SEED STAGE SAAS

SOC 2 Readiness Checklist

Every control domain you need in place before your first audit. Check them off one at a time.

swipe

01

PRE-AUDIT

Pick Your Auditor Before You Build

- ☐ Big 4 (PwC, Deloitte, EY, KPMG). Overkill for seed stage. Expensive, slow to schedule, built for enterprises with dedicated compliance teams. Skip unless an enterprise customer demands it.
- ☐ Boutique CPA firms. Treat SOC 2 as a consulting engagement. They review your control design before the audit starts, flag gaps early, help you write policies that scale. More expensive but worth it if you can afford them.
- ☐ SOC-focused audit firms. Process hundreds of reports a year using repeatable, efficient workflows. Fast, predictable, and half the cost of a boutique. They audit what you hand them. You bring the program design.
- ☐ The hybrid model: hire a SOC-focused firm for the audit, bring in a contractor to design the program. Lower audit fee plus properly built controls. The contractor relationship persists after the report lands.

A bad auditor doesn't fail your Type 1. They pass it. You discover the problems when Type 2 findings pile up and unwinding costs more than doing it right the first time.

02

PRE-AUDIT

Scope, Platform & Calendar

- [ ] Decide which Trust Services Categories. Start with Security + Availability. Add Confidentiality if you handle sensitive customer data. Skip Processing Integrity unless you process financial transactions.
- [ ] Sign up for a compliance automation platform. Drata, Vanta, or Secureframe. Connect integrations: cloud provider, identity provider, HRIS, code repository, MDM.
- [ ] Create a shared compliance calendar visible to leadership. Not buried in a platform dashboard.
- [ ] Schedule quarterly access reviews, quarterly backup restore tests, monthly vulnerability scan review.
- [ ] Schedule annual DR test, annual policy reviews, certificate and domain renewal reminders.
- [ ] Write cadences into policy at sustainable levels. Quarterly for most things. The auditor grades you against your own policies.

GOVERNANCE

Full Policy Inventory

Start with the **Information Security Policy**. It is the top-level document. Every operational policy flows from it.

- ☐ **Information Security Policy** — governance, risk appetite, scope, annual review
- ☐ **Access Control Policy** — provisioning, deprovisioning, access reviews, MFA, least privilege
- ☐ **Change Management Policy** — PR reviews, CI/CD pipeline, emergency changes, separation of duties
- ☐ **Incident Response Policy** — roles, escalation, communication, post-mortems
- ☐ **Data Classification & Handling Policy** — tiers, labeling, encryption, retention, disposal
- ☐ **Vulnerability Management Policy** — scanning cadence, SLA by severity, risk acceptance process
- ☐ **Business Continuity & DR Policy** — RTO/RPO targets, test schedule, recovery procedures
- ☐ **Acceptable Use Policy** — company assets, personal use, monitoring, consequences
- ☐ **Third-Party Risk Management Policy** — vendor inventory, assessment criteria, review cadence
- ☐ **Encryption & Cryptography Policy** — standards, key management, at-rest and in-transit requirements
- ☐ **Network Security Policy** — segmentation, firewall rules, remote access, VPN requirements
- ☐ **Logging & Monitoring Policy** — collection scope, retention periods, alerting thresholds
- ☐ **Background Check Policy** — screening criteria, timing, documentation
- ☐ **Security Awareness Training Policy** — annual training, new-hire training, phishing simulations
- ☐ **Code of Conduct** — ethics, conflicts of interest, professional behavior

> **Policies are prescriptive, not descriptive.** A policy should read like a set of rules. "Must." "Required." "Shall." Not "We use MFA" or "The company values security." If you find yourself writing an essay, you are doing it wrong. The auditor does not need to understand your philosophy. They need a clear statement of what your organization requires, so they can test whether you actually do it. One sentence per requirement. No narrative. No justification paragraphs. The policy exists to be audited against.

04

HR & PEOPLE

Onboarding & Offboarding

- [ ] Documented onboarding process. Employee added to IdP, assigned to correct groups, access granted by role within 24 hours of start.
- [ ] Documented offboarding process. Access revoked within 24 hours. Accounts disabled, not deleted. Automated where possible.
- [ ] No shared accounts for individual contributor work. Every action attributable to a specific person.
- [ ] Signed documents stored with timestamps: offer letter, NDA, policy acknowledgments. HRIS integration with compliance platform.
- [ ] Quarterly access review scheduled on a fixed date. Managers sign off on their team's permissions. Evidence saved.

> This is consistently the most common place auditors find exceptions. Shared accounts make it impossible to prove who did what, and SOC 2 cares deeply about attribution. The fix is almost always procedural, not technical. Write the checklist. Follow it every time. If you miss even one quarter of access reviews, the auditor will notice. The calendar invite is the most important tool here.

05

HR & PEOPLE

Background Checks & Security Training

- [ ] Background checks for all employees before start date. Document the policy and the results.
- [ ] Annual security awareness training for all employees. Platform: KnowBe4, Curricula, or equivalent.
- [ ] New hire training within first week of onboarding. Completion tracked and reported to compliance platform.
- [ ] Phishing simulations recommended but not mandatory for SOC 2. Strong evidence if you run them.
- [ ] Role-based training for engineers with production access. Secure coding, OWASP Top 10, cloud security.

> Training is quick to implement but easy to let slide. Hook your training platform into your HRIS or SSO so completion is tracked automatically. The auditor will ask for completion reports, not whether people remember the content. Budget two hours to set up the training pipeline and one hour per employee per year after that.

06

ACCESS MANAGEMENT

IAM, MFA & Access Reviews

- [ ] Single sign-on via identity provider. Okta, Entra ID, Google Workspace with SAML/OIDC.
- [ ] Multi-factor authentication enforced for all users. No exceptions for administrators.
- [ ] Group-based permissions. Never assign permissions directly to individual users.
- [ ] Quarterly access reviews. Managers sign off on their team's permissions. Evidence saved.
- [ ] Privileged access management. Just-in-time elevation or separate admin accounts for production.
- [ ] Deprovisioning automation. SCIM provisioning where supported. Manual checklist as fallback.

> When an auditor asks "who had production access last Tuesday," you need to answer with a log, not a shrug. Infrastructure-as-code is the secret weapon here. When your access controls live in Terraform, every change has a git commit showing who requested it, who approved it, and when it was applied. The audit trail writes itself.

07

DEVICE MANAGEMENT

MDM, Encryption & Endpoint Controls

- [ ] MDM enrolled on all company devices. Jamf, Kandji, Intune, or equivalent.
- [ ] Full disk encryption enforced. FileVault on macOS, BitLocker on Windows.
- [ ] Screen lock policy. Auto-lock after 5-10 minutes of inactivity. Strong password required.
- [ ] Remote wipe capability. Must be able to erase a lost or stolen device.
- [ ] Malware protection enabled. Built-in (Defender, XProtect) or third-party.
- [ ] No personal laptops for production access. Company hardware only for anyone touching production.

> There is no great open source MDM. This is one domain where paying for a commercial tool is the strategic move. The time you save not managing an open source MDM will exceed the license cost within the first quarter. The auditor is not going to inspect laptops. They are going to ask for an MDM report showing encryption status and screen lock policy across your fleet.

CHANGE MANAGEMENT

Code Reviews, CI/CD & Separation of Duties

- [ ] Pull requests required for all merges to main. Branch protection enabled.
- [ ] At least one approving review from someone other than the author.
- [ ] CI/CD pipeline deploys. Nobody runs deploys from their laptop against production.
- [ ] Infrastructure changes follow same process. Terraform changes go through PR review.
- [ ] Emergency change procedure documented. Bypass allowed, but retroactive documentation required.
- [ ] Separation of duties. Author and approver are different people. CI deploys, not individuals.

> If you are a seed stage company deploying to production ten times a day, the auditor does not expect a change advisory board meeting for every merge. They expect a process that ensures changes are reviewed, tested, and traceable. A three-person team gets separation of duties through PR reviews: the author and the approver are different people. The CI system deploys. That is defensible even at very small scale.

09

LOGGING & MONITORING

Centralized Logs, Alerting & Retention

- [ ] Centralized logging from all production systems. Application, infrastructure, and audit logs.
- [ ] Audit logging enabled everywhere. CloudTrail or equivalent. Immutable storage with versioning.
- [ ] Minimum 90-day retention. One year recommended. Define and document your retention policy.
- [ ] Log integrity protection. Tamper-proof storage with access logging.
- [ ] Alerting configured. Failed logins, unusual API activity, infrastructure changes outside normal pipeline.
- [ ] Someone actually reviews the logs. Collection without review is not a control. It is storage.

> Almost every other control domain depends on logs. Access reviews reference logs. Incident response references logs. Change management references logs. If your logging is fragmented or unreliable, the whole program gets shaky. Budget a week to get every source centralized. Then budget time to define what normal looks like so your alerts are not just noise.

VULNERABILITY MANAGEMENT

Scanning, SLA & Remediation

- [ ] Regular vulnerability scanning. Weekly automated scans of hosts, containers, and dependencies.
- [ ] Defined remediation SLA. Critical: 72 hours. High: 7 days. Medium: 30 days. Low: accepted risk.
- [ ] Container image scanning in CI pipeline. Block images with critical vulnerabilities from production.
- [ ] Dependency scanning. SCA tool for open source libraries. Alert on known CVEs.
- [ ] Formal risk acceptance process. Documented exceptions for vulnerabilities that cannot be patched.
- [ ] Remediation tracking. Tickets or backlog items for every finding above accepted threshold.

> The first scan will be ugly. Hundreds of findings. Do not panic. Triage by severity. Fix the Criticals. Accept the Lows with a note. The remediation pipeline is what matters. Being able to show the auditor that you went from 47 Critical findings to zero in two weeks is stronger evidence than having zero findings on day one. They want to see that the process works, not that you were never vulnerable.

BACKUP MANAGEMENT

Backup Schedules, Retention & Restore Tests

- [ ] Defined backup schedule. Automated backups for all production databases and critical data stores.
- [ ] Documented retention policy. Minimum 30 days for databases. Aligned with business requirements.
- [ ] Immutable backups. WORM compliance where supported. Prevents accidental or malicious deletion.
- [ ] Quarterly restore tests. Pick a production database, restore to sandbox, verify data integrity.
- [ ] Documented restore test results. Pass or fail, with remediation plan if fail.
- [ ] Cross-region or off-site backup copies. Survive a single-region outage.

> Backups are one of those things that everyone agrees are important and almost nobody tests. The restore test is the part most teams skip and the part auditors ask about first. Schedule it quarterly. The first time you do it, you will find something broken. That is normal. Better to find it during a test than during an incident. Document the result regardless of outcome.

DISASTER RECOVERY

DR Plan, Testing & Business Continuity

- [ ] Documented DR plan. Defined RTO and RPO targets for critical systems.
- [ ] Annual DR test. Tabletop exercise minimum. Technical failover for stronger evidence.
- [ ] DR test results documented. Gaps identified, remediation tracked, lessons incorporated into plan.
- [ ] Multi-AZ or cross-region deployment for critical workloads. Single points of failure identified.
- [ ] Business continuity plan. Covers key personnel, communication plan, alternate work arrangements.
- [ ] DR/BCP plan reviewed and updated annually. Contact lists kept current.

> DR is the heavyweight. It is the domain most likely to reveal gaps in your architecture, and it is the one auditors scrutinize hardest because the blast radius of failure is the largest. Multi-AZ deployment is not a checkbox. It means your application has to handle connection drops, stale DNS, and eventual consistency. The DR conversation should happen during architecture design, not three months before the audit.

INCIDENT RESPONSE

IR Plan, Tabletop & Post-Mortems

- [ ] Documented IR plan. Defines incident classification, roles, communication channels, escalation.
- [ ] At least one tabletop exercise completed before Type 1 audit. Documented results.
- [ ] Incident detection mechanisms active. Alerts from logging and monitoring feed into IR process.
- [ ] Post-mortem process defined. Every incident documented: timeline, root cause, preventive measures.
- [ ] Communication protocol. Internal escalation, customer notification timeline, regulatory obligations.
- [ ] IR plan tested annually. Update based on lessons learned from exercises and real incidents.

> Incident response is the domain where the gap between policy and reality is usually widest. Most seed stage companies have no formal IR process. When something breaks, someone notices, someone fixes it, and everyone moves on. That is fine for operations. It is not fine for SOC 2. The first time you run a tabletop exercise, you will discover that half the team does not know who to call and the other half does not know what qualifies as an incident. That is normal. That is why you run the exercise.

VENDOR RISK & NETWORK

Third-Party Risk, Segmentation & Encryption

- [ ] Vendor inventory. Every vendor with access to customer data or production. Reviewed quarterly.
- [ ] Vendor risk assessments. SOC 2 reports or VSA questionnaires collected. Residual risk documented.
- [ ] Network segmentation. Production in private subnets. Only load balancers and bastions public.
- [ ] Firewall rules follow least privilege. No 0.0.0.0/0 on anything except public load balancers.
- [ ] Encryption in transit enforced. TLS 1.2 minimum. HSTS enabled on all public endpoints.
- [ ] Encryption at rest enabled. Default storage encryption or explicit KMS/CMK for sensitive data.

> Nobody has a vendor inventory the first time they look. You will discover SaaS tools you forgot you subscribed to. Budget an afternoon to go through your credit card statements and SSO logs. On the network side, every cloud account that has been running for more than six months has cruft: rules opened for a test and never closed, ports wider than they need to be. The audit prep is not creating rules. It is reviewing the ones you already have.

80%

READINESS SCORE

Get these right, you are 80% there.

No two companies will implement SOC 2 the same way. Your industry, architecture, team size, and auditor shape the specifics. But across every seed stage company, these domains consume the same 80% of the effort.

SOC 2 is not a mystery. It is operational practices any competent engineering team can implement. **The part that hurts is not the complexity. It is the calendar time.**

Full field manual: brooks-security.com/posts/soc-2-field-manual-seed-stage/