Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

COMPLIANCE FRAMEWORK SERVICE — READINESS TOOL

SOC 2 Readiness Self-Assessment

Common Criteria · Gap Analysis · Readiness Scoring

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

SOC 2 Readiness Self-Assessment

About SOC 2 and This Checklist

SOC 2 (Service Organization Control 2) is an auditing framework developed by the AICPA that evaluates a service organization's controls related to security, availability, processing integrity, confidentiality, and privacy. A SOC 2 Type II report — covering a minimum 6-month audit period — is increasingly required by enterprise clients, government agencies, and cyber insurance carriers from technology and professional services firms.

This self-assessment helps you determine whether your organization is ready to pursue SOC 2 and identifies the gaps that must be closed before engaging an auditor. Engaging an auditor before you are ready is expensive — auditors bill for every gap they find, and remediation during an active audit engagement costs 2–3x more than pre-audit remediation.

SOC 2 at a Glance

Type I — Point-in-time assessment: Are controls designed appropriately? Typically takes 4–8 weeks. Does NOT satisfy most enterprise client requirements.

Type II — Operating effectiveness assessment over a period (minimum 6 months, typically 12): Are controls consistently applied? This is what enterprise clients and insurers typically require.

Which Trust Services Criteria? Security (CC) is mandatory. Availability, Processing Integrity, Confidentiality, and Privacy are optional. Most organizations certify Security only for initial SOC 2.

PART 1: SECURITY (COMMON CRITERIA) — REQUIRED FOR ALL SOC 2 REPORTS

The Common Criteria (CC) controls apply to every SOC 2 engagement. Status: I = Implemented | P = Partial | N = Not Implemented | N/A = Not Applicable

CC1 — CONTROL ENVIRONMENT

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC1.1: COSO Principle 1: The entity demonstrates a commit...	Written code of conduct, management tone at the top, ethics policy. Annual ackno...		

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC1.2: COSO Principle 4: The entity demonstrates a commit...	Job descriptions, background checks, security training, performance reviews.		
CC1.3: COSO Principle 5: The entity holds individuals acc...	Defined security roles, disciplinary procedures, separation of duties.		

CC2 — COMMUNICATION AND INFORMATION

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC2.1: The entity obtains or generates and uses relevant,...	Security monitoring, logging, and reporting processes.		
CC2.2: The entity internally communicates information nec...	Security policies communicated to all staff. Training program in place.		
CC2.3: The entity communicates with external parties rega...	Privacy policy, vendor agreements with security terms, client disclosure.		

CC3 — RISK ASSESSMENT

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC3.1: The entity specifies objectives with sufficient cl...	Documented security objectives tied to business objectives.		
CC3.2: The entity identifies risks to achieving its objec...	Formal risk assessment process with documented findings. Annual at minimum.		
CC3.3: The entity considers the potential for fraud in as...	Fraud risk assessment included in risk management process.		
CC3.4: The entity identifies and assesses changes that co...	Change management process that triggers security review for significant changes.		

CC4 — MONITORING ACTIVITIES

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC4.1: The entity selects, develops, and performs ongoing...	Ongoing monitoring: log reviews, security alerts, access reviews. Separate evalu...		
CC4.2: The entity evaluates and communicates internal con...	Process to identify, document, and remediate control failures. Escalation to man...		

CC5 — CONTROL ACTIVITIES

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC5.1: The entity selects and develops control activities...	Controls mapped to identified risks. Evidence that controls are designed to addr...		
CC5.2: The entity selects and develops general controls o...	IT general controls: change management, access management, operations management...		
CC5.3: The entity deploys control activities through poli...	Comprehensive policy library covering all major security domains, enforced consi...		

CC6 — LOGICAL AND PHYSICAL ACCESS

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC6.1: The entity implements logical access security to p...	MFA for all external access, firewall rules, network segmentation, VPN for remot...		
CC6.2: Prior to issuing system credentials and granting a...	Formal onboarding process: access requests, approvals documented, principle of l...		
CC6.3: The entity authorizes, modifies, or removes access...	Access review process: quarterly review of all user access, offboarding checklis...		
CC6.6: The entity implements logical access security meas...	Intrusion detection, EDR, email filtering, DLP, security monitoring and alerting...		

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC6.7: The entity restricts the transmission, movement, a...	DLP controls, email filtering, data classification, removable media controls.		
CC6.8: The entity implements controls to prevent or detec...	EDR/antivirus, email gateway filtering, software approval process, patch managem...		

CC7 — SYSTEM OPERATIONS

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC7.1: To detect and respond to threats, the entity monit...	SIEM or security monitoring, log aggregation, alert response procedures.		
CC7.2: The entity monitors system components for anomalie...	Behavioral alerting, anomaly detection, 24/7 or defined-hours monitoring coverag...		
CC7.3: The entity evaluates security events to determine ...	Incident classification criteria, triage process, escalation procedures.		
CC7.4: The entity responds to identified security inciden...	Documented IR plan, defined roles, tested (tabletop exercise within past 12 mont...		
CC7.5: The entity identifies, develops, and implements ac...	Recovery procedures, backup and restoration tested, post-incident review process...		

CC8 — CHANGE MANAGEMENT

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC8.1: The entity authorizes, designs, develops, document...	Change management policy, documented change requests, testing before production ...		

CC9 — RISK MITIGATION

Control	What Auditors Look For	Evidence Needed	Status (I/P/N)
CC9.1: The entity identifies and manages risk associated ...	Vendor inventory, security questionnaires for high-risk vendors, contracts with ...		
CC9.2: The entity assesses and manages risks associated w...	Business continuity plan, disaster recovery plan, tested and documented.		

SOC 2 READINESS SUMMARY

Criteria Area	Total Controls	# Implemented	# Partial	# Not Implemented	Readiness %
CC1 — Control Environment	3				
CC2 — Communication	3				
CC3 — Risk Assessment	4				
CC4 — Monitoring	2				
CC5 — Control Activities	3				
CC6 — Logical Access	6				
CC7 — System Operations	5				
CC8 — Change Management	1				
CC9 — Risk Mitigation	2				
TOTAL	29				

SOC 2 Readiness Interpretation:

Readiness Score	Assessment	Recommendation
90–100% Implemented	Audit-ready	Engage auditor. Begin Type II observation period.
75–89% Implemented	Near-ready	Close remaining gaps (target 60 days). Then engage auditor.
50–74% Implemented	Significant gaps	Structured remediation program needed (90–180 days). Axiom Sovereign can accelerate.
Below 50% Implemented	Early stage	6–12 month program build recommended before audit engagement.

Ready to Get Started?

Schedule your complimentary 30-minute discovery call: calendly.com/cmissimore-62kc/20min
info@axiomsovereign.com · axiomsovereign.com