SecurityDocs
SOC 2 Compliance Templates

Interactive Compliance Guide

SOC 2 Compliance Checklist

Your step-by-step guide to SOC 2 compliance. Track your progress, understand requirements, and ensure you don't miss critical steps on your compliance journey.

Your Progress Overview

0%	0	45
Overall Progress	Items Completed	Items Remaining

Pro Tips for Success

- **Start early:** SOC 2 preparation typically takes 6-12 months
- **Focus on your scope:** Don't try to include everything at once
- **Document everything:** Evidence collection starts from day one

Getting Started (Before Implementation)

0/5 completed

These foundational steps set you up for success. Complete these before diving into technical implementation.

- [ ] **Define your scope** - Identify systems that store, process, or transmit customer data
  Required · Easy

- [ ] **Choose your criteria** - Start with Security + Availability for most SaaS companies
  Required ● Easy
- [ ] **Assign ownership** - Designate a compliance lead and cross-functional team
  Required ●● Medium
- [ ] **Set timeline** - Plan 6-12 months for implementation + evidence collection ● Easy
- [ ] **Budget planning** - Allocate resources for tools, auditor, and internal time ●● Medium

💡 **Need help with planning?** Check out our Implementation Guides at security-docs.com/resources/implementation-guides

Documentation & Policies ✨ Templates Available

0/5 completed

✨ **Templates Available:** Save months of work with our professionally written, SOC 2-aligned policy templates.

- [ ] **Information Security Policy** - Master policy covering all security practices
  Required ●●● Advanced
- [ ] **Access Control Policy** - User access management and authentication requirements
  Required ●● Medium
- [ ] **Incident Response Plan** - Procedures for detecting and responding to security incidents Required ●● Medium
- [ ] **Data Management Policy** - How customer data is handled throughout its lifecycle
  Required ●● Medium
- [ ] **Risk Management Policy** - Process for identifying and mitigating risks
  Required ●● Medium

🎯 **Save time:** Our Policy Templates are professionally written and SOC 2 aligned. Visit security-docs.com/products/policies

Technical Security Controls

0/7 completed

- [ ] **Multi-factor authentication** - Implement MFA for all administrative access
  Required · Easy
- [ ] **Network security** - Firewalls, network segmentation, VPN access
  Required · Medium
- [ ] **Data encryption** - Encrypt data at rest and in transit Required · Medium
- [ ] **Backup and recovery** - Regular backups with tested restore procedures
  Required · Medium
- [ ] **System monitoring** - Security information and event management (SIEM)
  Advanced
- [ ] **Vulnerability management** - Regular scans and patch management Medium
- [ ] **Antivirus/anti-malware** - Endpoint protection across all systems Easy

Need detailed guidance? Check our Evidence Explanations for implementation details at security-docs.com/products/evidence

Administrative Controls

0/5 completed

- [ ] **Employee background checks** - Verify identity and background for new hires Easy
- [ ] **Security awareness training** - Regular training for all employees Required · Easy
- [ ] **Access reviews** - Quarterly reviews of who has access to what systems
  Required · Medium
- [ ] **Vendor management** - Due diligence and contracts for third-party providers
  Medium
- [ ] **Physical security** - Secure facilities and device management Easy

Operational Procedures

0/5 completed

- [ ] **Change management** - Formal process for system and application changes
  Required ●● Medium
- [ ] **Asset inventory** - Maintain list of all hardware and software assets ● Easy
- [ ] **Log monitoring** - Collect and review security logs regularly Required ●● Medium
- [ ] **Performance monitoring** - Track system availability and performance ● Easy
- [ ] **Disaster recovery testing** - Regular tests of backup and recovery procedures
  ●● Medium

⚡ **Ready-to-use forms:** Our Document Templates provide procedures and forms at security-docs.com/products/documents

Evidence Collection (3-12 months before audit)

0/7 completed

Start collecting evidence as soon as your controls are operational. Auditors need to see that controls operated effectively over time.

- [ ] **Access control evidence** - Logs of user provisioning/deprovisioning
  Required · Easy
- [ ] **Security monitoring logs** - Evidence of ongoing monitoring activities
  Required · Medium
- [ ] **Training records** - Documentation of employee security training Required · Easy
- [ ] **Incident documentation** - Records of any security incidents and responses
  Medium
- [ ] **Vulnerability scan reports** - Regular security assessments and remediation
  Medium
- [ ] **Change management logs** - Documentation of all system changes
  Required · Medium
- [ ] **Backup verification** - Proof that backups are working and tested Easy

🎯 **Confused about evidence?** Our Evidence Bundle explains exactly what auditors expect at security-docs.com/products/evidence-bundle

Pre-Audit Preparation

0/5 completed

- [ ] **Internal readiness assessment** - Self-evaluation against SOC 2 requirements
  Medium
- [ ] **Auditor selection** - Research and interview potential audit firms Easy
- [ ] **Evidence organization** - Compile all documentation and evidence Medium
- [ ] **Team preparation** - Brief all team members who will interact with auditors Easy

- [ ] **Gap remediation** - Address any identified control gaps ●●● Advanced

Common Pitfalls to Avoid

0/5 completed

⚠ **Avoid these mistakes:** These are the most common reasons companies fail their first audit.

- [ ] **Scope too broad** - Start narrow with core customer-facing systems only ● Easy
- [ ] **Documentation overload** - Focus on what you actually do, not aspirational goals ●● Medium
- [ ] **Last-minute preparation** - Controls need to operate for months before audit ●● Medium
- [ ] **Ignoring availability** - Most SaaS companies need this criterion ● Easy
- [ ] **Weak access controls** - This is the #1 area where companies fail audits ●●● Advanced

Ready to Get Started?

Don't start from scratch. Our templates and guidance help you implement these controls correctly the first time.

Policy Templates

Professional policies that address SOC 2 requirements

security-docs.com/products/policies

Evidence Guidance

Learn what auditors look for with detailed explanations

security-docs.com/products/evidence

Complete Bundle

Everything you need for SOC 2 compliance

security-docs.com/products/complete-bundle

This checklist provides general guidance. Every organization's SOC 2 journey is unique based on their specific systems, risks, and business model.