SOC 2 Compliance Checklist

Checklist · 116 items · 15 sections

A step-by-step SOC 2 readiness checklist for B2B SaaS startups pursuing a Type II report under the AICPA Trust Services Criteria (2017, revised 2022). Covers the 5 TSCs, the Common Criteria controls, evidence collection, auditor selection, and a realistic 6-12 month timeline with a $25K-$100K budget.

Open the editable version online:
https://genechecklist.com/checklist/soc-2-compliance-checklist

SOC 2 FUNDAMENTALS - DECIDE YOUR SCOPE

- [ ] Decide Type I vs Type II
  HIGH
  Type I: design at a point in time (4-8 weeks, $10K-$25K). Type II: operating effectiveness over 3-12 months ($25K-$100K).
- [ ] Default to Type II for enterprise sales (~90% of procurement teams require Type II, not Type I)
  HIGH
- [ ] Pick observation window: start with 3 months for first Type II, then move to 12-month renewals
  HIGH
- [ ] Set the report period dates in writing before audit starts (e.g., April 1 - June 30, 2026)
  HIGH
  Auditor will only test evidence dated inside that window.
- [ ] Plan a Type I first if you need a report in under 90 days for a single deal, then bridge to Type II within 6 months
- [ ] Budget the full program
  $15K-$30K platform (Vanta/Drata/Secureframe) + $15K-$50K auditor + 0.25-1.0 FTE internal for 6-12 months.
- [ ] Schedule audit window to end 60+ days before your largest renewal cycle so the report is fresh during negotiations
- [ ] Decide SOC 1 vs SOC 2 vs SOC 3
  SOC 1: financial reporting controls (rare for SaaS). SOC 2: operational. SOC 3: public summary.

TRUST SERVICE CRITERIA SELECTION

- [ ] Include Security (Common Criteria, CC series): mandatory in every SOC 2 report
  HIGH
  33-64 controls depending on revision.
- [ ] Decide on Availability TSC: include if you have uptime SLAs in customer contracts (99.5%, 99.9%, 99.95%)
  HIGH

- [ ] Decide on Confidentiality TSC: include if you handle customer data under NDA, marked restricted, or DPA-covered
- [ ] Decide on Processing Integrity TSC: include if you process financial transactions, payroll, billing (skip for most SaaS)
- [ ] Decide on Privacy TSC: only if you collect personal data directly from data subjects under your own privacy notice

  Most B2B SaaS uses Confidentiality instead.
- [ ] Document TSC selection in the System Description (Section III of the report) with rationale
- [ ] Each optional TSC adds 10-25 controls and 15-30% to audit fees

SECURITY TSC - ACCESS MANAGEMENT (CC6)

- [ ] Implement SSO via Okta, Google Workspace, Azure AD, or Jumpcloud for all production systems and SaaS tools

  HIGH
- [ ] Enforce MFA on SSO, cloud root accounts, GitHub, repos, and admin consoles (TOTP or hardware key, not SMS)

  HIGH
- [ ] Document an access provisioning workflow with manager approval ticket evidence

  HIGH
- [ ] Run quarterly user access reviews (UAR) for every production system and SaaS tool

  HIGH
- [ ] Revoke all access within 24 hours of termination: ticket evidence, SSO deactivation logs

  HIGH
- [ ] Apply least privilege: separate IAM roles for read-only, developer, admin; no shared accounts

  HIGH
- [ ] Disable inactive accounts after 90 days of no login (30 for privileged)

  HIGH
- [ ] Implement just-in-time (JIT) access for production (Teleport, AWS IAM Identity Center, ConductorOne)
- [ ] Password policy: 12+ characters, no expiration if MFA enforced (NIST SP 800-63B)
- [ ] Lock accounts after 5 failed login attempts within 15 minutes
- [ ] Maintain a personnel access matrix mapping every role to every system

SECURITY TSC - ENCRYPTION (CC6.1, CC6.7)

- [ ] Encrypt data at rest with AES-256: S3 (SSE-S3/SSE-KMS), RDS, EBS, encrypted backups

  HIGH
- [ ] Encrypt data in transit with TLS 1.2+: force HTTPS, redirect HTTP, disable TLS 1.0/1.1

HIGH

- [ ] Use AWS KMS, GCP KMS, Azure Key Vault, or HashiCorp Vault with automatic key rotation
  HIGH
- [ ] Encrypt laptops (FileVault/BitLocker/LUKS) and monitor via MDM (Kandji, Jamf, Intune)
  HIGH
- [ ] Document encryption standard policy: algorithms (AES-256-GCM, RSA-2048+, ECDSA P-256+) and key rotation cadence
  HIGH
- [ ] Generate and pin TLS certificates via ACM, Let's Encrypt, or DigiCert; alert 30 days before expiration
- [ ] Disable weak ciphers (RC4, DES, 3DES); run quarterly SSL Labs tests targeting A or A+
- [ ] Rotate KMS customer master keys (CMKs) annually or after suspected compromise
- [ ] Encrypt app-layer secrets (DB passwords, API keys) in Vault, AWS Secrets Manager, or Doppler; never in env files

SECURITY TSC - VULNERABILITY MANAGEMENT (CC7.1)

- [ ] Run weekly automated vulnerability scans (Nessus, Qualys, Tenable, AWS Inspector); document remediation in ticketing
  HIGH
- [ ] Run annual third-party penetration test with CREST or OSCP-certified firm ($8K-$40K)
  HIGH
- [ ] Patch SLAs: critical within 30 days, high 60, medium 90
  HIGH
- [ ] Scan container images (Trivy, Snyk, Aqua) before deploy; block builds with critical CVEs
  HIGH
- [ ] Scan dependencies (Dependabot, Snyk, Renovate) with auto-PRs for critical patches
  HIGH
- [ ] Run SAST tools (Semgrep, SonarQube, GitHub CodeQL) in CI on every PR
- [ ] Maintain a software bill of materials (SBOM) per release (Syft or CycloneDX)
- [ ] Document CVSS scoring methodology and risk acceptance process for vulnerabilities you cannot fix
- [ ] Subscribe to vendor security advisories for every major dependency

SECURITY TSC - CHANGE MANAGEMENT (CC8.1)

- [ ] Require PR review with at least 1 approval from a non-author engineer before merging to main
  HIGH
- [ ] Capture PR approval evidence: GitHub branch protection rules, required reviews, CODEOWNERS

HIGH

- [ ] Block direct pushes to production branches via GitHub branch protection / GitLab protected branches

  HIGH
- [ ] Run automated tests in CI before merge: unit, integration, lint, type checks

  HIGH
- [ ] Document a change management policy: normal, emergency, and standard changes with approval paths

  HIGH
- [ ] Track every production deploy with deployer name, commit SHA, timestamp

  HIGH
- [ ] Require emergency change post-mortems within 5 business days documenting what bypassed normal process and why
- [ ] Separate dev, staging, and production environments with distinct credentials and network segmentation
- [ ] Tag releases via semver and changelog so auditors can sample a population of changes

SECURITY TSC - INCIDENT RESPONSE (CC7.3-7.5)

- [ ] Document an Incident Response Plan with SEV1/SEV2/SEV3, roles, escalation paths, communication templates

  HIGH
- [ ] Run at least 1 tabletop incident exercise per year; capture notes, attendees, lessons learned

  HIGH
- [ ] Maintain an incident log: every SEV1/SEV2 with timestamps, root cause, impact, remediation, post-mortem link

  HIGH
- [ ] Define customer notification SLAs: typically 72 hours for confirmed breaches (GDPR Article 33)

  HIGH
- [ ] Set up 24x7 alerting (PagerDuty, Opsgenie, VictorOps) with on-call rotations documented

  HIGH
- [ ] Implement centralized logging (Datadog, Sumo Logic, Splunk, CloudWatch) with 1-year retention minimum
- [ ] Configure SIEM rules or anomaly detection for failed logins, privilege escalation, unusual data egress
- [ ] Document a forensic preservation procedure: snapshot affected systems, preserve logs, chain of custody
- [ ] Maintain contacts: legal counsel, cyber insurance carrier, law enforcement (FBI IC3), breach notification vendors

AVAILABILITY TSC

- [ ] Publish an uptime SLA (99.5%-99.95%) and instrument a status page (Statuspage, Better Stack, Instatus)

  HIGH
- [ ] Document Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) with RTO/RPO per service tier

  HIGH
- [ ] Test backup restoration at least annually; document test results, restore time, data integrity verification

  HIGH
- [ ] Automate database backups: daily snapshots with 30-day retention, cross-region replication for production

  HIGH
- [ ] Document RPO (typically 1 hour for production databases) and RTO (typically 4 hours for SEV1)

  HIGH
- [ ] Run capacity planning quarterly: forecast CPU, memory, storage, DB connection headroom for 2x growth
- [ ] Monitor SLIs (latency, error rate, throughput, saturation) with alerting on SLO burn rate
- [ ] Multi-AZ deploy for production databases (RDS Multi-AZ, Cloud SQL HA) with documented failover test results
- [ ] Test full region failover annually if your SLA requires regional redundancy

CONFIDENTIALITY TSC

- [ ] Publish a data classification policy with 3-4 tiers (Public, Internal, Confidential, Restricted)

  HIGH
- [ ] Sign NDAs with every employee, contractor, vendor before data access (signed copies in HRIS)

  HIGH
- [ ] Document secure data disposal: NIST SP 800-88 sanitization for laptops, certificates of destruction for drives

  HIGH
- [ ] Apply DLP controls on email and cloud storage (Google DLP, Microsoft Purview) for cards, SSNs, API keys
- [ ] Restrict production data access to a named list reviewed quarterly
- [ ] Mask or tokenize PII in non-production environments (staging, QA, analytics)

HR AND ONBOARDING CONTROLS (CC1.4-1.5)

- [ ] Run background checks on every new hire (Checkr, Certn, HireRight): criminal, employment, education

  HIGH

- [ ] Sign confidentiality and IP assignment agreements on day 1 before system access

  HIGH

- [ ] Deliver security awareness training within 30 days of hire and annually thereafter (KnowBe4, Hoxhunt, Curricula)

  HIGH

- [ ] Run quarterly phishing simulation campaigns; track click rates per team

  HIGH

- [ ] Document an offboarding checklist: revoke SSO, collect laptop, disable badge, transfer file/repo ownership, exit interview

  HIGH

- [ ] Maintain current org chart and job descriptions defining security responsibilities per role
- [ ] Capture training completion evidence: LMS reports, attendance logs, signed acknowledgments

VENDOR AND THIRD-PARTY RISK MANAGEMENT (CC9.2)

- [ ] Maintain a vendor inventory (subprocessors, SaaS tools, infrastructure) with data classification per vendor

  HIGH

- [ ] Collect SOC 2 Type II reports or ISO 27001 certificates from every critical vendor annually

  HIGH

- [ ] Sign Data Processing Agreements (DPAs) with every subprocessor handling customer data

  HIGH

- [ ] Run vendor security reviews before signing: questionnaire, SOC 2 review, security architecture review

  HIGH

- [ ] Re-review critical vendors annually; document findings and risk acceptance for any gaps
- [ ] Publish a public subprocessor list; notify customers of changes 30 days in advance

DOCUMENTATION AND POLICIES

- [ ] Document policies: Information Security, Access Control, AUP, Change Management, IR, BC/DR, Vendor Mgmt, Data Classification, Retention, HR Security, Vulnerability Management, Encryption

  HIGH

  Each policy: owner, review cadence (annual), leadership signature.

- [ ] Acknowledge all policies at hire and annually via HRIS or LMS workflow

HIGH

PRE-AUDIT GAP ASSESSMENT

- [ ] Pick a compliance automation platform: Vanta ($12K-$35K/yr), Drata ($15K-$40K), Secureframe ($10K-$30K), Thoropass, Sprinto

HIGH

- [ ] Run a readiness assessment with a CPA firm or platform consultant 60-120 days before audit start

HIGH

- [ ] Map every Common Criteria control to a named owner, system, and evidence type

HIGH

- [ ] Connect compliance platform to AWS/GCP/Azure, GitHub, Okta, HRIS, MDM, and ticketing for continuous evidence collection

HIGH

- [ ] Resolve every red/critical gap before the audit window starts

HIGH

- [ ] Pick an auditor: regional CPA firms specializing in SOC 2 (A-LIGN, Schellman, Prescient, Insight Assurance, Johanson Group) over Big 4 for cost ($15K-$50K vs $100K+)
- [ ] Verify audit firm holds active AICPA peer review and CPA license in your state
- [ ] Run a mock audit 30 days before the official audit kicks off

DURING THE AUDIT

- [ ] Hold kickoff meeting: confirm scope, period, system description, exclusions, evidence request list (PBC)

HIGH

- [ ] Respond to evidence requests within 5 business days via the auditor's portal

HIGH

- [ ] Prepare for control walkthroughs: 30-60 min live demo per control area with system owner

HIGH

- [ ] Expect sampling: auditors will pick 25-40 samples per population (terminations, changes, access reviews, incidents)

HIGH

- [ ] Document management response for every finding: root cause, corrective action, target date

HIGH

- [ ] Track open questions in a single shared sheet: auditor name, request, response, status
- [ ] Schedule weekly status meetings with the lead auditor for the duration of fieldwork (4-8 weeks)

- [ ] Save the final draft report for management review before the auditor issues the final signed report

POST-AUDIT MAINTENANCE

- [ ] Close every Type II exception within the next audit period; document remediation evidence
  HIGH
- [ ] Set up continuous monitoring via the compliance platform to detect control drift between audits
  HIGH
- [ ] Run quarterly internal testing on high-risk controls (access reviews, change mgmt, backups)
  HIGH
- [ ] Refresh policies annually with leadership signoff and re-acknowledgment by all employees
  HIGH
- [ ] Schedule the next Type II audit so report periods are contiguous (no gaps) for customers requiring continuous coverage
  HIGH
- [ ] Update the System Description as architecture, vendors, or scope changes
- [ ] Track new SaaS tools and subprocessors; onboard them to the vendor review process
- [ ] Publish the SOC 2 Type II report behind NDA to prospects via a trust center (SafeBase, Drata Trust Center, Vanta Trust)