Cloud Security & SOC 2 Readiness Checklist

A 30-point self-assessment across the AWS controls auditors actually test — for SOC 2, ISO 27001, PCI DSS and HIPAA. Tick what's already true. Every unticked box is a finding waiting to happen.

Sahil Dubey
Cloud · DevOps · Compliance Architect
CISA · CISM · AWS SA Pro
sahildubey.us

Identity & Access IAM

- [ ] Root account locked: MFA on, no access keys, unused. CC6.1
- [ ] Human access via SSO / Identity Center — no shared IAM users.
- [ ] MFA enforced for every human principal.
- [ ] Least-privilege roles; no wildcard `*:*` policies in prod.
- [ ] Quarterly access review with exportable evidence.

Network & Perimeter VPC

- [ ] No `0.0.0.0/0` to SSH/RDP or databases.
- [ ] Private subnets for data tier; public only for LB/CDN.
- [ ] Security groups + NACLs documented and diagrammed. CC6.6
- [ ] WAF + Shield on public edges; TLS 1.2+ everywhere.

Data Protection KMS

- [ ] Encryption at rest on all stores (EBS, RDS, S3). CC6.7
- [ ] Customer-managed KMS keys with rotation enabled.
- [ ] Secrets in Secrets Manager / SSM — none in code or env files.
- [ ] S3 Object Lock / versioning on evidence + backups.

Logging & Detection CLOUDTRAIL

- [ ] Org-wide CloudTrail to a locked, central log account. CC7.2
- [ ] AWS Config enabled with conformance packs.
- [ ] GuardDuty + Security Hub on, findings triaged.
- [ ] Alerting routes to a real on-call, not a dead inbox.

Change & CI/CD PIPELINE

- [ ] All infra as code (Terraform / OpenTofu); no console drift. CC8.1
- [ ] PRs require review; protected main branch.
- [ ] IaC scanning (Checkov / OPA) blocks non-compliant merges.
- [ ] Deploy history + approvals retained as evidence.

Resilience & Governance CC7 / A.17

- [ ] Automated backups + a *tested* restore, with RTO/RPO defined.
- [ ] Multi-AZ for critical data; DR runbook exists.
- [ ] Documented incident-response plan, rehearsed once a year.
- [ ] Policy set matches what's actually running (not a template).
- [ ] Vendor / sub-processor risk reviewed and logged.

How to read your score. 27–30 ticked → you're audit-ready; book a confirmation review. 20–26 → a 6–10 week remediation gets you there. Under 20 → start with identity, logging and encryption — they carry the most audit weight. This checklist maps to SOC 2 Trust Services Criteria; the same controls satisfy ISO 27001, PCI DSS and HIPAA.

Want the gaps closed?

Free 30-min readiness review:
sahildubey.us/#book