SOC2COMPLIANCE · BY CYBER SECURITY SERVICES

SOC 2 Readiness Checklist

87 control items across 8 categories. The exact framework used by Cyber Security Services to take clients from kickoff to audit-ready.

87	8	8–16
CONTROL ITEMS	CATEGORIES	WEEK TIMELINE

Published by

CYBER SECURITY SERVICES

cybersecurityservices.com · soc2compliance.com

sales@cybersecurityservices.com

Updated June 2026

How to Use This Checklist

This checklist is organized into 8 categories that map directly to the AICPA Trust Services Criteria. Each item is a control or piece of evidence that an auditor will look for during your SOC 2 audit.

Three Evaluation Columns Per Item

EXISTS	Do you have this control or document at all? Even informally?
DOCUMENTED	Is the policy or procedure written down and approved by leadership?
OPERATING	Is there evidence (logs, tickets, signed forms) showing the control runs consistently?

A control that exists but isn't documented will be flagged. A documented control that doesn't operate consistently will be flagged worse. The third column — operating with evidence — is where most first-time SOC 2 projects fail.

> Time estimate: Work through this checklist with your team in 4–8 hours. Plan another 4–8 weeks to remediate the gaps you find before scheduling your audit.

CATEGORY 01

Scope & Foundational Documentation

10 items

The auditor needs to know what you're claiming to control. These items define the boundary of your audit.

		EXISTS	DOC'D	OPER.
1	System description documented (services, infrastructure, software, people, data, processes)	☐	☐	☐
2	Trust Services Criteria selected (Security required; Availability, Confidentiality, Processing Integrity, Privacy optional)	☐	☐	☐
3	Audit scope boundary defined (which systems, environments, business units are in/out)	☐	☐	☐
4	Customer commitments documented (SLAs, contractual security promises)	☐	☐	☐
5	System boundary diagram created and current	☐	☐	☐
6	Data flow diagrams for in-scope systems	☐	☐	☐
7	Information security policy written, approved by leadership, reviewed annually	☐	☐	☐
8	Acceptable use policy signed by all employees	☐	☐	☐
9	Code of conduct / ethics policy documented	☐	☐	☐
10	Roles and responsibilities matrix for security functions (RACI)	☐	☐	☐

CATEGORY 02

Logical Access Controls

15 items

The largest category in most SOC 2 audits. Auditors will sample heavily here.

		EXISTS	DOC'D	OPER.
11	Multi-factor authentication required on all production systems	☐	☐	☐
12	MFA required on all admin accounts (SSO, cloud, code repos)	☐	☐	☐
13	Role-based access control (RBAC) implemented with least-privilege defaults	☐	☐	☐
14	User access reviews performed at minimum quarterly with documentation	☐	☐	☐
15	Privileged access management (PAM) for sensitive systems	☐	☐	☐
16	Service account inventory maintained with ownership and rotation	☐	☐	☐
17	Password policy documented and technically enforced (length, complexity, expiry where applicable)	☐	☐	☐
18	Password manager required for all employees	☐	☐	☐
19	SSO implemented for all SaaS applications where available	☐	☐	☐
20	Automated provisioning of access tied to HR system	☐	☐	☐
21	Automated deprovisioning within defined timeframe of employment change	☐	☐	☐
22	Production access logs retained for minimum 12 months	☐	☐	☐
23	Anomalous access alerts configured (impossible travel, after-hours admin actions)	☐	☐	☐
24	Console / production access restricted to engineers with documented need	☐	☐	☐
25	Customer data access logged and reviewable	☐	☐	☐

CATEGORY 03

System Operations & Monitoring

12 items

How you run, watch, and protect your systems.

		EXISTS	DOC'D	OPER.
26	Centralized logging (SIEM or equivalent) deployed	☐	☐	☐
27	Log retention policy documented (minimum 12 months typical)	☐	☐	☐
28	Intrusion detection deployed on production environments	☐	☐	☐
29	Endpoint detection and response (EDR) on all employee devices	☐	☐	☐
30	Vulnerability scanning runs at minimum monthly	☐	☐	☐
31	Vulnerability remediation SLAs documented (critical: 30 days, high: 60, etc.)	☐	☐	☐
32	Patch management documented and operating with evidence	☐	☐	☐
33	Backup procedures documented with retention schedule	☐	☐	☐
34	Backup restoration tested at minimum annually with documentation	☐	☐	☐
35	Disaster recovery plan documented and tested	☐	☐	☐
36	Encryption at rest for all customer data	☐	☐	☐
37	Encryption in transit (TLS 1.2+ minimum) for all customer data	☐	☐	☐

CATEGORY 04

Change Management

8 items

How code and configuration changes reach production.

		EXISTS	DOC'D	OPER.
38	Change management policy documented	☐	☐	☐
39	Code review required for all production changes	☐	☐	☐
40	Separation of duties between developer and deployer (or compensating controls)	☐	☐	☐
41	Change tickets linked to deployments (Jira/Linear CI/CD)	☐	☐	☐
42	Production deployment approval workflow documented	☐	☐	☐
43	Rollback procedures documented and tested	☐	☐	☐
44	Configuration management for production infrastructure (IaC, version control)	☐	☐	☐
45	Emergency change procedures documented separately	☐	☐	☐

CATEGORY 05

Risk Management

10 items

How you identify, assess, and treat risk.

		EXISTS	DOC'D	OPER.
46	Risk assessment performed at minimum annually with documentation	☐	☐	☐
47	Risk register maintained with treatment plans	☐	☐	☐
48	Risk acceptance procedure documented (who approves accepted risk, at what level)	☐	☐	☐
49	Risk owners assigned for each identified risk	☐	☐	☐
50	Threat modeling performed for new features or material changes	☐	☐	☐
51	Annual penetration test completed by qualified third party	☐	☐	☐
52	Penetration test remediation tracked to closure	☐	☐	☐
53	Compliance with applicable regulations (HIPAA, PCI, GDPR, etc.) documented	☐	☐	☐
54	Risk reporting to leadership at minimum quarterly	☐	☐	☐
55	Risk management process reviewed and approved annually	☐	☐	☐

CATEGORY 06

Incident Response

9 items

How you detect, respond to, and recover from security incidents.

		EXISTS	DOC'D	OPER.
56	Incident response plan documented	☐	☐	☐
57	Incident classification scheme defined (severity levels)	☐	☐	☐
58	Incident response team identified with on-call rotation	☐	☐	☐
59	Communication templates for incident communications (internal, customers, regulators)	☐	☐	☐
60	Breach notification procedures aligned with applicable laws	☐	☐	☐
61	Tabletop exercises performed at minimum annually	☐	☐	☐
62	Tabletop documentation retained showing scenario, participants, lessons learned	☐	☐	☐
63	Incident ticket history retained for sampling	☐	☐	☐
64	Post-incident reviews documented for material incidents	☐	☐	☐

CATEGORY 07

Human Resources & Training

12 items

People are the largest control surface. Auditors will sample heavily.

		EXISTS	DOC'D	OPER.
65	Background checks performed for all employees pre-hire	☐	☐	☐
66	Background check documentation retained (verification of completion, not full reports)	☐	☐	☐
67	Onboarding security training required within defined timeframe of start	☐	☐	☐
68	Annual security training required for all employees	☐	☐	☐
69	Training completion records retained	☐	☐	☐
70	Phishing simulations run at minimum quarterly	☐	☐	☐
71	Phishing simulation results tracked with remediation training for failures	☐	☐	☐
72	Confidentiality agreements signed by all employees	☐	☐	☐
73	Offboarding checklist documented and completed for every termination	☐	☐	☐
74	Asset return documented at termination (laptops, badges, etc.)	☐	☐	☐
75	Access revocation timing documented (immediate for involuntary, defined timeframe for voluntary)	☐	☐	☐
76	Contractor / consultant security requirements documented	☐	☐	☐

CATEGORY 08

Vendor Risk Management

11 items

Auditors heavily scrutinize how you manage third-party risk.

		EXISTS	DOC'D	OPER.
77	Vendor inventory maintained (often not just a spreadsheet — auditors want a system)	☐	☐	☐
78	Vendor classification by risk level (critical, high, moderate, low)	☐	☐	☐
79	Vendor security assessment completed before onboarding for critical/high risk vendors	☐	☐	☐
80	Vendor SOC 2 reports collected for all critical vendors	☐	☐	☐
81	Vendor contracts include security and confidentiality terms	☐	☐	☐
82	Data processing agreements (DPAs) in place where required	☐	☐	☐
83	Vendor offboarding procedure documented	☐	☐	☐
84	Annual vendor reassessment for critical vendors	☐	☐	☐
85	Vendor incident notification requirements in contracts	☐	☐	☐
86	Subprocessor list maintained if applicable	☐	☐	☐
87	Vendor risk reviewed in risk register	☐	☐	☐

BEFORE YOUR AUDIT

Pre-Audit Evidence Gathering

In the final 4–6 weeks before your audit, gather these evidence artifacts. The auditor will request samples of each during fieldwork.

- [ ] Access review documentation (last 4 quarters for Type II)
- [ ] Change tickets linked to deployments (sample for testing)
- [ ] Vulnerability scan reports and remediation evidence
- [ ] Penetration test report and remediation tracker
- [ ] Risk assessment with sign-off
- [ ] Incident response tabletop documentation
- [ ] Training completion records
- [ ] Phishing simulation results
- [ ] Background check completion verification
- [ ] Onboarding and offboarding checklists (samples)
- [ ] Vendor risk assessments for critical vendors
- [ ] Customer data encryption verification
- [ ] Backup restoration test documentation
- [ ] Disaster recovery test documentation
- [ ] Policy review and re-approval records
- [ ] Quarterly risk reporting to leadership
- [ ] Board / leadership oversight documentation
- [ ] Annual policy acknowledgments by employees

INTERPRETING YOUR RESULTS

What to Do With This Checklist

If most items are missing or undocumented:

You're in early-stage readiness. Plan 12–20 weeks of work before scheduling your audit. Focus first on policy development and foundational control implementation.

If most items exist but aren't documented:

You're in policy and evidence mode. Plan 6–10 weeks of work focused on documentation. Most controls are likely in place — they just need formal write-ups.

If items are documented but you can't produce evidence:

You're in evidence operations mode. Plan 8–12 weeks of running the controls before the audit window opens to build a track record auditors can sample.

READY FOR YOUR SOC 2?

Want Us to Run This Readiness for You?

Cyber Security Services has guided dozens of organizations through this exact checklist. We bring the methodology, the policy templates, and the auditor relationships. Most clients reach audit-ready in 8–16 weeks.

What You Get With Cyber Security Services

- Gap assessment against this exact checklist
- Prioritized remediation roadmap with effort estimates
- Pre-built policy templates calibrated to your environment
- Direct audit liaison and evidence support
- Auditor-agnostic — we work with your preferred firm or recommend partners
- Fixed-fee scoping — no hourly surprises

Book a Free 30-Minute Scoping Call

Get a fixed-fee quote tailored to your environment, scope, and timeline. No pressure, no upselling.

calendly.com/cybersecurity-services

Prefer email? sales@cybersecurityservices.com

Cyber Security Services · cybersecurityservices.com/risk-assessments/soc-2

SOC 2 readiness and audit support practitioners. Auditor-agnostic. Transparent, fixed-fee scoping.