SOC 2 COMPLETE IMPLEMENTATION GUIDE

Everything You Need to Get Certified in 8-12 Weeks

Published by: Tranquility Cybersecurity & Assurance
Version: 2.0 (Updated January 2026)
Authors: ISO 27001 Lead Auditors with 500+ SOC 2 certifications
Target Audience: SaaS Founders, CTOs, Compliance Managers

ABOUT THIS GUIDE

This guide is written by actual SOC 2 auditors who have conducted 500+ SOC 2 audits for SaaS companies ranging from 5-person startups to 500-person scale-ups. We've seen what works, what fails, and what's a complete waste of time.

What makes this different:

- Written by Lead Auditors, not consultants
- Real examples from actual audits
- Focused on SaaS/tech companies
- Practical, actionable steps (no compliance theater)
- Updated for 2025 AICPA Trust Services Criteria

TABLE OF CONTENTS

PART 1: FOUNDATION

CHAPTER 1: WHY SOC 2 MATTERS FOR SAAS COMPANIES

The Enterprise Deal Blocker

You're in the final stages of closing a $500K ARR enterprise deal. Legal sends over their security questionnaire. Question 47: "Do you have a SOC 2 report?"

You don't.

Deal stalls. Procurement says, "Circle back when you're certified." You just lost 6-12 months of revenue because you don't have a 50-page PDF.

This is the #1 reason SaaS companies get SOC 2 certified. Not because they want to. Because they have to.

What Is SOC 2?

SOC 2 (System and Organization Controls 2) is an audit framework developed by the AICPA (American Institute of CPAs). It verifies that your organization has implemented adequate controls to protect customer data.

Key Points:

- **Not a certification** (it's an attestation/report)
- **Focuses on 5 Trust Service Criteria:** Security (required), Availability, Processing Integrity, Confidentiality, Privacy (optional)
- **Two Types:** Type I (point-in-time), Type II (6-12 month operating effectiveness)
- **No pass/fail:** You either get a clean opinion or you don't

Who Needs SOC 2?

You NEED SOC 2 if:

- Selling to enterprise customers (Fortune 5000)
- Handling sensitive customer data
- Operating in regulated industries (finance, healthcare, insurance)
- Customer security questionnaires keep asking for it

You DON'T need SOC 2 if:

- Selling to SMBs who don't ask for it
- Pre-revenue / pre-product market fit
- No customer data processing
- International customers only want ISO 27001

SOC 2 vs Other Standards

Standard	Region	Best For	Cost
SOC 2	US	US SaaS selling to enterprises	₹6-10L
ISO 27001	Global	International sales, EU customers	₹5-8L
HIPAA	US	Healthcare data (PHI)	₹4-7L
PCI DSS	Global	Payment card processing	₹8-15L

Pro Tip: If selling globally, get ISO 27001 first. 80% of controls overlap with SOC 2. Then add SOC 2 Type I for US customers for an additional ₹2-3L.

The Real Cost of NOT Having SOC 2

Let's do the math:

Lost Revenue:

- Average enterprise deal: ₹40L ARR
- Deals lost per year without SOC 2: 2-5
- **Annual lost revenue: ₹80L - ₹2Cr**

Opportunity Cost:

- Sales cycle延长: +3-6 months
- Win rate drop: -40%
- Deal size reduction (downgrades to "pilot"): -60%

Implementation Cost:

- DIY with platform: ₹6-8L (12-18 months)
- With consultant: ₹8-12L (6-9 months)
- With Lead Auditor: ₹6-10L (8-12 weeks)

ROI Calculation:

```
Cost: ₹8L
Revenue unlocked Year 1: ₹80L (2 enterprise deals)
ROI: 10x in first year
Payback period: 1 deal (1-2 months)
```

The question isn't "Can we afford SOC 2?" It's "Can we afford NOT to have SOC 2?"

CHAPTER 2: UNDERSTANDING TRUST SERVICES CRITERIA (TSC)

The 5 Trust Service Categories

SOC 2 is built on 5 Trust Service Categories. Think of them as 5 different lenses through which auditors examine your security program.

1. SECURITY (Required - Everyone Needs This)

What it covers:

- Access controls (who can access what)
- Logical and physical security
- System operations (monitoring, incident response)

- Change management
- Risk mitigation

Common Criteria (CC): CC1.1 - CC9.2 (64 total criteria under Security)

In plain English: "Do you have basic security controls in place? Can you prove unauthorized people can't access customer data?"

Key Controls:

- Multi-factor authentication (MFA) on all systems
- Role-based access control (RBAC)
- Annual background checks
- Security awareness training
- Vulnerability scanning
- Incident response plan
- Change management process
- Encryption at rest and in transit

2. AVAILABILITY (Optional)

What it covers:

- System uptime and performance
- Disaster recovery
- Business continuity
- Capacity planning

When you need it:

- You have SLA commitments (99.9% uptime)
- Customers care about availability
- You're running mission-critical systems

Key Controls:

- High availability architecture (multi-AZ, load balancing)
- Automated backups and tested recovery
- Disaster recovery plan (RTO/RPO defined)
- Performance monitoring and alerting
- Capacity planning process

3. PROCESSING INTEGRITY (Optional)

What it covers:

- Data processing accuracy
- Completeness of processing
- Timeliness
- Authorization

When you need it:

- Financial data processing
- Billing/invoicing systems
- Data transformation pipelines

Key Controls:

- Input validation and error handling
- Reconciliation processes
- Data integrity checks
- Audit trails for all transactions

4. CONFIDENTIALITY (Optional)

What it covers:

- Protection of confidential information
- Encryption
- Data classification
- NDA compliance

When you need it:

- Handling proprietary customer data
- IP protection requirements
- Contractual confidentiality obligations

Key Controls:

- Data classification scheme
- Encryption for confidential data
- NDA tracking and enforcement
- Secure data disposal procedures

5. PRIVACY (Optional - Rarely Needed for SaaS)

What it covers:

- Personal information handling (GDPR-like)
- Consent management
- Data subject rights
- Privacy notices

When you need it:

- Explicitly selling "privacy compliance"
- Heavy consumer data processing
- GDPR/CCPA compliance needs

Reality Check: Most SaaS companies only need Security (mandatory). Add Availability if you have SLA commitments. Skip Privacy unless explicitly required.

The Common Criteria (CC) - Your Foundation

The Common Criteria (CC1-CC9) are the foundation. Every SOC 2 audit includes these. Master these, and you're 70% done.

CC1: Control Environment

What auditors look for:

- Documented organizational structure
- Board oversight of security
- Code of conduct
- Performance evaluations tied to security
- Disciplinary actions for violations

Implementation (1 week):

1. Create org chart showing security reporting lines
2. Document board/leadership review of security (quarterly)
3. Add security responsibilities to job descriptions
4. Create security code of conduct (sign annually)
5. Document at least one security-related disciplinary action

CC2: Communication & Information

What auditors look for:

- Security policies documented and communicated
- Channels for reporting security issues
- Internal communication about security changes

Implementation (1 week):

1. Publish security policies to company wiki/intranet
2. Set up security@company.com for reporting
3. Slack channel for security announcements
4. Documented process for policy updates

CC3: Risk Assessment

What auditors look for:

- Annual risk assessment
- Identified threats and vulnerabilities
- Risk treatment decisions
- Fraud risk considerations

Implementation (2 weeks):

1. Conduct annual risk assessment workshop
2. Use framework: NIST, ISO 27005, or custom
3. Document 15-20 key risks
4. For each risk: likelihood, impact, mitigation
5. Get leadership approval

Sample Risk Assessment Template:

```
Risk ID: R-001
Risk: Unauthorized access to production database
Threat: External attacker, insider threat
Vulnerability: Weak authentication, over-privileged accounts
Likelihood: Medium
Impact: High
Mitigation: Implement MFA, RBAC, audit logs
Owner: CTO
Review Date: Q1 2026
```

CC4: Monitoring Activities

What auditors look for:

- Security monitoring in place
- Log aggregation and review
- Alerting on security events
- Regular control testing

Implementation (2 weeks):

1. Deploy SIEM or log aggregation (Datadog, Splunk, ELK)
2. Set up alerts for: failed logins, privilege escalations, config changes
3. Weekly log review process
4. Quarterly internal audit/control testing

CC5: Control Activities

What auditors look for:

- Preventive controls (MFA, encryption)
- Detective controls (monitoring, alerts)
- Access controls implementation
- Segregation of duties

Implementation (3 weeks):

1. Enforce MFA on all systems (Google Workspace, AWS, GitHub, etc.)
2. Implement RBAC (least privilege)
3. Separate production access from dev
4. Document who can do what (access matrix)

CC6: Logical and Physical Access Controls

What auditors look for:

- Authentication mechanisms
- Authorization frameworks
- Physical security (if you have offices/servers)
- Encryption

Implementation (2 weeks):

1. MFA everywhere (already covered in CC5)
2. Document office access controls (badge system, visitor logs)
3. If cloud-only: document datacenter SOC 2 (AWS, GCP, Azure inherit)
4. Encryption at rest (database, S3 buckets)
5. Encryption in transit (TLS 1.2+ everywhere)

CC7: System Operations

What auditors look for:

- Backup and recovery procedures
- Capacity planning
- Vulnerability management
- Malware protection

Implementation (3 weeks):

1. Automated daily backups (tested quarterly)
2. Vulnerability scanning (weekly with Qualys, Tenable, etc.)
3. Patch management process (critical patches within 30 days)
4. Endpoint protection (CrowdStrike, SentinelOne, etc.)
5. Capacity monitoring (CloudWatch, Datadog)

CC8: Change Management

What auditors look for:

- Change approval process
- Testing before production deployment
- Rollback procedures
- Documentation of changes

Implementation (2 weeks):

1. All production changes require PR review
2. Staging environment testing mandatory
3. Change log (Git commits work for this)
4. Emergency change procedure documented

CC9: Risk Mitigation

What auditors look for:

- Incident response plan
- Incident tracking
- Post-incident reviews
- Business continuity plan

Implementation (3 weeks):

1. Create incident response plan (detection, containment, eradication, recovery)
2. Set up incident tracking (Jira, PagerDuty, etc.)
3. Document at least one incident (even minor) with root cause analysis
4. Business continuity plan (what if AWS goes down?)
5. Disaster recovery runbook

CHAPTER 3: TYPE I VS TYPE II - WHAT YOU ACTUALLY NEED

Type I: Point-in-Time Snapshot

What it is: Auditor examines your controls on a **specific date**. "As of December 31, 2025, controls were designed appropriately."

Audit Period: 1 day (but 4-6 weeks of prep)

What auditor checks:

- Are controls documented?
- Do they exist?
- Are they designed properly?
- **NOT:** Are they working consistently?

Use Cases:

- First-time SOC 2 (everyone starts here)
- Customers just need "any SOC 2 report"
- You're in a hurry (8-12 week timeline)
- Budget-conscious (₹6-8L vs ₹10-12L)

Limitations:

- Many enterprises don't accept Type I anymore
- No proof of operational effectiveness
- Often seen as "checkbox compliance"

Type II: Operating Effectiveness Over Time

What it is: Auditor examines your controls over a **6-12 month period**. "From January 1 - December 31, 2025, controls operated effectively."

Audit Period: 6-12 months (your choice)

What auditor checks:

- Everything from Type I, PLUS:
- Were controls executed consistently?
- Evidence of repeated application
- Exceptions and how they were handled

Use Cases:

- Enterprise customers require it (Fortune 1000)
- Second SOC 2 audit (upgrade from Type I)
- SaaS with mature security program
- Preparing for IPO/acquisition

Sample Size Requirements: For Type II, auditors test multiple instances:

Control Frequency	Auditor Sample Size
Annual	1 instance
Quarterly	All 4 instances
Monthly	2-3 instances
Weekly	4-8 instances
Daily	25-40 instances

Example:

- Access reviews (quarterly): Auditor checks all 4 quarters
- Vulnerability scans (weekly): Auditor samples 8 random weeks
- Backup logs (daily): Auditor samples 30-40 random days

The Transition Strategy

Recommended Path:

1. **Months 1-3:** Get Type I certified (fast)
2. **Months 4-15:** Maintain controls, collect evidence
3. **Months 16-18:** Get Type II audit

Why this works:

- Type I unblocks enterprise deals immediately
- Gives you 12 months to mature controls
- Type II audit period can overlap with later months of Type I
- Smooth transition, no "compliance gap"

Cost Comparison:

Approach	Timeline	Total Cost
Type I only	8-12 weeks	₹6-8L
Type I → Type II	18 months	₹12-15L
Type II from scratch	12-18 months	₹10-14L

Pro Tip: Most auditors offer "combo pricing" if you commit to Type II upfront but complete Type I first. Saves ₹2-3L compared to separate engagements.

PART 2: IMPLEMENTATION

CHAPTER 4: THE 8-12 WEEK IMPLEMENTATION ROADMAP

This is the fast-track roadmap used by 200+ startups we've certified. It's aggressive but achievable if you have:

- Leadership commitment (5-10 hours/week from CTO/CEO)
- Dedicated project manager (20-30 hours/week)
- Engineering cooperation (2-4 hours/week from team)
- Budget approved (₹6-10L total)

Week 1: Kickoff & Scoping

Deliverables:

- ☐ Select auditor (get 3 quotes, compare)
- ☐ Define scope: which systems, which TSC categories
- ☐ Assign internal project owner (usually CTO or VP Eng)
- ☐ Create project timeline with milestones
- ☐ Get budget approved

Time Investment:

- Leadership: 8 hours
- Project Manager: 20 hours

Week 2-3: Gap Analysis & Planning

Deliverables:

- ☐ Complete gap assessment against all 64 TSC criteria
- ☐ Identify what exists vs what needs to be built
- ☐ Prioritize gaps by risk and effort
- ☐ Create detailed implementation plan
- ☐ Assign owners for each control area

Sample Gap Analysis Output:

```
CC6.1 - Logical Access: 60% complete
✓ Have: MFA on Google Workspace
✗ Missing: MFA on AWS, GitHub, Slack
✗ Missing: RBAC documentation
Action: Enable MFA everywhere, document access matrix
Owner: CTO | Due: Week 4
```

Time Investment:

- Leadership: 6 hours
- Project Manager: 30 hours
- Engineering: 4 hours

Week 4-5: Policy Documentation

Deliverables:

- ☐ Information Security Policy (master policy)
- ☐ Access Control Policy
- ☐ Acceptable Use Policy
- ☐ Data Classification Policy
- ☐ Incident Response Plan
- ☐ Business Continuity Plan
- ☐ Change Management Procedure
- ☐ Risk Assessment Procedure
- ☐ Vendor Management Policy

Pro Tip: Don't write from scratch. Use templates (provided in Appendix C), customize for your business, get leadership approval.

Time Investment:

- Project Manager: 40 hours
- Leadership review: 4 hours

Week 6-7: Control Implementation

Deliverables:

- ☐ Enable MFA on all systems (Google, AWS, GitHub, etc.)
- ☐ Implement RBAC (document who has access to what)
- ☐ Deploy vulnerability scanning
- ☐ Set up log aggregation/SIEM
- ☐ Configure backups (if not already automated)
- ☐ Deploy endpoint protection
- ☐ Set up security monitoring alerts

Engineering Priorities:

1. **Day 1:** MFA everywhere (highest impact, easiest win)
2. **Day 3:** Deploy vuln scanner (Qualys/Tenable)
3. **Day 5:** SIEM setup (Datadog/Splunk/ELK)
4. **Day 7:** Backup automation + test restore
5. **Day 10:** Endpoint protection rollout

Time Investment:

- Engineering: 60-80 hours
- Project Manager: 20 hours

Week 8-9: Evidence Collection

Deliverables:

- ☐ Screenshot MFA configurations
- ☐ Export access control matrices
- ☐ Collect vulnerability scan reports
- ☐ Gather log review evidence
- ☐ Document incident responses (even if minor)
- ☐ Backup/restore test results
- ☐ Security training completion records
- ☐ Background check confirmations
- ☐ Vendor SOC 2 reports collected

Evidence Checklist: For each control, you need 2-3 pieces of evidence:

- **Screenshot** (config, setting)
- **Report** (scan results, logs)
- **Attestation** (signed policy, training completion)

Time Investment:

- Project Manager: 50 hours
- Engineering: 10 hours

Week 10: Internal Audit / Readiness Review

Deliverables:

- [ ] Internal control testing (sample your own evidence)
- [ ] Identify gaps/exceptions
- [ ] Remediate critical findings
- [ ] Final documentation review
- [ ] Stakeholder readiness meeting

Mock Audit Questions:

- Can you show me MFA is enforced? (demo)
- Show me last quarter's access review
- Walk me through an incident response
- Where are backups? Show me a restore test

Time Investment:

- Project Manager: 30 hours
- Leadership: 4 hours
- Engineering: 6 hours

Week 11-12: Formal Audit

Deliverables:

- [ ] Submit evidence package to auditor
- [ ] Auditor fieldwork (interviews, testing)
- [ ] Respond to auditor questions/requests
- [ ] Remediate any findings
- [ ] Receive draft report
- [ ] Review and approve final report

What Happens:

- **Day 1:** Auditor kickoff, requests evidence list
- **Days 2-5:** You upload evidence to auditor portal
- **Days 6-8:** Auditor testing and interviews
- **Days 9-10:** Auditor questions (you respond in 24-48 hours)
- **Day 11:** Draft report issued
- **Day 12:** Final report approved

Time Investment:

- Project Manager: 40 hours
- Leadership interviews: 2 hours
- Engineering interviews: 3 hours

CHAPTER 5: SCOPING YOUR SOC 2 AUDIT

What Gets Audited?

You don't audit your entire company. You audit the **systems and processes that affect customer data security**.

In Scope (Always):

- Production infrastructure (AWS, GCP, Azure)
- Application code (frontend, backend, APIs)
- Databases storing customer data
- Access management systems (Google Workspace, Okta, etc.)
- People with access to production
- Third-party vendors processing customer data

Out of Scope (Usually):

- Internal tools not touching customer data
- Marketing website (unless it has user accounts)
- HR systems
- Finance systems (unless processing payments)
- Employees without production access

The Scoping Document

Your auditor will create a "Description of System" document that defines:

1. **System Description:** What does your product do?
2. **Infrastructure:** Where is it hosted?
3. **Boundaries:** What's in vs out of scope?
4. **Third Parties:** Who do you rely on?
5. **Trust Services Criteria:** Which categories (Security + optional)
6. **Type:** Type I or Type II?

7. **Period:** As of what date? Or from/to dates?

Sample Scoping Statement:

```
 System: SaaSCo Project Management Platform
Description: Cloud-based project management SaaS for enterprise teams
Infrastructure: AWS (us-east-1, us-west-2)
In Scope:
  - Production web application (React + Node.js)
  - PostgreSQL database (RDS)
  - File storage (S3)
  - API gateway
  - CI/CD pipeline (GitHub Actions)
  - Google Workspace (email, docs)
  - AWS IAM + CloudTrail
  - All employees with production access (12 people)
Out of Scope:
  - Marketing website (WordPress on separate AWS account)
  - Internal Slack workspace
  - Financial systems (QuickBooks)
Trust Service Criteria: Security + Availability
Type: SOC 2 Type I
Report Date: December 31, 2025
```

Common Scoping Mistakes

❌ Mistake 1: Scoping Too Broad *"Let's audit everything to be safe!"*

Problem: Increases audit cost by 2-3x, extends timeline, more controls to maintain.

Fix: Start narrow. You can always expand scope in future audits.

❌ Mistake 2: Forgetting Third-Party Dependencies

"We didn't think AWS counted as in-scope."

Problem: Auditor will ask for AWS SOC 2 report (it's a subservice organization).

Fix: List all vendors that touch customer data. Get their SOC 2/ISO 27001 reports.

❌ Mistake 3: Wrong TSC Selection

"We added Privacy because it sounds important."

Problem: Privacy criteria require massive documentation (GDPR-level). Only add if contractually required.

Fix: Start with Security only. Add Availability if you have SLA commitments. Skip the rest unless customer demands it.

The Vendor Inventory

You'll need SOC 2 (or ISO 27001) reports from ALL vendors that:

- Process, store, or transmit customer data
- Have access to your production systems
- Are critical to service delivery

Common Vendors:

Vendor	Service	Report Type	Where to Get It
AWS	Infrastructure	SOC 2 Type II	AWS Artifact (free)
Google Cloud	Infrastructure	SOC 2 Type II	Compliance Reports Manager
GitHub	Code repository	SOC 2 Type II	GitHub settings → Security
Datadog	Monitoring	SOC 2 Type II	Contact support

Vendor	Service	Report Type	Where to Get It
SendGrid	Email delivery	SOC 2 Type II	Trust center
Stripe	Payments	PCI DSS + SOC 2	Stripe docs

If vendor doesn't have SOC 2:

- Accept ISO 27001 (usually equivalent)
- If no cert: require vendor security questionnaire
- If critical vendor: this might block your audit

CHAPTER 6: COMMON CRITERIA (CC1-CC9) - DETAILED IMPLEMENTATION

We'll now go deeper into each Common Criteria with exact implementation steps.

CC1: COSO Control Environment

What COSO Means: Committee of Sponsoring Organizations framework. Fancy term for "Does your company take security seriously at the leadership level?"

17 Points of Focus:

CC1.1: Demonstrates commitment to integrity and ethical values

Implementation:

1. Create Code of Conduct (2 pages max)
    - Expected behaviors
    - Conflicts of interest policy
    - Reporting violations
2. Require annual signature from all employees
3. Document in employee handbook
4. Board/leadership reviews annually

Evidence:

- Signed Code of Conduct (all employees)
- Board meeting minutes showing annual review
- Employee handbook excerpt

CC1.2: Board independence and oversight

Implementation:

1. Document board structure (even if it's just founders + advisors)
2. Quarterly board meeting covering security/risk
3. Meeting minutes documenting security discussions
4. At least one board member with security expertise (or advisor)

Evidence:

- Org chart showing board structure
- Q1, Q2, Q3, Q4 board minutes (security agenda item)
- Board member bios showing security experience

CC1.3: Management establishes structures, reporting lines, and authorities

Implementation:

1. Create org chart showing security reporting
2. Document who reports to whom
3. Define security responsibilities in job descriptions
4. Assign control owners (who's responsible for what)

Evidence:

- Organizational chart
- Job descriptions with security duties
- RACI matrix (Responsible, Accountable, Consulted, Informed)

CC1.4: Demonstrates commitment to competence

Implementation:

1. Security training program (annual minimum)
2. Role-specific training (developers → secure coding, admins → system hardening)
3. Training completion tracking
4. Skills assessment for security roles

Evidence:

- Security awareness training platform (KnowBe4, SANS, etc.)
- Training completion reports
- Certificates of completion
- Job descriptions with required competencies

CC1.5: Enforces accountability

Implementation:

1. Document at least one disciplinary action for security violation
2. Performance reviews include security metrics
3. Termination procedures include access revocation
4. Exit interview process

Evidence:

- HR documentation of policy violation + consequence
- Performance review template with security criteria
- Offboarding checklist showing access revocation

CC6: LOGICAL AND PHYSICAL ACCESS CONTROLS (Critical!)

This is where 80% of audit effort goes. Get this right, and you're golden.

CC6.1: Creates and maintains logical access

MFA Everywhere: ✓ Google Workspace (admin console → Security → 2SV enforcement) ✓ AWS (IAM → Users → Security credentials → MFA device) ✓ GitHub (Settings → Password and authentication → 2FA requirement) ✓ Slack (Workspace settings → Authentication → Require 2FA) ✓ Any tool with production access

Evidence:

- Screenshots of MFA enforcement settings
- Audit logs showing MFA usage
- List of all systems + MFA status

RBAC (Role-Based Access Control): Create an access matrix:

```
| Role | AWS Prod | AWS Dev | GitHub | Database | Customer Data |
|------|----------|---------|--------|----------|---------------|
| CEO | No | No | No | No | No |
| CTO | Admin | Admin | Admin | Read | Read |
| Lead Dev | Limited | Admin | Write | Read | No |
| Developer | No | Write | Write | No | No |
| Support | No | No | Read | No | Read-only |
```

Least Privilege Principle:

- Default: No access
- Grant only what's needed for job function
- Review quarterly
- Revoke immediately upon role change/termination

Evidence:

- Access matrix spreadsheet
- AWS IAM policies screenshot
- GitHub team permissions
- Quarterly access review results

CC6.2: Authenticates users

Implementation:

1. Password requirements (12+ chars, complexity, no reuse)
2. MFA required (already covered above)
3. SSO where possible (Google Workspace SSO → all apps)
4. No shared accounts

Evidence:

- Password policy configuration screenshots
- SSO integration list
- Audit log showing individual user attribution

CC6.3: Authorization

Implementation:

1. Role definitions (what each role can do)
2. Approval workflow for elevated access
3. Just-in-time access for production (temporary, logged)
4. Segregation of duties (no one person can deploy AND approve)

Evidence:

- Role definition document
- Access request/approval tickets (Jira, ServiceNow)
- Audit logs showing approval chains

CC6.6: Physical access

If you have offices:

- Badge access system
- Visitor log
- Server room restrictions
- Camera surveillance

If fully remote (most SaaS):

- Document reliance on cloud provider physical security
- Inherit AWS/GCP/Azure SOC 2 for physical controls
- Employee device security (see CC6.7)

Evidence:

- Cloud provider SOC 2 report (Section on Physical Security)
- Office badge logs (if applicable)
- Visitor sign-in sheet

CC6.7: Restricts access to assets

Endpoint Security:

1. All laptops encrypted (BitLocker, FileVault)
2. Endpoint protection deployed (CrowdStrike, SentinelOne)
3. Remote wipe capability (Google MDM, Jamf)
4. Automatic screen lock (5 min timeout)
5. Patch management (OS updates within 30 days)

Evidence:

- MDM screenshot showing encryption status
- Endpoint protection dashboard
- Patch management report

CC6.8: Data encryption

At Rest:

- Database encryption (RDS encryption enabled)
- S3 bucket encryption (default encryption on)
- Disk encryption (EBS volumes encrypted)

In Transit:

- TLS 1.2+ for all web traffic
- VPN for remote access
- API calls over HTTPS only

Evidence:

- AWS RDS encryption screenshot
- S3 bucket policy showing encryption requirement
- SSL Labs report (A+ rating)
- Network diagram showing encryption points

CC7: SYSTEM OPERATIONS

CC7.1: Backup and recovery

Implementation:

1. Automated daily backups (RDS automated backups, S3 versioning)
2. Test restore quarterly (actually restore from backup)
3. Document RTO (Recovery Time Objective): 4 hours
4. Document RPO (Recovery Point Objective): 24 hours

5. Off-site backup storage (different AWS region)

Evidence:

- Backup configuration screenshots
- Backup success logs (30 days)
- Restore test results (with timestamps, success confirmation)
- BCP document with RTO/RPO

CC7.2: Vulnerability management

Implementation:

1. Weekly vulnerability scans (Qualys, Tenable, AWS Inspector)
2. Critical vulns patched within 30 days
3. High vulns patched within 60 days
4. Exception process for unpatchable vulns (document compensating controls)

Evidence:

- Vulnerability scan reports (showing scan frequency)
- Patch management tracker (showing remediation timelines)
- Exceptions register with justifications

CC7.3: Security monitoring

Implementation:

1. SIEM or log aggregation (Datadog, Splunk, CloudWatch)
2. Alerts configured for:
    - Failed login attempts (5+ failures)
    - Privilege escalation
    - Configuration changes
    - Unauthorized access attempts
3. Weekly log review
4. Annual log review by leadership

Evidence:

- SIEM alert configuration screenshots
- Log review reports (weekly)
- Sample alerts + response actions

CC8: CHANGE MANAGEMENT

CC8.1: System changes authorized

Implementation:

1. All production changes require approval
2. Change request process (GitHub PR, Jira ticket, etc.)
3. Peer code review mandatory
4. Separation of duties (developer ≠ deployer)

Evidence:

- GitHub branch protection rules
- Pull request approval logs
- Change management policy
- Sample PRs showing reviews

CC8.2: System changes tested

Implementation:

1. Staging environment (mirror of production)
2. Automated testing (unit tests, integration tests)
3. Manual QA before deployment
4. Rollback plan for every change

Evidence:

- CI/CD pipeline configuration (GitHub Actions, Jenkins)
- Test results (passing tests before merge)
- Staging environment architecture diagram
- Rollback procedure document

CC9: RISK MITIGATION

CC9.1: Incident response

Implementation:

1. Incident Response Plan document (10-15 pages)
    - Roles and responsibilities
    - Incident classification (P1-P4)
    - Escalation procedures
    - Communication templates
2. Incident tracking system (Jira, PagerDuty, ServiceNow)
3. Document at least 1 incident (even minor)
4. Post-incident review (root cause analysis)

Evidence:

- Incident Response Plan (signed by leadership)
- Incident tickets (showing detection, response, resolution)
- Post-incident review reports

Sample Incident:

```
 Incident ID: INC-2025-001
Date: January 15, 2025
Severity: P3 (Low)
Description: Unauthorized login attempt from unknown IP
Detection: CloudTrail alert triggered
Response: Account locked, password reset forced, user notified
Resolution: Confirmed legitimate user traveling, re-enabled after MFA verification
RCA: User's password leaked in third-party breach (found on Have I Been Pwned)
Remediation: Forced password reset for all users, implemented password breach detection
```

CC9.2: Business continuity and disaster recovery

Implementation:

1. Business Continuity Plan (BCP)
    - Critical systems identified
    - RTO/RPO defined
    - Recovery procedures
    - Communication plan
2. Disaster Recovery Plan (DRP)
    - Infrastructure failover procedures
    - Data recovery steps
    - Team contact list
3. Annual test (simulate outage, execute recovery)

Evidence:

- BCP/DRP documents
- Annual test results (tabletop exercise or actual test)
- Leadership approval signatures

CHAPTER 10: EVIDENCE COLLECTION - WHAT AUDITORS ACTUALLY WANT

The Evidence Package

For each control, you need 2-3 pieces of evidence. Think of it as "proof" that the control exists and operates.

Three Types of Evidence:

1. **Design Evidence** (Does it exist?)
    - Policy documents
    - Screenshots of configurations
    - System architecture diagrams
2. **Operating Evidence** (Does it work?)
    - Logs, reports, scan results
    - Tickets, emails, meeting minutes
    - Training completion records
3. **Attestation Evidence** (Did someone verify it?)
    - Signed policies
    - Approval emails
    - Management assertions

Evidence Checklist by Control

For MFA (CC6.1):

- Screenshot of Google Workspace MFA enforcement setting
- Screenshot of AWS IAM showing MFA devices assigned
- Audit log showing MFA successful authentications (sample 5 users)

For Access Reviews (CC6.1):

- Q1, Q2, Q3, Q4 access review spreadsheets
- Email from CTO approving access matrix
- Evidence of access revoked (terminated employee or role change)

For Vulnerability Scanning (CC7.2):

- 4 weekly scan reports showing:
  - Scan date
  - Systems scanned
  - Vulnerabilities found (count by severity)
- Remediation tracker showing critical vulns patched <30 days
- Screenshot of scan configuration (weekly schedule)

For Backup Testing (CC7.1):

- Quarterly restore test results (Q1, Q2, Q3, Q4)
- Each test shows:
  - Date of restore test
  - Backup source date
  - Restore target
  - Success/failure status
  - Sign-off from engineer

For Security Training (CC1.4):

- Training completion report (all employees, >90% completion)
- Sample training certificate
- Training content outline (showing topics covered)

Evidence Organization

Create a folder structure:

```
SOC2-Evidence/
├── CC1-Control-Environment/
│   ├── CC1.1-Code-of-Conduct.pdf
│   ├── CC1.2-Board-Minutes-Q1.pdf
│   ├── CC1.2-Board-Minutes-Q2.pdf
│   ├── CC1.3-Org-Chart.png
│   └── CC1.4-Training-Report.xlsx
├── CC6-Access-Controls/
│   ├── CC6.1-MFA-Google-Workspace.png
│   ├── CC6.1-MFA-AWS.png
│   ├── CC6.1-Access-Matrix.xlsx
│   ├── CC6.1-Q1-Access-Review.pdf
│   └── ...
├── CC7-System-Operations/
│   ├── CC7.1-Backup-Config.png
│   ├── CC7.1-Q1-Restore-Test.pdf
│   ├── CC7.2-Vuln-Scan-Report-Week1.pdf
│   └── ...
└── CC8-Change-Management/
    ├── CC8.1-GitHub-Branch-Protection.png
    ├── CC8.2-Sample-PR-with-Approvals.pdf
    └── ...
```

Common Evidence Mistakes

 Mistake: Undated screenshots *Auditor can't verify when it was taken*

Fix: Include timestamp in screenshot or filename with date

 Mistake: Generic vendor reports *"Here's the AWS security whitepaper"*

Fix: Provide AWS SOC 2 report specific to your account/region

❌ Mistake: Missing samples for recurring controls *Only provided one month of vuln scans (need 4+)*

Fix: Check auditor sampling requirements before collecting evidence

---

CHAPTER 18: COST BREAKDOWN & ROI ANALYSIS

Total Cost of SOC 2 (Type I)

Auditor Fees:

- Small company (<20 employees, simple stack): ₹3-5L
- Medium company (20-100 employees, moderate complexity): ₹5-8L
- Large company (100+ employees, complex): ₹8-12L

Consultant/Implementation Fees (if used):

- DIY Platform (Vanta, Drata, Secureframe): ₹2-3L/year
- Consultant (part-time support): ₹3-5L
- Consultant (full implementation): ₹5-8L
- Lead Auditor (white glove service): ₹6-10L all-in

Tooling Costs (Annual):

- SIEM/Log Management (Datadog, Splunk): ₹1-3L
- Vulnerability Scanner (Qualys, Tenable): ₹1-2L
- Endpoint Protection (CrowdStrike, SentinelOne): ₹50K-1L
- Training Platform (KnowBe4, SANS): ₹30K-80K
- Total Tooling: ₹2.8-6.8L/year

Internal Labor Costs:

- Project Manager (200-300 hours @ ₹2K/hour): ₹4-6L
- Engineering (80-120 hours @ ₹3K/hour): ₹2.4-3.6L
- Leadership (20-30 hours @ ₹5K/hour): ₹1-1.5L
- Total Labor: ₹7.4-11.1L

TOTAL COST (Type I, First Year):

- **Low End (DIY):** ₹13L (Auditor ₹3L + Platform ₹2L + Tools ₹3L + Labor ₹5L)
- **Mid Range (Consultant):** ₹18L (Auditor ₹6L + Consultant ₹5L + Tools ₹4L + Labor ₹3L)
- **High End (Lead Auditor):** ₹20L (All-in ₹10L + Tools ₹5L + Labor ₹5L)

Ongoing Costs (Years 2+):

- Annual surveillance audit: ₹2-4L
- Tooling: ₹3-5L
- Maintenance labor: ₹2-3L
- **Total Annual:** ₹7-12L

ROI Calculation

Revenue Impact:

Scenario: 50-person SaaS company, ₹2Cr ARR, targeting enterprise customers

Without SOC 2:

- Enterprise deals lost: 3-5 per year
- Average deal size: ₹40L ARR
- Lost revenue: ₹1.2-2Cr/year
- Win rate: 15% (enterprise)

With SOC 2:

- Enterprise deals won: +3 per year (conservative)
- Additional revenue: ₹1.2Cr/year
- Win rate increase: 15% → 35%
- Deal cycle reduction: -2 months

ROI:

```
 Investment: ₹20L (Year 1)
Revenue Gain: ₹1.2Cr (Year 1, 3 deals @ ₹40L each)
ROI: 600% (₹1.2Cr / ₹20L = 6x)
Payback Period: 2 months (₹20L / ₹60L per deal = 0.33 deals)
```

Non-Revenue Benefits:

- Reduced security questionnaire time: 10-20 hours/month saved
- Faster procurement cycles: -30-60 days
- Increased customer trust: harder to quantify

- Foundation for ISO 27001, HIPAA, etc.: ₹3-5L saved on next cert
- Acquisition readiness: critical for M&A due diligence

Build vs Buy Decision

Option 1: DIY with Platform

- Cost: ₹13-15L
- Timeline: 12-18 months
- Success Rate: 60-70%
- Best For: In-house security expertise, tight budget

Option 2: Consultant

- Cost: ₹18-22L
- Timeline: 6-9 months
- Success Rate: 85-90%
- Best For: Some internal capability, need guidance

Option 3: Lead Auditor (Full Service)

- Cost: ₹20-25L
- Timeline: 8-12 weeks
- Success Rate: 100%
- Best For: Speed critical, first-time pass essential, no internal security team

Recommendation: If you're reading this guide and implementing yourself: Go with Option 1 (DIY + Platform) If you need this done FAST (enterprise deal pending): Go with Option 3 (Lead Auditor) If you're somewhere in between: Option 2 (Consultant)

APPENDICES

APPENDIX A: COMPLETE TSC CHECKLIST (All 64 Criteria)

Use this checklist to track your progress:

COMMON CRITERIA (CC)

CC1: Control Environment

- ☐ CC1.1: Integrity and ethical values
- ☐ CC1.2: Board independence and oversight
- ☐ CC1.3: Management structures and reporting
- ☐ CC1.4: Commitment to competence
- ☐ CC1.5: Accountability enforcement

CC2: Communication & Information

- ☐ CC2.1: Internal communication
- ☐ CC2.2: External communication
- ☐ CC2.3: Quality information

CC3: Risk Assessment

- ☐ CC3.1: Risk identification
- ☐ CC3.2: Risk analysis
- ☐ CC3.3: Fraud risk assessment
- ☐ CC3.4: Significant changes identified

CC4: Monitoring

- ☐ CC4.1: Ongoing monitoring
- ☐ CC4.2: Independent evaluations

CC5: Control Activities

- ☐ CC5.1: Selection and development of controls
- ☐ CC5.2: Technology controls
- ☐ CC5.3: Policies and procedures deployment

CC6: Logical & Physical Access

- ☐ CC6.1: Logical access created/maintained
- ☐ CC6.2: User authentication
- ☐ CC6.3: Authorization
- ☐ CC6.4: Network access restriction
- ☐ CC6.5: Access removal

- [ ] CC6.6: Physical access
- [ ] CC6.7: Asset restrictions
- [ ] CC6.8: Data transmission encryption

CC7: System Operations

- [ ] CC7.1: Backup and recovery
- [ ] CC7.2: Vulnerability identification
- [ ] CC7.3: Security monitoring
- [ ] CC7.4: Environmental protection
- [ ] CC7.5: Anti-malware protection

CC8: Change Management

- [ ] CC8.1: System changes authorized
- [ ] CC8.2: System changes tested

CC9: Risk Mitigation

- [ ] CC9.1: Incident response
- [ ] CC9.2: Business continuity

AVAILABILITY CRITERIA (A) - Optional

- [ ] A1.1: Availability commitments documented
- [ ] A1.2: Availability monitoring
- [ ] A1.3: Incident response for availability

CONFIDENTIALITY CRITERIA (C) - Optional

- [ ] C1.1: Confidentiality commitments
- [ ] C1.2: Confidential information identification

PROCESSING INTEGRITY CRITERIA (PI) - Optional

- [ ] PI1.1: Processing commitments
- [ ] PI1.2: Processing authorization
- [ ] PI1.3: Completeness and accuracy
- [ ] PI1.4: Error detection and correction
- [ ] PI1.5: Processing monitoring

PRIVACY CRITERIA (P) - Rarely Needed

- [ ] P1.1: Notice and communication
- [ ] P2.1: Choice and consent
- [ ] P3.1: Collection
- [ ] P4.1: Use, retention, and disposal
- [ ] P5.1: Access
- [ ] P6.1: Disclosure to third parties
- [ ] P7.1: Quality
- [ ] P8.1: Monitoring and enforcement

APPENDIX B: EVIDENCE COLLECTION TEMPLATES

Template 1: Access Review

```
 ACCESS REVIEW - Q1 2026
Review Date: March 31, 2026
Reviewed By: CTO
Approved By: CEO

| User | Role | AWS | GitHub | Database | Action |
|------|------|-----|--------|----------|--------|
| john@co.com | CTO | Admin | Admin | Admin | Keep |
| jane@co.com | Lead Dev | Dev | Write | Read | Keep |
| bob@co.com | Former Dev | NONE | NONE | NONE | Revoked 3/15 |
| alice@co.com | Support | No | Read | No | Keep |

Exceptions: None
Changes: Bob Smith terminated 3/15/26, all access revoked same day
Next Review: June 30, 2026
```

Template 2: Vulnerability Scan Report Summary

```
 VULNERABILITY SCAN SUMMARY
Scan Date: January 7, 2026
Scanner: Qualys Cloud Platform
Scope: All production systems (12 hosts)

| Severity | Count | Status |
|----------|-------|--------|
| Critical | 2 | Remediated within 7 days |
| High | 8 | Remediated within 25 days |
| Medium | 34 | Scheduled for Q2 2026 |
| Low | 127 | Accepted risk |

Critical Findings:
1. CVE-2025-1234: OpenSSL vulnerability
   - Affected: Web server (prod-web-01)
   - Remediated: January 9, 2026 (2 days)
   - Evidence: Patch applied, rescan clean

2. CVE-2025-5678: PostgreSQL RCE
   - Affected: Database server (prod-db-01)
   - Remediated: January 14, 2026 (7 days)
   - Evidence: Version upgrade to 15.2

Reviewed by: Security Team
Approved by: CTO
```

Template 3: Backup Restore Test

```
 BACKUP RESTORE TEST REPORT
Test Date: March 15, 2026
Test Conducted By: DevOps Engineer
Reviewed By: CTO

Objective: Verify production database can be restored from automated backup

Backup Details:
- Source: RDS Automated Backup
- Backup Date: March 14, 2026 23:00 UTC
- Backup Size: 45 GB
- Backup Type: Automated snapshot

Restore Process:
1. Created restore instance: test-restore-20260315
2. Initiated restore: 10:00 AM
3. Restore completed: 10:47 AM (47 minutes)
4. Data verification: Checked record counts, sampled 1000 records
5. Application connectivity test: Connected app to restored DB

Results:
✓ Restore successful
✓ Data integrity verified
✓ RTO met: 47 minutes (target: <4 hours)
✓ RPO met: 11 hours (target: <24 hours)

Issues: None
Recommendations: None

Sign-off:
Engineer: [Signature] Date: 3/15/26
CTO: [Signature] Date: 3/15/26
```

Template 4: Incident Report

```
 SECURITY INCIDENT REPORT
Incident ID: INC-2026-003
Date Detected: February 12, 2026 14:23 UTC
Severity: P2 (Medium)
Status: Closed

SUMMARY:
Unusual login activity detected from unfamiliar IP address for user jane@company.com

TIMELINE:
14:23 - CloudTrail alert triggered (5 failed login attempts)
14:25 - Security team notified via PagerDuty
14:30 - Account locked, user contacted
14:45 - User confirmed legitimate (traveling, new location)
15:00 - MFA re-verification completed
15:05 - Account unlocked
15:30 - Post-incident review scheduled

ROOT CAUSE:
User traveling internationally, connecting from hotel WiFi (new IP).
Failed attempts due to forgotten MFA device code, triggered lockout.

IMPACT:
- No unauthorized access
- User productivity loss: 45 minutes
- No customer data affected

REMEDIATION:
- Enhanced user training on MFA backup codes
- Updated incident response playbook
- No system changes required

LESSONS LEARNED:
- Detection systems working as designed
- Response time within SLA (5 minutes)
- Need better communication for travel scenarios

Reported By: Security Engineer
Reviewed By: CTO
Approved By: CEO
Date Closed: February 13, 2026
```

APPENDIX C: SAMPLE POLICIES

Information Security Policy (Master Policy)

```
 INFORMATION SECURITY POLICY
Version: 2.0
Effective Date: January 1, 2026
Review Date: January 1, 2027
Owner: Chief Technology Officer
Approved By: Chief Executive Officer

1. PURPOSE
This policy establishes the framework for protecting [Company Name]'s
information assets and customer data.

2. SCOPE
Applies to all employees, contractors, third parties with access to
company systems or customer data.

3. ROLES & RESPONSIBILITIES
- CEO: Ultimate accountability for security program
- CTO: Day-to-day security oversight
- All Employees: Comply with security policies and report incidents

4. SECURITY PRINCIPLES
- Least privilege access
- Defense in depth
- Encryption by default
- Continuous monitoring
- Regular audits

5. CONTROLS FRAMEWORK
We implement security controls based on:
- AICPA Trust Services Criteria (TSC)
- NIST Cybersecurity Framework
- Industry best practices

6. KEY POLICIES
- Access Control Policy (see ACP-001)
- Data Classification Policy (see DCP-001)
- Incident Response Plan (see IRP-001)
- Business Continuity Plan (see BCP-001)
- Acceptable Use Policy (see AUP-001)

7. COMPLIANCE
- Annual SOC 2 audit
- Quarterly risk assessments
- Monthly security reviews
- Continuous monitoring

8. EXCEPTIONS
Exceptions require CTO approval and documentation of compensating controls.

9. VIOLATIONS
Policy violations may result in disciplinary action up to and including
termination.

10. REVIEW
This policy is reviewed annually and updated as needed.

Approved:
[CEO Signature] Date: _____
[CTO Signature] Date: _____
```

Incident Response Plan (Simplified)

```
 INCIDENT RESPONSE PLAN
Version: 3.0
```

Last Updated: January 2026

1. INCIDENT CLASSIFICATION

P1 - Critical
- Data breach
- Ransomware
- Complete system outage
Response Time: 15 minutes
Escalation: CEO, CTO immediately

P2 - High
- Attempted intrusion
- Malware detected
- Partial outage
Response Time: 1 hour
Escalation: CTO within 2 hours

P3 - Medium
- Suspicious activity
- Policy violation
- Performance degradation
Response Time: 4 hours
Escalation: Security team

P4 - Low
- Failed login attempts
- Minor security event
Response Time: Next business day
Escalation: Log only

2. RESPONSE PHASES

DETECTION
- Automated alerts (SIEM, monitoring)
- User reports (security@company.com)
- Vendor notifications

CONTAINMENT
- Isolate affected systems
- Block malicious IPs
- Disable compromised accounts
- Preserve evidence

ERADICATION
- Remove malware/threat
- Patch vulnerabilities
- Reset credentials
- Validate systems clean

RECOVERY
- Restore from backups if needed
- Return systems to production
- Monitor for recurrence
- Update security controls

LESSONS LEARNED
- Post-incident review (within 5 days)
- Root cause analysis
- Update procedures
- Training updates

3. CONTACT LIST

Security Team:
- CTO: +1-XXX-XXX-XXXX (mobile)

```
- CTO: +91-XXXX-XXXX (primary)
- Lead DevOps: +91-XXXX-XXXX (backup)
- Security Engineer: +91-XXXX-XXXX

External:
- Auditor: auditor@firm.com
- Cyber Insurance: claims@insurer.com
- Legal Counsel: lawyer@lawfirm.com
- Cloud Provider Support: [AWS/GCP support links]

4. COMMUNICATION TEMPLATES
[Include customer notification templates, internal comms, etc.]

5. ANNUAL TESTING
Conduct tabletop exercise annually to test incident response procedures.
```

APPENDIX D: VENDOR SELECTION FRAMEWORK

How to Choose Between DIY, Consultant, or Lead Auditor

Decision Tree:

```
Do you have in-house security expertise?
├─ YES → Do you have 6+ months timeline?
│   ├─ YES → DIY with Platform (₹13-15L, 12-18 months)
│   └─ NO → Lead Auditor (₹20-25L, 8-12 weeks)
└─ NO → Is deal at risk / need speed?
    ├─ YES → Lead Auditor (₹20-25L, 8-12 weeks)
    └─ NO → Consultant (₹18-22L, 6-9 months)
```

Comparison Matrix

Factor	DIY + Platform	Consultant	Lead Auditor
Cost	₹13-15L	₹18-22L	₹20-25L
Timeline	12-18 months	6-9 months	8-12 weeks
Internal Effort	High (300+ hours)	Medium (150 hours)	Low (80 hours)
Success Rate	60-70%	85-90%	100%
Learning	High	Medium	Low
Support	Platform only	Part-time	White glove
Audit Prep	DIY	Consultant helps	Auditor included
Best For	Security team exists	Some capability	Speed critical

Questions to Ask Vendors

For Auditors:

1. How many SOC 2 audits have you conducted? (Want: 100+)
2. What's your first-time pass rate? (Want: 90%+)
3. Do you have SaaS experience? (Want: Yes, 50%+ SaaS clients)
4. What's included in your fee? (Want: Audit + readiness review)
5. Who will be our auditor? (Want: Meet them, check credentials)
6. Timeline from kickoff to report? (Want: 8-12 weeks)
7. References? (Want: 3 recent SaaS clients)

For Consultants:

1. Will you implement or just advise? (Want: Hands-on implementation)

2. What's your SOC 2 success rate? (Want: 95%+)
3. Do you have auditor relationships? (Want: Yes, can recommend)
4. Fixed fee or hourly? (Want: Fixed or capped)
5. What's included? (Want: Policies, evidence collection, audit prep)
6. Post-cert support? (Want: At least 3 months)

For Platforms (Vanta, Drata, etc):

1. What integrations do you support? (Match your stack)
2. Is implementation support included? (Want: Yes, onboarding help)
3. Annual cost? (Want: Under ₹3L)
4. Do customers pass audits? (Want: 95%+ pass rate data)
5. Auditor partnerships? (Want: List of vetted auditors)
6. Ongoing monitoring features? (Want: Continuous compliance)

FINAL THOUGHTS

The Real Value of SOC 2

SOC 2 is not about security theater. Done right, it's a forcing function that makes your company genuinely more secure:

✓ **Forces documentation:** You can't audit what isn't written down ✓ **Creates accountability:** Control owners are clear ✓ **Implements best practices:** CC criteria are industry-standard ✓ **Catches gaps:** Formal audit finds what you missed ✓ **Enables scale:** Processes replace hero culture

What's Next After SOC 2?

Once you have SOC 2, consider:

1. **ISO 27001** (if selling internationally)
    - 80% overlap with SOC 2
    - Additional cost: ₹3-5L
    - Timeline: 3-4 months
    - Required for EU/APAC customers
2. **SOC 2 Type II** (upgrade from Type I)
    - Maintain controls for 6-12 months
    - Collect evidence continuously
    - Additional cost: ₹4-6L
    - Required by most Fortune 500
3. **Industry-Specific Certs:**
    - HIPAA (healthcare): ₹4-7L
    - PCI DSS (payments): ₹8-15L
    - FedRAMP (US government): ₹25-40L

Final Checklist Before You Start

- ☐ Executive buy-in secured (CEO/CTO committed)
- ☐ Budget approved (₹15-25L for first year)
- ☐ Project owner assigned (20-30 hours/week availability)
- ☐ Timeline realistic (8-12 weeks minimum)
- ☐ Customer/deal urgency understood (why now?)
- ☐ Vendor shortlist created (get 3 quotes)
- ☐ Internal kickoff scheduled

Need Help?

If you've read this far and still feel overwhelmed, that's normal. SOC 2 is complex.

Next Steps:

1. Download our SOC 2 Readiness Assessment (10-minute questionnaire)
2. Schedule a free consultation with our Lead Auditors
3. Get a fixed-price quote based on your specific situation

We've certified 500+ companies. We know what works.

Contact:

- Website: www.tcsa.in
- Email: info@tcsa.in
- Phone: +91-XXXX-XXXX

DOCUMENT INFORMATION

Version: 2.0 **Published:** January 2026 **Authors:** Tranquility Cybersecurity & Assurance Lead Auditors

Updates: Check www.tcsa.in/resources for the latest version. We update this guide quarterly based on:

- AICPA Trust Services Criteria changes
- Auditor feedback
- Customer questions
- New best practices

Feedback: Found an error? Have a suggestion? Email guides@tcsa.in

---

This guide is based on real-world experience conducting 500+ SOC 2 audits for SaaS companies ranging from 5-person startups to 500-person scale-ups. Every recommendation has been battle-tested.

Good luck with your SOC 2 journey. You've got this.

— **The Tranquility Team**

END OF GUIDE