SOC 2 Type I Security Readiness Checklist

Your Essential Guide to SOC 2 Security Compliance

What is SOC 2 Type I?

SOC 2 (Service Organization Control 2) is a security framework developed by the American Institute of CPAs (AICPA) that demonstrates your organization has proper controls in place to protect customer data. A Type I audit evaluates whether your security controls are properly designed and documented at a specific point in time. Think of it as a comprehensive snapshot that proves you have the right safeguards established and ready to operate.

This checklist covers the Security Trust Service Criteria, which is the foundation of any SOC 2 audit and focuses on protecting systems and data from unauthorized access. While SOC 2 also offers additional criteria for Availability, Confidentiality, Processing Integrity, and Privacy, Security is mandatory and represents the core requirements every service organization must meet.

The elements outlined here represent the minimum viable security program needed to successfully complete a SOC 2 Type I audit. Organizations typically need 3-6 months to implement these requirements from scratch, though timelines vary based on your current security maturity and organizational complexity.

1. Organizational Foundation

The organizational foundation establishes the scope and structure of your security program. Auditors need to understand what systems and data are in scope, how your organization is structured, and who is responsible for security decisions. This documentation provides the context for evaluating all other controls.

System Description

Your system description is a comprehensive narrative that explains what your service does, how it works, and what's included in the SOC 2 scope. This becomes part of the final audit report and helps report readers understand your environment. Key elements include:

- Document what your system does, who uses it, and what data it processes
- Define the boundaries of what's included in your SOC 2 scope (which applications, infrastructure, data)
- List the key technology components (cloud platforms, databases, applications)
- Identify what types of data you handle (customer data, payment information, personal data)

Organizational Chart & Roles

Auditors need to see that security responsibilities are clearly defined and that appropriate personnel have been assigned to key security functions. This demonstrates organizational commitment and accountability. Essential requirements include:

- Create an org chart showing reporting structure and key security roles
- Assign a Security Officer or CISO responsible for security program
- Define who owns security decisions and approvals

- Document team members' security responsibilities in their job descriptions

2. Policies & Governance

Policies are the foundation of your security program. They document your organization's commitment to security and establish the rules and procedures that govern how systems and data are protected. All policies should be formally approved by executive management, reviewed at least annually, and communicated to relevant personnel.

Core Security Policies (Required)

These policies govern internal operations and are required by SOC 2 auditors. Each policy should be comprehensive, clearly written, and include specific procedures for implementation:

- Information Security Policy - Your master security policy defining program scope and objectives
- Acceptable Use Policy - Rules for using company systems and data appropriately
- Access Control Policy - How you grant, review, and remove access to systems
- Data Classification Policy - How you categorize data by sensitivity level
- Incident Response Policy - What happens when something goes wrong
- Business Continuity/Disaster Recovery Policy - Your plan to keep running during disruptions
- Change Management Policy - How you safely make changes to production systems
- Vendor Management Policy - How you evaluate and monitor third-party providers

Public-Facing Policies (Required on Website)

These policies must be published on your public website, typically in the footer or a dedicated security/trust page. They demonstrate transparency and commitment to customers:

- Privacy Policy - How you collect, use, and protect customer information
- Terms of Service - Legal agreement with your customers
- Security Page - Overview of your security practices and certifications

3. Cybersecurity Governance

Effective governance demonstrates that security is actively managed at an executive level, not just delegated to IT. Auditors look for evidence that leadership is engaged, informed, and making decisions about security risks and initiatives.

Security Meetings & Documentation

Regular security meetings with documented minutes provide evidence of ongoing oversight and decision-making. At minimum, conduct quarterly meetings that include executive leadership. Meeting documentation should capture:

- Hold regular security meetings (at minimum quarterly) with leadership
- Document meeting minutes showing security topics discussed and decisions made
- Review security metrics, incidents, and risk status at each meeting
- Ensure executive management is engaged and approves major security decisions

4. Risk Management

Risk management is a core requirement of SOC 2 and demonstrates that you systematically identify, assess, and respond to security threats. The risk assessment drives your control selection and helps justify security investments to leadership.

Risk Assessments

Conduct a comprehensive risk assessment at least annually and whenever significant changes occur to your environment. Your risk assessment process should include:

- Conduct an annual organizational risk assessment identifying security threats
- Document risks with likelihood, impact, and treatment plans
- Maintain a Risk Register tracking all identified risks and their status
- Get executive approval for accepting any high risks
- Review and update risk assessment when major changes occur

Vulnerability Management

Technical vulnerability scanning provides concrete evidence of security weaknesses and your process for addressing them. This is one of the most objective measures of security posture. Essential elements include:

- Run vulnerability scans on your infrastructure at least quarterly
- Prioritize and track remediation of identified vulnerabilities
- Document how quickly you patch critical, high, and medium severity issues
- Maintain evidence of scan results and remediation activities

Financial Risk Assessment

Understanding the financial implications of security risks helps leadership make informed decisions about security investments and risk acceptance. This analysis should consider:

- Evaluate financial impacts of potential security incidents
- Consider costs of data breaches, downtime, and reputational damage
- Review cyber insurance coverage and limits
- Document financial risk tolerance and mitigation strategies

5. Access Controls

Access controls are fundamental to security and among the most scrutinized areas in a SOC 2 audit. Proper access management ensures that only authorized individuals can access systems and data, and that access is appropriate for their job responsibilities.

User Access Management

A formal user access lifecycle process ensures consistency and auditability. This process should cover the entire user lifecycle from onboarding through termination:

- Implement formal process for provisioning access when employees join
- Require manager approval before granting system access

- Follow principle of least privilege - give minimum access needed for the job
- Review user access at least annually to ensure it's still appropriate
- Immediately revoke access when employees leave or change roles
- Document all access requests and approvals

Multi-Factor Authentication (MFA)

MFA is now essentially mandatory for SOC 2 compliance and represents one of the most effective security controls. MFA significantly reduces the risk of unauthorized access even if passwords are compromised. Implementation requirements:

- Require MFA for all access to production systems and sensitive data
- Enforce MFA for remote access and administrative accounts
- Use authenticator apps or hardware tokens (not SMS when possible)
- Document MFA requirements in your Access Control Policy

Password Requirements

While MFA is the primary authentication control, strong password policies remain important for defense in depth. Modern password requirements should balance security with usability:

- Require strong passwords (minimum 12 characters, complexity requirements)
- Prohibit password sharing and reuse
- Lock accounts after failed login attempts

6. Incident Response Plan (IRP)

An incident response plan demonstrates that your organization is prepared to handle security events effectively, minimizing damage and recovery time. Auditors want to see both a documented plan and evidence that you've tested it.

- Create a documented plan for responding to security incidents
- Define what constitutes a security incident (data breach, unauthorized access, malware, etc.)
- Assign roles and responsibilities for incident response team
- Establish procedures for detection, containment, investigation, and recovery
- Include communication plans for notifying affected parties
- Test your incident response plan at least annually (tabletop exercise)
- Document all security incidents, even minor ones, with response actions taken

7. Secure Development Lifecycle (SDLC)

For organizations that develop software, documenting your development and deployment processes is essential. The SDLC demonstrates that security is considered throughout the development process and that changes to production are controlled, tested, and tracked.

- Document your software development process from design to deployment
- Require code reviews before changes go to production
- Separate development, testing, and production environments
- Use version control (Git) for all code changes
- Test changes before deploying to production

- Maintain change logs documenting what was changed and why
- Implement automated testing in your CI/CD pipeline

8. Data Protection & Encryption

Data protection controls ensure that sensitive information remains confidential and protected from unauthorized access or disclosure. Encryption is the primary technical control for protecting data, both when it's being transmitted over networks and when it's stored on disks or in databases.

Encryption

- Encrypt data in transit using TLS/SSL (HTTPS for websites and APIs)
- Encrypt data at rest in databases and file storage
- Encrypt laptop and mobile device hard drives (full disk encryption)
- Use encrypted connections for remote access (VPN or zero-trust tools)

Data Handling

- Classify data by sensitivity (public, internal, confidential, restricted)
- Define data retention and deletion policies
- Prohibit storing production data in development environments
- Implement secure data disposal procedures for end-of-life equipment

9. Backup & Recovery

Backup and recovery capabilities are critical for business continuity. These controls ensure you can recover from data loss, system failures, or disasters. Auditors want to see not just that you have backups, but that you regularly test restoration.

- Implement automated daily backups of critical systems and data
- Store backups in separate geographic location or cloud region
- Encrypt backup data at rest and in transit
- Test backup restoration at least quarterly to ensure they work
- Document recovery time objectives (RTO) and recovery point objectives (RPO)
- Maintain backup logs and monitor for failures

10. Vendor & Third-Party Management

Third-party vendors represent an extension of your security perimeter. When vendors access your systems or process your data, their security becomes your security. SOC 2 requires that you assess and monitor vendor security risks.

- Maintain inventory of all vendors who access your data or systems
- Assess security risks before engaging new vendors
- Review vendor security documentation (SOC 2 reports, questionnaires, policies)
- Include security requirements in vendor contracts

- Review vendor security posture annually or when contracts renew
- Document vendor risk assessments and approval decisions

11. Security Awareness Training

Employees are often described as the weakest link in security, but with proper training they become your strongest defense. Security awareness training ensures all personnel understand their security responsibilities and can recognize common threats.

- Provide security awareness training to all employees upon hire
- Conduct annual refresher training covering common threats (phishing, social engineering)
- Train employees on acceptable use of company systems and data handling
- Document training completion and maintain attendance records
- Test employee awareness through simulated phishing exercises

12. Monitoring & Logging

Comprehensive logging and monitoring capabilities enable you to detect security incidents, investigate suspicious activities, and demonstrate compliance. Logs provide the audit trail showing who did what, when they did it, and from where.

- Enable logging on all critical systems (applications, databases, infrastructure)
- Log security-relevant events including authentication, access, and configuration changes
- Retain logs for at least 90 days (one year recommended)
- Implement automated monitoring and alerts for suspicious activities
- Review logs regularly for security anomalies
- Protect log data from unauthorized modification or deletion

Getting Started: Your 90-Day Roadmap

Achieving SOC 2 readiness typically takes 3-6 months. Here's a suggested phased approach:

Month 1: Foundation

- Define system scope and create system description
- Assign security roles and create org chart
- Draft core policies (Information Security, Access Control, Acceptable Use)
- Conduct initial risk assessment

Month 2: Implementation

- Complete all required policies and publish public-facing policies
- Implement MFA and access controls
- Set up vulnerability scanning and backup testing
- Document SDLC and change management processes

Month 3: Evidence & Readiness

- Conduct vendor risk assessments
- Complete employee security training
- Hold security meeting and document minutes
- Test incident response plan
- Collect and organize audit evidence
- Engage SOC 2 auditor

Final Tips for Success

- Start early - Don't wait until you need SOC 2 to begin implementing controls
- Document everything - If it's not documented, it didn't happen in an audit
- Use a GRC platform - Tools like Secureframe, Vanta, or Drata streamline the process
- Be consistent - Follow your own policies; auditors look for gaps between policy and practice
- Ask for help - Consider working with a consultant or auditor who can guide you through the process

This checklist covers the essential minimum requirements. Every organization is different, and your specific needs may vary based on your technology stack, industry, and customer requirements. The goal is to build a security program that not only passes an audit but genuinely protects your organization and customers.

Need help getting started? Contact us to learn how we can support your compliance journey.