and building reliable evidence.

Use this checklist to identify the major areas your organization should review before beginning a SOC 2 engagement.

This checklist is an educational starting point, not an audit opinion, legal advice, or a substitute for professional SOC 2 guidance.

1. Define Your SOC 2 Scope

Before implementing controls, determine what products, services, systems, people, locations, and data are actually in scope.

- [ ] We have clearly identified the product or service being evaluated.
- [ ] We have documented the boundaries of the system in scope.
- [ ] We have identified the applications, infrastructure, cloud services, databases, and other technologies supporting the service.
- [ ] We know what customer data and sensitive information the system processes.
- [ ] We have identified relevant internal teams and third parties supporting the service.
- [ ] We have documented key system dependencies and external service providers.
- [ ] We have identified which Trust Services Criteria are relevant to our engagement.

Start with scope. Trying to prepare the entire company for SOC 2 at once can create unnecessary work.

2. Establish Security Governance

- [ ] Security responsibilities are clearly assigned to individuals or teams.
- [ ] We have a documented information security policy.
- [ ] We have documented access control requirements.
- [ ] We have documented incident response procedures.
- [ ] We have documented change management procedures.
- [ ] We have documented risk management practices.
- [ ] We review and update security policies periodically.
- [ ] Employees and relevant contractors acknowledge applicable security policies.
- [ ] Management receives appropriate visibility into security risks and control performance.

Policies should reflect how the company actually operates. Avoid creating policies that exist only for the audit.

3. Control Access to Systems and Data

- [ ] Each employee has an individual account where practical.
- [ ] Access is granted based on job responsibilities.
- [ ] Privileged access is restricted.
- [ ] Access requests and approvals are documented.
- [ ] Employee access is reviewed periodically.
- [ ] Access is removed or modified promptly when someone changes roles or leaves.
- [ ] Multi-factor authentication is enabled for critical systems.
- [ ] Administrative accounts are appropriately protected.
- [ ] Service accounts and API credentials are controlled.
- [ ] We know who has access to production systems and sensitive data.

4. Secure Your Technology Environment

- [ ] Production infrastructure is separated appropriately from development environments.
- [ ] Security configurations are documented for critical systems.
- [ ] Security updates and patches are managed.
- [ ] Endpoint devices are protected using appropriate security controls.

- [ ] Network access is restricted based on business need.
- [ ] Cloud infrastructure permissions are reviewed.
- [ ] Secrets, API keys, and credentials are securely stored.
- [ ] Encryption is used appropriately for sensitive data.
- [ ] Security logging is enabled for important systems.
- [ ] Logs are retained for an appropriate period.
- [ ] Security alerts are monitored and investigated.

5. Identify and Manage Security Risks

- [ ] We maintain a process for identifying security risks.
- [ ] Security risks are documented and prioritized.
- [ ] Risk owners are assigned where appropriate.
- [ ] Vulnerabilities are identified and tracked.
- [ ] Critical vulnerabilities have defined remediation expectations.
- [ ] Security assessments or testing are performed where appropriate.
- [ ] Exceptions to security requirements are documented and approved.
- [ ] Risk treatment decisions are tracked.

6. Prepare for Security Incidents

- [ ] We have a documented incident response plan.
- [ ] Security incidents have defined severity levels or escalation criteria.
- [ ] Roles and responsibilities during an incident are defined.
- [ ] Relevant employees know how to report a suspected security incident.
- [ ] Security incidents are documented.
- [ ] We have a process for investigating and responding to incidents.
- [ ] We have considered customer and regulatory notification requirements where applicable.
- [ ] We periodically test or review our incident response process.

7. Control Changes to Production

- [ ] Changes to production systems follow a defined process.
- [ ] Changes are reviewed and approved appropriately.
- [ ] Code changes are tracked through version control.
- [ ] Production deployments are traceable to specific changes.
- [ ] Testing is performed before significant production changes where appropriate.
- [ ] Emergency changes have a defined process.
- [ ] Access to production deployment systems is restricted.

8. Manage Third-Party Risk

- [ ] We maintain an inventory of relevant vendors and service providers.
- [ ] We identify vendors that can access sensitive information or critical systems.
- [ ] Security requirements are considered during vendor selection.
- [ ] Vendor risk is assessed based on the nature of the service and information involved.
- [ ] Relevant contracts include appropriate security or data protection requirements.
- [ ] Critical vendors are reviewed periodically.
- [ ] We collect and review relevant third-party assurance information where appropriate.

9. Build Security Awareness

- [ ] Employees receive security awareness training.
- [ ] Training covers relevant security responsibilities.
- [ ] Employees understand how to report security incidents.
- [ ] Security responsibilities are included in onboarding where appropriate.
- [ ] Security responsibilities are addressed during offboarding.

- [ ] Personnel with specialized security responsibilities receive appropriate training.

10. Build Your Evidence Trail

SOC 2 readiness is not just about having policies. You need to demonstrate that relevant controls are designed appropriately and, for a Type 2 examination, operated over the applicable examination period.

- [ ] We know which controls require evidence.
- [ ] Evidence is stored in a centralized location.
- [ ] Evidence has identifiable dates and owners.
- [ ] Evidence demonstrates that controls actually operated, not merely that policies exist.
- [ ] Access reviews are documented.
- [ ] Security training completion is documented.
- [ ] Risk assessments are documented.
- [ ] Incident records are retained where applicable.
- [ ] Change management records are retained.
- [ ] Vendor reviews are documented.
- [ ] Security monitoring and testing evidence is retained where appropriate.
- [ ] We can explain who performs each control, how often it occurs, and what evidence proves it occurred.

The exact engagement scope and observation period should be confirmed with your CPA firm or auditor.

Your Initial Readiness Check

Count how many areas you can confidently answer "Yes" to.

- [ ] Scope is defined
- [ ] Security policies exist and reflect actual practices
- [ ] Access controls are established
- [ ] MFA protects critical systems
- [ ] Production systems are appropriately protected
- [ ] Risk management is documented
- [ ] Incident response is established
- [ ] Change management is controlled
- [ ] Vendor risk is managed
- [ ] Security training is documented
- [ ] Evidence is centralized
- [ ] Control owners are identified

What your score means:

Strong foundation: Most areas are established, documented, and producing evidence.

Needs attention: Several controls exist, but documentation, ownership, consistency, or evidence needs improvement.

Early stage: Important foundational controls are still being established. A readiness assessment can help prioritize the highest-impact gaps before investing in the full SOC 2 process.

This checklist does not assign a readiness score or claim that any specific result means a company is SOC 2 ready.

Before Starting a SOC 2 Engagement

Ask these five questions:

1. **What exactly is in scope?**
2. **Which Trust Services Criteria are relevant to our business and engagement?**
3. **Which controls already exist?**
4. **Which controls are missing or inconsistently operated?**
5. **Can we produce reliable evidence showing that our controls operate as intended?**

If you cannot confidently answer these questions, a readiness assessment may be the right starting point.

Not Sure Where Your SOC 2 Gaps Are?

SecureHops helps startups and scale-ups identify security and compliance gaps, prioritize remediation, and build a practical roadmap toward audit readiness.

Get Your Security Assessment !' securehops.com/assessment
Explore GRC Consulting !' securehops.com/services/grc-consulting

---

SecureHops
Security for Startups & Scale-Ups | securehops.com