SOC 2 READINESS TOOLKIT

SOC 2 Readiness Toolkit

A self-serve starting point for a first SOC 2: a Trust Services Criteria gap worksheet, a policy starter list, an evidence checklist and Type I vs Type II planning notes.

1. How to use this toolkit

Work through the gap worksheet with the people who run each area. Mark each row Y, Partial or N. Every N becomes a remediation task with an owner and date. Then build the policy set in section 3 and start collecting the evidence in section 4. SOC 2 reports are issued only by licensed CPA firms; this toolkit prepares you for that audit.

2. Trust Services Criteria gap worksheet (Security — Common Criteria)

Criteria	Control area	What auditors look for	Status (Y / Partial / N)	Owner	Notes
CC1	Control environment	Org chart, code of conduct, board/ management oversight			
CC2	Communication & information	Policies communicated to staff; customer-facing security commitments			
CC3	Risk assessment	Documented annual risk assessment including fraud risk			
CC4	Monitoring	Ongoing control monitoring; deficiencies tracked to closure			
CC5	Control activities	Controls mapped to risks; policies approved			
CC6	Logical & physical access	MFA, onboarding/offboarding, quarterly access reviews, encryption			
CC7	System operations	Logging, alerting, vulnerability scanning, incident response			
CC8	Change management	Code review, approvals, separation of duties, deployment records			
CC9	Risk mitigation	Vendor risk management, insurance, business continuity			
A1 (optional)	Availability	Capacity monitoring, backups, DR testing			
C1 (optional)	Confidentiality	Data classification, retention and disposal			

3. Policy starter list

Policy	Must cover
Information Security	Scope, roles, management commitment, review cycle
Acceptable Use	Permitted use of systems and devices
Access Control	Provisioning, MFA, least privilege, access reviews
Change Management	Review, approval, testing and rollback
Incident Response	Roles, severity levels, customer notification
Business Continuity & DR	RTO/RPO, backups, annual test
Risk Assessment	Method, frequency, risk register
Vendor Management	Due diligence, contracts, annual review
Data Classification & Retention	Classes, handling, retention, deletion
Encryption	In transit, at rest, key management
HR Security	Background checks, training, termination
Vulnerability Management	Scan cadence, patch SLAs, pen testing

4. Evidence checklist

Area	Typical evidence
Governance	Approved policies with version history; org chart; board/management meeting notes
People	Signed policy acknowledgements; training completion records; onboarding and offboarding tickets
Access	User lists per system; quarterly access review sign-offs; MFA enforcement screenshots
Change	Pull requests with approvals; change tickets; deployment logs
Operations	Alert samples and responses; vulnerability scan reports and remediation
Vendors	Vendor inventory; vendor SOC reports or questionnaires; contracts
Continuity	Backup job logs; restore test record; DR test report
Risk	Risk register; annual risk assessment sign-off

5. Type I vs Type II planning

	Type I	Type II
Tests	Control design at a point in time	Design and operating effectiveness over a period
Observation window	None	Typically 3–12 months
Good for	Early deals, first report	Most enterprise buyers
Plan	Fix gaps, then book the audit	Fix gaps, run controls for the window, then audit

6. 30-day action plan

Week	Actions
1	Complete the gap worksheet; choose Trust Services Criteria in scope
2	Assign owners; draft missing policies
3	Turn on MFA everywhere; run first access review; start evidence folders
4	Vendor inventory; risk assessment; shortlist CPA firms

> Need help? Quantum Audit Engine offers a Compliance Readiness Assessment and SOC 2 Readiness + Audit at quantumauditengine.com. General guidance only; not legal or audit advice.