PLATOPS

Get SOC 2 certified with confidence

PlatOps provides security-first DevOps, cloud, and managed IT services for small and mid-sized businesses. We help organizations achieve compliance certifications, secure their infrastructure, and modernize their operations — without the enterprise price tag.

From SOC 2 and HIPAA compliance to cloud migrations and 24/7 monitoring, our team of engineers delivers measurable results with a 100% audit pass rate across 60+ client engagements.

100%	**60+**	**8-12 wk**	**24/7**
AUDIT PASS RATE	ORGANIZATIONS	AVG. TO COMPLIANCE	MONITORING

SOC 2 Readiness Checklist

Complete Guide to SOC 2 Type I & Type II Certification

Prepared by PlatOps Security Version 1.0 | January 2026

SOC 2 AT A GLANCE

What is SOC 2?

SOC 2 (Service Organization Control 2) is an auditing framework developed by the AICPA that evaluates how service organizations manage customer data based on five Trust Service Criteria.

The 5 Trust Service Criteria

1. **Security** (Required) - Protection against unauthorized access
2. **Availability** (Optional) - System uptime and accessibility
3. **Processing Integrity** (Optional) - Accurate and timely data processing
4. **Confidentiality** (Optional) - Protection of sensitive information
5. **Privacy** (Optional) - Collection and use of personal information

Type I vs Type II Comparison

ASPECT	TYPE I	TYPE II
What it proves	Controls are designed properly	Controls operate effectively over time
Observation period	Point-in-time (single date)	3-12 months (typically 6 months)
Customer acceptance	Initial due diligence	Industry standard - most require this
Time to complete	4-8 weeks	Observation period + 4-8 weeks
Cost	$20,000-$50,000	$30,000-$80,000

SOC 2 TIMELINE

Phase 1: Gap Assessment (2-4 weeks)

- □ Inventory all systems in scope
- □ Review existing policies and procedures
- □ Identify control gaps
- □ Prioritize remediation efforts
- □ Estimate budget and resources needed

Phase 2: Remediation (2-6 months)

- □ Draft/update security policies
- □ Implement technical controls
- □ Establish monitoring and logging
- □ Train employees on procedures
- □ Document all processes

Phase 3: Readiness Assessment (2-4 weeks)

- □ Conduct internal audit
- □ Test all controls
- □ Collect evidence samples
- □ Address any findings
- □ Prepare evidence repository

Phase 4: SOC 2 Audit (4-8 weeks)

- □ Select and engage auditor
- □ Provide evidence and access
- □ Respond to auditor inquiries
- □ Address any findings
- □ Receive final report

Total Timeline: 3-6 months for Type I, 6-12 months for Type II

SECURITY (Required TSC)

Security is the only mandatory Trust Service Criteria. All SOC 2 audits must include Security.

Access Control (7 items)

- □ Implement role-based access control (RBAC)
- □ Enforce unique user IDs for all employees
- □ Require multi-factor authentication (MFA)
- □ Establish password complexity requirements (12+ characters, complexity)
- □ Review and revoke access for terminated employees within 24 h

Network Security (6 items)

- □ Deploy and configure firewalls
- □ Segment networks (production vs. development)
- □ Encrypt data in transit (TLS 1.2+)
- □ Implement intrusion detection/prevention (IDS/IPS)
- □ Secure and monitor VPN access
- □ Disable unnecessary ports and services

Endpoint Security (5 items)

- □ Deploy endpoint protection on all devices
- □ Enable full-disk encryption
- □ Implement mobile device management (MDM)
- □ Maintain software patch management program
- □ Configure automatic screen locks (5 min max)

Monitoring & Logging (5 items)

- □ Centralize log collection and storage
- □ Monitor and alert on security events
- □ Retain logs for at least 1 year
- □ Implement SIEM or equivalent monitoring
- □ Document incident response procedures

Security Section Total: 23 items

AVAILABILITY (Optional TSC)

Add Availability if you have SLA commitments or uptime guarantees.

Infrastructure (5 items)

- □ Define and document SLAs with uptime commitments
- □ Implement redundant infrastructure
- □ Configure auto-scaling capabilities
- □ Deploy load balancers
- □ Establish multiple availability zones/regions

Disaster Recovery (6 items)

- □ Create and document disaster recovery plan
- □ Define RPO and RTO objectives
- □ Implement automated backups
- □ Test backup restoration quarterly
- □ Maintain off-site backup copies
- □ Document failover procedures

Monitoring (5 items)

- □ Publish status page for customers
- □ Document on-call procedures

Availability Section Total: 16 items

PROCESSING INTEGRITY (Optional TSC)

Add Processing Integrity if data accuracy is critical (financial systems, healthcare).

Data Validation (5 items)

- □ Implement input validation controls
- □ Verify data completeness checks
- □ Establish error handling procedures
- □ Document data processing workflows
- □ Implement transaction logging

Quality Assurance (5 items)

- □ Conduct regular data quality audits
- □ Implement automated testing pipelines
- □ Establish code review requirements
- □ Document change management procedures
- □ Maintain staging/testing environments

Monitoring (4 items)

- □ Monitor processing errors and exceptions
- □ Track data reconciliation metrics
- □ Alert on processing anomalies
- □ Document and investigate failures

Processing Integrity Section Total: 14 items

CONFIDENTIALITY (Optional TSC)

Add Confidentiality if you handle sensitive business data or trade secrets.

Data Classification (5 items)

- □ Define data classification policy
- □ Identify and label confidential data
- □ Document data handling procedures
- □ Establish data retention schedules
- □ Implement secure data disposal procedures

- □ Encrypt data in transit (TLS 1.2+)
- □ Implement key management procedures
- □ Rotate encryption keys annually
- □ Secure key storage (HSM or equivalent)

Access Controls (5 items)

- □ Restrict access to confidential data
- □ Implement data loss prevention (DLP)
- □ Monitor access to sensitive systems
- □ Require NDAs for employees/contractors
- □ Audit third-party data access

Confidentiality Section Total: 15 items

PRIVACY (Optional TSC)

Add Privacy if you collect personal information from end users or are subject to GDPR/CCPA.

Privacy Governance (5 items)

- □ Publish privacy policy
- □ Document data collection practices
- □ Establish data subject rights procedures
- □ Appoint privacy officer/DPO if required
- □ Conduct privacy impact assessments

Consent & Notice (5 items)

- □ Obtain consent before data collection
- □ Provide clear privacy notices
- □ Document legal basis for processing
- □ Honor opt-out requests
- □ Maintain consent records

Data Subject Rights (5 items)

- □ Enable access requests (DSAR)
- □ Support data deletion requests
- □ Allow data portability
- □ Document request handling procedures
- □ Respond within regulatory timeframes (30 days GDPR, 45 days CCPA)

Privacy Section Total: 15 items

1. Starting Too Late

Problem: SOC 2 prep takes 3-6 months. Starting with urgent deadlines leads to gaps. **Solution:** Begin at least 6 months before target audit date.

2. Incomplete Documentation

Problem: Controls in place but lacking evidence. Auditors need proof. **Solution:** Document all policies, procedures, and evidence from day one.

3. Scope Creep

Problem: Including too many systems or all 5 TSC unnecessarily. **Solution:** Start with Security only and minimum scope for customer requirements.

4. Neglecting Employee Training

Problem: Technical controls alone aren't enough. Human error causes most breaches. **Solution:** Implement security awareness training and track completion.

5. No Continuous Monitoring

Problem: Treating SOC 2 as point-in-time vs ongoing compliance. **Solution:** Implement continuous monitoring and regular control testing.

6. Choosing the Wrong Auditor

Problem: Not all CPA firms understand your tech stack or industry. **Solution:** Select auditor with relevant experience in your industry.

CHECKLIST SUMMARY & SCORING

Total Controls by Category

CATEGORY	REQUIRED	OPTIONAL	TOTAL
Security	Yes	-	23
Availability	-	Yes	16
Processing Integrity	-	Yes	14
Confidentiality	-	Yes	15
Privacy	-	Yes	15
TOTAL	**23**	**60**	**83**

Your Readiness Score

Minimum for Type I: Security complete (23 items) **Typical Enterprise:** Security + 1-2 optional TSCs (35-50 items) **Full Compliance:** All 5 TSCs (83 items)

Scoring Guide

Ready to Get Started?

Let our team of security and infrastructure experts help you achieve your goals faster.

100%	60+	8-12 wk	24/7
AUDIT PASS RATE	ORGANIZATIONS SERVED	AVG. TIME TO COMPLIANCE	MONITORING & SUPPORT

Get Free Assessment | Book Strategy Call | SOC 2 Compliance Services

Email: hello@platops.com   Phone: (202) 864-1197   Web: platops.com

This document is provided for informational purposes only. Requirements may vary based on your organization's specific circumstances. PlatOps is a registered trademark. Redistribution without permission is prohibited.