SOC 2 Readiness Assessment

Self-Assessment Tool for SOC 2 Type II Certification | Prepared by TCSA

About This Assessment

What's Included: 64 Trust Services Criteria (TSC) controls across 5 trust principles, readiness scoring system, gap analysis, timeline and cost estimator.

Who This Is For: B2B SaaS companies targeting US enterprise customers who require SOC 2 Type II certification.

How to Use: Check each control you have implemented. Calculate your readiness score. Use the gap analysis to prioritize missing controls.

Your SOC 2 Readiness Score

Total Controls Implemented: _____ / 64

Readiness Percentage: _____ %

Interpretation: 0-30% = Not Ready (6-9 months) | 30-60% = Partially Ready (3-6 months) | 60-85% = Mostly Ready (2-3 months) | 85-100% = Ready (1-2 months)

CC — Common Criteria (17 controls)

These controls apply to all SOC 2 audits regardless of which trust principles you choose.

Control	Description	Implemented	Priority	Notes
CC1.1	COSO Principle 1: Demonstrates commitment to integrity and ethical values	□	High	
CC1.2	COSO Principle 2: Board independence and oversight	□	High	
CC1.3	COSO Principle 3: Management establishes structure, authority, and responsibility	□	High	
CC1.4	COSO Principle 4: Demonstrates commitment to competence	□	Medium	
CC1.5	COSO Principle 5: Holds individuals accountable	□	High	
CC2.1	COSO Principle 6: Specifies objectives with sufficient clarity	□	High	
CC2.2	COSO Principle 7: Identifies and analyzes risk	□	High	
CC2.3	COSO Principle 8: Assesses fraud risk	□	High	
CC3.1	COSO Principle 9: Identifies and assesses changes that could impact internal control	□	Medium	
CC3.2	COSO Principle 10: Selects and develops control activities	□	High	
CC3.3	COSO Principle 11: Selects and develops general controls over technology	□	High	
CC3.4	COSO Principle 12: Deploys control activities through policies and procedures	□	High	
CC4.1	COSO Principle 13: Uses relevant information to support internal control	□	Medium	
CC4.2	COSO Principle 14: Communicates internally	□	Medium	
CC5.1	COSO Principle 15: Selects, develops, and performs ongoing evaluations	□	High	
CC5.2	COSO Principle 16: Evaluates and communicates deficiencies	□	High	
CC5.3	COSO Principle 17: Communicates externally	□	Medium	

A — Availability (13 controls)

System is available for operation and use as committed or agreed.

Control	Description	Implemented	Priority	Notes
A1.1	Current processing capacity meets commitments and system requirements	□	High	
A1.2	Environmental protections, software, data backup, and recovery infrastructure in place	□	High	
A1.3	Recovery plan procedures in place and tested	□	High	
CC6.1	Logical and physical access controls restrict access to authorized personnel	□	High	
CC6.2	Prior to issuing credentials, personnel are registered and authorized	□	High	
CC6.3	Credentials are removed when access is no longer required	□	High	
CC6.4	Physical access is restricted to authorized personnel	□	Medium	
CC6.5	Logical access is restricted to authorized personnel	□	High	
CC6.6	Access is reviewed and removed when no longer required	□	High	
CC6.7	Restricted access to data, software, and infrastructure	□	High	
CC6.8	Encryption protects data at rest and in transit	□	High	
CC7.1	Procedures exist to identify, report, and act upon system security breaches	□	High	
CC7.2	System monitoring detects and responds to security incidents	□	High	

C — Confidentiality (11 controls)

Information designated as confidential is protected as committed or agreed.

Control	Description	Implemented	Priority	Notes
C1.1	Confidential information is protected during collection, use, retention, and disposal	□	High	
C1.2	Confidential information is protected during transmission and transport	□	High	
CC6.1	Logical and physical access controls restrict access to confidential information	□	High	
CC6.2	Prior to issuing credentials, personnel are registered and authorized	□	High	
CC6.3	Credentials are removed when access is no longer required	□	High	
CC6.5	Logical access to confidential information is restricted	□	High	
CC6.6	Access to confidential information is reviewed and removed when no longer required	□	High	
CC6.7	Restricted access to confidential data, software, and infrastructure	□	High	
CC6.8	Encryption protects confidential information at rest and in transit	□	High	
CC7.1	Procedures exist to identify, report, and act upon breaches of confidential information	□	High	
CC7.2	System monitoring detects and responds to confidentiality breaches	□	High	

PI — Processing Integrity (12 controls)

System processing is complete, valid, accurate, timely, and authorized.

Control	Description	Implemented	Priority	Notes
PI1.1	Processing inputs are complete, accurate, and timely	□	High	
PI1.2	Processing is complete, accurate, and timely	□	High	
PI1.3	Processing outputs are complete, accurate, and timely	□	High	
PI1.4	Data and output are complete, accurate, and consistent	□	High	
PI1.5	Processing errors are identified and corrected in a timely manner	□	High	
CC6.1	Logical and physical access controls restrict unauthorized processing	□	High	
CC6.2	Prior to issuing credentials, personnel are registered and authorized	□	High	
CC6.3	Credentials are removed when access is no longer required	□	High	
CC6.6	Access is reviewed and removed when no longer required	□	High	
CC7.1	Procedures exist to identify, report, and act upon processing integrity issues	□	High	
CC7.2	System monitoring detects and responds to processing integrity issues	□	High	
CC8.1	Change management procedures ensure processing integrity	□	High	

P — Privacy (11 controls)

Personal information is collected, used, retained, disclosed, and disposed of in conformity with commitments.

Control	Description	Implemented	Priority	Notes
P1.1	Privacy notice provided to data subjects	□	High	
P2.1	Explicit consent obtained for collection, use, and disclosure of personal information	□	High	
P3.1	Personal information collected is limited to what is necessary	□	High	
P3.2	Personal information is used only for purposes identified in privacy notice	□	High	
P4.1	Personal information is retained only as long as necessary	□	High	
P4.2	Personal information is securely disposed of when no longer needed	□	High	
P4.3	Personal information is disclosed only to authorized parties	□	High	
P5.1	Data subjects can access their personal information	□	High	
P5.2	Data subjects can correct inaccurate personal information	□	High	
P6.1	Personal information is protected during collection, use, retention, and disposal	□	High	
P7.1	Quality of personal information is maintained	□	Medium	

Gap Analysis & Implementation Timeline

Priority 1: Critical Gaps (Must-Have for SOC 2)

List all "High" priority controls you haven't implemented:

1. ________________________

2. ________________________

3. ________________________

Estimated Time: 2-4 months | **Estimated Cost:** ₹3-6 lakhs

Priority 2: Important Gaps (Should-Have)

List all "Medium" priority controls you haven't implemented:

1. ________________________

2. ________________________

Estimated Time: 1-2 months | **Estimated Cost:** ₹1-2 lakhs

SOC 2 Timeline Estimator

Readiness Level	Implementation Time	Audit Period	Total Time to Certification
0-30% Ready (Not Ready)	6-9 months	3-6 months	9-15 months
30-60% Ready (Partially Ready)	3-6 months	3-6 months	6-12 months
60-85% Ready (Mostly Ready)	2-3 months	3-6 months	5-9 months
85-100% Ready (Ready)	1-2 months	3-6 months	4-8 months

SOC 2 Cost Estimator (India)

Component	DIY (Platform)	Consulting (TCSA)
Gap Assessment	₹0 (self-service)	₹1-2 lakhs
Implementation (controls, policies, tools)	₹8-12 lakhs/year (platform fees)	₹4-8 lakhs (one-time)
Audit Fees (Type II)	₹6-10 lakhs	₹6-10 lakhs
Annual Surveillance	₹8-12 lakhs/year (platform) + ₹4-6 lakhs (audit)	₹2-3 lakhs (consulting) + ₹4-6 lakhs (audit)
Year 1 Total	**₹14-22 lakhs**	**₹11-20 lakhs**
3-Year Total	**₹38-58 lakhs**	**₹23-38 lakhs**

Next Steps

Based on Your Readiness Score:

If 0-30% Ready: Start with foundational controls (access management, encryption, logging, incident response). Consider hiring a consultant to avoid costly mistakes.

If 30-60% Ready: Focus on closing critical gaps in your weakest trust principle. Document existing controls. Start building evidence for audit.

If 60-85% Ready: Complete remaining controls, conduct internal audit, select auditor, begin 3-6 month observation period.

If 85-100% Ready: Select auditor, begin Type II audit observation period (3-6 months), maintain evidence collection.

Common Mistakes to Avoid:

❌ Starting audit before controls are fully implemented (wastes time and money)

❌ Not collecting evidence during observation period (delays certification)

❌ Choosing wrong trust principles (Security is mandatory; choose A/C/PI/P based on customer needs)

❌ Underestimating documentation requirements (policies, procedures, evidence)

❌ Not involving engineering team early (they implement most controls)

Tranquility Cybersecurity & Assurance (TCSA)

Need help with SOC 2 certification? Contact us at hello@tcsa.in | www.tcsa.in

This assessment covers all 64 Trust Services Criteria for SOC 2 Type II certification