cycore

FREE DOWNLOAD

2026 EDITION

SOC 2

SOC 2 Readiness Checklist

Cycore's 70-item SOC 2 diagnostic. Mark what's done, score yourself out of 70, and bring the gaps to your first auditor conversation.

PREPARED BY

Cycore

ONLINE

cycoresecure.com

Cycore built this 70-item checklist for teams getting ready for a SOC 2 audit. Go through it, mark what's done, and put a name next to every gap. You'll walk into your first auditor conversation with a specific list. It's organized around the AICPA Trust Services Criteria.

How to use this checklist

Go through every item and mark it done or not done. Each done item is one point, so your raw score runs from 0 to 70, with a subtotal for each of the ten sections. The score is a planning number. It doesn't tell you how the audit will go or how long the work will take.

Every item carries one of three labels, so you can tell what comes from the criteria and what's our advice:

- **TSC-aligned diagnostic.** Our reading of a Trust Services Criteria (TSC) topic.
- **Cycore recommended practice.** Something we advise that the criteria don't spell out.
- **Scope-dependent.** Whether you need it depends on your system, what you've promised customers, the categories you pick, and your auditor.

Section 1: Foundational Decisions

Settle these before implementation work starts. Changing scope midway is the delay we see most often, and it's the easiest one to avoid.

- [ ] **Decided on SOC 2 Type I or Type II.** Type I reports on the design of your controls at a point in time. Type II covers how those controls operated over a review period, and it's what we see enterprise customers ask for.

  Cycore recommended practice

- [ ] **Selected Trust Services Criteria (TSC).** The common criteria, which make up the Security category, apply to every SOC 2 report. Availability, Processing Integrity, Confidentiality, and Privacy are added only when your customers or contracts call for them. Pick what you actually need. Extra categories mean extra controls and extra evidence. TSC-aligned diagnostic

- [ ] **Defined your audit window.** For Type II, agree the review period with your auditor and work backwards from the date you want the report in hand. Scope-dependent

- [ ] **Identified your auditor.** Engage or shortlist a CPA firm early. Ask how they scope, what evidence they expect, and when they can start. Cycore recommended practice

- [ ] **Chosen a GRC platform (if applicable).** Vanta, Drata, Secureframe, and Thoropass are the four platforms we work with. A platform is optional, and it saves a lot of manual evidence collection. This checklist is for the scope, gaps, and owners you settle before you load one. Cycore recommended practice

Section 2: Policies and Documentation

Policies are usually the first thing an auditor asks for. Each one needs to exist, be approved by leadership, get to your employees, and describe what your company actually does. In our experience, generic copy-pasted policies are a common source of audit exceptions, and they're no help to your team when something goes wrong.

The ten policies

- [ ] **Information Security Policy.** The top-level policy. It states what you protect, who is accountable, and which other policies sit under it. TSC-aligned diagnostic

- [ ] **Acceptable Use Policy.** What employees may and may not do with company systems, devices, and data. TSC-aligned diagnostic
- [ ] **Access Control Policy.** How access is requested, approved, reviewed, and removed. TSC-aligned diagnostic
- [ ] **Change Management Policy.** How code and infrastructure changes get proposed, tested, approved, and deployed. TSC-aligned diagnostic
- [ ] **Incident Response Plan.** Who does what when something goes wrong, from detection through post-mortem. TSC-aligned diagnostic
- [ ] **Risk Assessment and Management Policy.** How you identify risks, rate them, decide what to do about them, and how often you repeat the exercise. TSC-aligned diagnostic
- [ ] **Data Classification Policy.** Which data is public, internal, confidential, or restricted, and how each class is handled. TSC-aligned diagnostic
- [ ] **Business Continuity / Disaster Recovery Plan.** How you keep operating and recover when a primary system goes down. The depth an auditor expects depends on whether Availability is in scope. TSC-aligned diagnostic
- [ ] **Vendor Management Policy.** How you evaluate, approve, and monitor third parties that touch your systems or data. TSC-aligned diagnostic
- [ ] **HR / Personnel Security Policy (hiring, onboarding, offboarding).** Security responsibilities across the employee lifecycle, from screening to the day someone leaves. TSC-aligned diagnostic

Policy hygiene

- [ ] **All policies reviewed and approved by leadership.** Signed or documented approval, so you can show who approved what and when. TSC-aligned diagnostic
- [ ] **Policies distributed to all employees.** Shared drive, wiki, or GRC platform. People can find them, and you can show they were shared. TSC-aligned diagnostic
- [ ] **Policies include a version number and review date.** The simplest way to show a policy is current. Cycore recommended practice
- [ ] **Annual review cadence scheduled.** Yearly at minimum, on the calendar, with a named owner. Cycore recommended practice

Section 3: Access Controls

This is where we see the biggest gaps, and it's where the real risk lives. Get this section right and the rest goes faster.

- [ ] **Unique user accounts.** No shared accounts. Every person has their own login. TSC-aligned diagnostic
- [ ] **Multi-factor authentication (MFA) enforced on all critical systems.** Our minimum list: cloud consoles, code repositories, the identity provider, the GRC platform, and production databases. Cycore recommended practice
- [ ] **Single sign-on (SSO) implemented where possible.** One place to grant and revoke access. It makes access reviews and offboarding much easier. Cycore recommended practice
- [ ] **Role-based access control (RBAC).** Grant permissions by job function and remove blanket admin access. TSC-aligned diagnostic

- [ ] **Principle of least privilege applied.** People have access to what their job needs and nothing more. TSC-aligned diagnostic
- [ ] **Quarterly access reviews scheduled or completed.** Quarterly is our cadence. Record who reviewed, when, and what changed. Cycore recommended practice
- [ ] **Offboarding process documented and followed.** A checklist that IT and HR both use. We recommend revoking access within 24 hours of departure. Cycore recommended practice
- [ ] **Admin/root access restricted.** Limited to named individuals. No standing root access unless there is a documented reason. TSC-aligned diagnostic
- [ ] **Service accounts inventoried.** API keys, service accounts, and bot accounts tracked, each with an owner. Cycore recommended practice

Section 4: Infrastructure and Network Security

- [ ] **Cloud infrastructure hardened.** Default security groups reviewed. No rules open to 0.0.0.0/0 on production. Scope-dependent
- [ ] **Encryption at rest enabled on all data stores.** Databases, object storage, and backups. We recommend it everywhere customer data lives. Cycore recommended practice
- [ ] **Encryption in transit.** We recommend TLS 1.2 or higher on every endpoint and no plain HTTP. Cycore recommended practice
- [ ] **Firewall / security groups configured and documented.** You can explain what is allowed in and out, and why. TSC-aligned diagnostic

- [ ] **Intrusion detection or monitoring in place.** A tool that flags suspicious activity in your cloud accounts and workloads, with a named person looking at the alerts. TSC-aligned diagnostic

- [ ] **Vulnerability scanning running on a regular cadence.** At least quarterly, with findings tracked to closure. Cycore recommended practice

- [ ] **Penetration test completed within the last 12 months (or scheduled before audit).** We recommend an annual test by an outside firm. Whether your auditor expects one depends on your system and the criteria in scope. Cycore recommended practice

- [ ] **Production environment separated from staging/development.** Separate accounts or projects, separate credentials, and no production data in test. Cycore recommended practice

- [ ] **Logging enabled on critical systems.** Cloud audit logs, application logs, and access logs. We recommend keeping them for at least one year. Cycore recommended practice

Section 5: Change Management

If your engineers already use pull requests and an automated pipeline, you're most of the way there. What's left is writing down what you already do.

- [ ] **Version control in use for all application code.** Every change is tied to a person and a time. TSC-aligned diagnostic

- [ ] **Pull request / code review process enforced.** No direct commits to main or production branches. A second person looks at every change. TSC-aligned diagnostic

- [ ] **CI/CD pipeline documented.** The automated test and deployment steps are written down, so an auditor can follow a change from commit to production. Cycore recommended practice

- [ ] **Change approval process documented.** Who approves changes, and where the approval is recorded. TSC-aligned diagnostic

- [ ] **Rollback procedures defined.** How you revert a bad deployment, written down and tried at least once. Cycore recommended practice

- [ ] **Infrastructure changes tracked.** Infrastructure as code, or a documented manual process with the same approval trail as application code. TSC-aligned diagnostic

Section 6: Monitoring and Incident Response

- [ ] **Monitoring and alerting configured for production systems.** Uptime, error rates, latency, and resource use, with alerts going to a person. TSC-aligned diagnostic

- [ ] **Incident response plan exists.** The plan from Section 2, with identification, containment, eradication, recovery, and post-mortem written in. TSC-aligned diagnostic

- [ ] **Incident response roles assigned.** Who gets paged, who decides, and who talks to customers. TSC-aligned diagnostic

- [ ] **Incident communication plan.** How and when you notify affected customers. Set the timelines in advance and be straight with customers when something happens. TSC-aligned diagnostic

- [ ] **At least one tabletop exercise or incident drill conducted (or scheduled).** Walk through a realistic scenario with the people who would handle it, and keep notes. Cycore recommended practice

- [ ] **Incidents are logged and tracked.** Even if there haven't been any. Document that. TSC-aligned diagnostic

Section 7: HR and Security Awareness

- [ ] **Background checks conducted on employees.** We recommend them at least for roles with production access, where local law allows. Scope-dependent

- [ ] **Security awareness training completed by all employees.** Keep completion records. Once a year is the cadence we recommend. TSC-aligned diagnostic

- [ ] **Employee handbook or code of conduct includes security responsibilities.** People know what is expected of them and have acknowledged it. TSC-aligned diagnostic

- [ ] **Onboarding includes security training.** Get new hires through it in their first week. Cycore recommended practice

- [ ] **Confidentiality / NDA agreements signed by all employees and contractors.** Signed copies on file, contractors included. Cycore recommended practice

Section 8: Vendor and Third-Party Management

- [ ] **Critical vendors inventoried.** Every SaaS tool, cloud provider, and contractor that touches customer data, in one list with an owner. TSC-aligned diagnostic

- [ ] **Vendor SOC 2 reports collected.** Request one from each critical vendor that has one, note what you reviewed for those that don't, and repeat every year. Cycore recommended practice

- [ ] **Vendor risk assessment process documented.** How you evaluate a new vendor before they get access. TSC-aligned diagnostic

- [ ] **Data Processing Agreements (DPAs) in place with vendors handling customer data.** Whether you need one depends on the data, the jurisdiction, and what you promised your own customers. Scope-dependent

- [ ] **Vendor access reviewed.** Which third-party integrations have access to your systems, and whether they still need it. TSC-aligned diagnostic

Section 9: Business Continuity and Disaster Recovery

- [ ] **Business Continuity Plan (BCP) documented.** What happens if your primary system goes down, and who runs the response. TSC-aligned diagnostic

- [ ] **Disaster Recovery Plan (DRP) documented.** Recovery time objective (RTO) and recovery point objective (RPO) defined. The depth an auditor expects depends on whether Availability is in scope. Scope-dependent

- [ ] **Backups configured and tested.** Automated backups running, and a restore tested at least once. Cycore recommended practice

- [ ] **Backup data encrypted and stored in a separate region/account.** One compromised account or one regional outage should not take the backups with it. Cycore recommended practice

- [ ] **DR test completed (or scheduled before audit).** Run the plan, record what happened, and fix what broke. Scope-dependent

Section 10: Evidence Collection and Audit Prep

If the earlier sections are in place, evidence collection is mostly pulling together what's already there.

- [ ] **Evidence mapped to controls.** You know which piece of evidence supports which criterion before the auditor asks. Cycore recommended practice
- [ ] **Automated evidence collection configured (if using a GRC platform).** Screenshots, configurations, and logs pulling in automatically. Cycore recommended practice
- [ ] **Manual evidence gathered.** Board minutes, policy approval records, training completion logs, and access review records. Cycore recommended practice
- [ ] **System description drafted.** Your auditor will expect a written description of your system (see the AICPA SOC 2 resources). Draft it early. Cover what the system does, the infrastructure, the people, and the controls. Cycore recommended practice
- [ ] **Management assertion letter prepared.** A signed statement from management that the system description is accurate and the controls meet the criteria. For Type II, it also covers how they operated over the review period. Your auditor usually provides a template. Cycore recommended practice
- [ ] **Readiness assessment completed.** Self-assessed with this checklist, or done with outside help. Either way, you walk into the audit knowing your gaps. Cycore recommended practice

Your score

SECTION	ITEMS	YOUR SUBTOTAL
1. Foundational Decisions	5	
2. Policies and Documentation	14	
3. Access Controls	9	
4. Infrastructure and Network Security	9	
5. Change Management	6	
6. Monitoring and Incident Response	6	
7. HR and Security Awareness	5	
8. Vendor and Third-Party Management	5	
9. Business Continuity and Disaster Recovery	5	
10. Evidence Collection and Audit Prep	6	
Total	70	

Whatever your number, the next moves are the same. Start with the open items that would hurt most if an auditor found them, give each one an owner and a date, and take the list into your first auditor conversation so scope and evidence get settled early. If you're not sure where to begin, policies and access controls are where we'd start.

Cocoon's result

Cycore reports that Cocoon reached SOC 2 Type 2 compliance within three weeks and saved an estimated 30 hours of internal work.

Read the case study

More Cycore guides and checklists

- ISO 27001 Gap Assessment
- HIPAA Compliance Checklist
- HITRUST Readiness Guide
- AI Governance Starter Kit

Next step

Talk to Cycore about your SOC 2 timeline