SOC 2 Evidence Collection Checklist

Trust Services Criteria — owner-role · cadence · sample-size

A working checklist of the evidence artifacts a SOC 2 auditor asks a 10–250 person SMB to produce, grouped by the five Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy). Each row lists the owner-role (who owns the artifact), cadence (how often it is generated), and sample-size (how many to keep on file across the observation window). Use this alongside the framework hub at /soc-2-checklist while you build out Type II evidence.

AT A GLANCE

5 Trust Services Criteria · 37 evidence artifacts

Security is required in every SOC 2 audit. Availability / Processing Integrity / Confidentiality / Privacy are optional, added based on customer demand.

HOW TO USE

Start with Security — the other four TSCs are optional and layered later. For each artifact: (1) confirm owner-role is on staff or contracted, (2) confirm cadence fits the auditor observation window (typically 6–12 months), (3) collect sample-size evidence as dated exports / screenshots. Pair this PDF with the free Compliance Gap Analysis (cyberstackhub.ai/assess) to pre-score your TSC coverage before paying for Sprinto / Drata / Defendify / Vanta.

1 Security (Common Criteria — CC1–CC9)

TSC CC1–CC9

The only required SOC 2 category. Covers governance, communication, risk assessment, monitoring, control activities, logical & physical access, system operations, change management, and risk mitigation.

CISO/Exec

1. Security charter + code of conduct

Signed charter naming the security owner, reporting lines, and a code of conduct every employee signs at hire.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

HR/Legal

2. Security awareness training completion log

Dated record of every active employee completing annual security awareness training (KnowBe4, Proofpoint, or internal LMS).

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 25 artifacts

Security Lead

3. Annual risk register with executive sign-off

Top 10–20 risks scored (likelihood × impact), risk-treatment decisions, and an executive review signature.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

IT/Ops

4. SSO + MFA enforcement evidence

Configuration export from your identity provider (Okta, Entra, Google Workspace) showing MFA enforced on every production app.

CADENCE: Quarterly
SAMPLE-SIZE / OBSERVATION WINDOW: 4 artifacts

IT/Ops

5. Quarterly user access review

Quarterly screenshots showing who has access to production systems with role justification; terminate-on-exit evidence.

CADENCE: Quarterly
SAMPLE-SIZE / OBSERVATION WINDOW: 4 artifacts

IT/Ops

6. Centralized authentication logs ("e90 day retention)

Auth log exports from production covering at least the last 90 days (SIEM, CloudWatch, Datadog logs).

CADENCE: Continuous
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

IT/Ops

7. Endpoint EDR coverage report

Monthly EDR coverage report (Defender for Endpoint, CrowdStrike, SentinelOne) — % endpoints with EDR active.

CADENCE: Monthly
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

IT/Ops

8. Monthly vulnerability scan + remediation tickets

Configured scan output (Tenable, Qualys, AWS Inspector) with the high/critical finding remediation tickets closed within 30 days.

CADENCE: Monthly
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

Security Lead

9. Incident response plan + tabletop test write-up

Current IR plan plus a dated tabletop exercise write-up with attendees, scenario, and lessons learned.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

Engineering

10. Production change tickets with peer review

Sampled deploy / change tickets in the last quarter with mandatory peer-review approval and rollback evidence.

CADENCE: Weekly
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

Security Lead

11. Subprocessor inventory + annual SOC 2 reviews

Maintained subprocessor list plus annual SOC 2 reports collected for each critical vendor (AWS, Stripe, data warehouse).

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

Engineering

12. Encryption-at-rest + in-transit configuration evidence

Cloud console screenshots showing TLS 1.2+ enforced and database / laptop encryption (KMS, BitLocker, FileVault) active.

CADENCE: Quarterly
SAMPLE-SIZE / OBSERVATION WINDOW: 4 artifacts

2 Availability (A1)

TSC A1.1–A1.3

Optional TSC. Covers system uptime commitments, capacity planning, environmental protections, and recovery testing — the controls enterprise procurement teams probe alongside Security.

CISO/Exec

1. Customer-facing uptime SLA

Published SLA in customer contracts or a public status page promising a specific % monthly uptime (often 99.9%).

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

IT/Ops

2. Capacity + performance monitoring dashboards

Dashboards showing CPU, memory, request-rate, queue depth — with alerting thresholds tuned to the SLA target.

CADENCE: Continuous
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

Engineering

3. Infrastructure-as-code definitions + change history

Terraform / CloudFormation / Pulumi definitions committed to version control with the last quarter of IaC changes.

CADENCE: Weekly
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

Engineering

4. Multi-AZ failover test report

Quarterly failover or game-day test report with the simulated failure, recovery time, and any follow-up remediations.

CADENCE: Quarterly
SAMPLE-SIZE / OBSERVATION WINDOW: 4 artifacts

IT/Ops

5. Backup job success + verification log

Daily / weekly backup job logs with verified successful completion and quarterly restore-into-test-environment evidence.

CADENCE: Continuous
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

Engineering

6. Documented RTO / RPO per service tier

A matrix of every production service with target RTO and RPO, signed by engineering + leadership annually.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

IT/Ops

7. Incident communication procedure + outage postmortems

Documented notification procedure plus postmortems from production incidents with customer-facing status updates.

CADENCE: On change
SAMPLE-SIZE / OBSERVATION WINDOW: 6 artifacts

IT/Ops

8. Disaster recovery plan + annual restore test

Current DR plan with at least one annual cross-region restore exercise and the resulting RTO / RPO measurements.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

3 Processing Integrity (PI1)

TSC PI1.1–PI1.5

Optional TSC. Covers completeness, accuracy, timeliness, and authorization of system processing — most relevant for SaaS where customers care about data accuracy (payments, claims, billing).

Engineering

1. End-to-end data-flow diagram

Diagram of every input !' processing !' output flow for a critical service (payments, claims) with control points labeled.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

Engineering

2. Input validation + rejection sample

Quarterly sample of rejected / anomalous inputs with the validation rules that caught them and the resulting tickets.

CADENCE: Quarterly
SAMPLE-SIZE / OBSERVATION WINDOW: 4 artifacts

Engineering

3. Output reconciliation + variance report

Monthly reconciliation between source-of-truth totals and downstream outputs with variance explanations and sign-offs.

CADENCE: Monthly
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

Engineering

4. Defect / error-rate trend dashboard

Monthly defect / error-rate metrics with the threshold and the customer-visible impact for each incident or anomaly.

CADENCE: Monthly
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

Engineering

5. Processing SLA + service-level scorecard

Published processing SLA (latency, accuracy) and the monthly scorecard showing observed performance vs. target.

CADENCE: Monthly
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

IT/Ops

6. Authorization rules + dual-control for high-risk transactions

Config evidence of dual-control / four-eyes approval for high-risk processing actions (refunds, settlements, account deletions).

CADENCE: Quarterly
SAMPLE-SIZE / OBSERVATION WINDOW: 4 artifacts

4 Confidentiality (C1)

TSC C1.1–C1.2

Optional TSC. Covers protection of confidential information beyond PII — relevant when customers share trade secrets, financial data, or other non-PII sensitive material via your platform.

Security Lead

1. Data classification policy + inventory

Written classification scheme (Public / Internal / Confidential / Restricted) and the inventory of systems holding each tier.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

IT/Ops

2. DLP or access-control export for confidential data

Quarterly ACL / DLP / S3-bucket-policy export showing that confidential data is restricted to least-privilege roles.

CADENCE: Quarterly
SAMPLE-SIZE / OBSERVATION WINDOW: 4 artifacts

Engineering

3. Encryption-key custody + rotation log

Monthly KMS / HSM key-rotation log plus documented key-custody / break-glass procedure for confidential data stores.

CADENCE: Monthly
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

IT/Ops

4. Confidential-data disposal evidence

Quarterly evidence (wipe logs, shred records, certificate-of-destruction) showing confidential data is disposed on schedule.

CADENCE: Quarterly
SAMPLE-SIZE / OBSERVATION WINDOW: 4 artifacts

HR/Legal

5. Confidentiality clauses in customer + vendor contracts

Standard NDA / confidentiality language extracted from customer and vendor contracts, redacted as needed for the auditor.

CADENCE: On change
SAMPLE-SIZE / OBSERVATION WINDOW: 6 artifacts

5 Privacy (P1–P8)

TSC P1–P8

Optional TSC. Covers collection, use, retention, and disposal of personal information per the AICPA Generally Accepted Privacy Principles — the add-on most relevant for SMBs subject to GDPR / CCPA / CPRA.

HR/Legal

1. Privacy notice + consumer-rights URL

Current privacy notice covering collection / use / sharing / retention, plus a public URL describing consumer rights (access, deletion, portability).

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

Privacy/DPO

2. Records of processing activity (RoPA)

Per-article-30 register of personal-data processing activities: data categories, lawful basis, retention, subprocessors.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

Privacy/DPO

3. Data subject access request (DSAR) fulfillment log

Quarterly log of DSARs received, response time, and the data package delivered (access) or deletion confirmation (erasure).

CADENCE: Quarterly
SAMPLE-SIZE / OBSERVATION WINDOW: 4 artifacts

Privacy/DPO

4. Cookie / tracking consent evidence

Monthly export from your consent management platform (OneTrust, Cookiebot) showing consent rates and opt-out evidence.

CADENCE: Monthly
SAMPLE-SIZE / OBSERVATION WINDOW: 12 artifacts

Privacy/DPO

5. Breach notification procedure + tabletop

Documented breach-notification procedure with at least one annual tabletop covering GDPR 72-hour notice obligations.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

HR/Legal

6. Vendor DPA inventory + flow-down evidence

Inventory of vendors with personal data plus evidence of GDPR / CCPA-aligned DPAs in each vendor contract.

CADENCE: Annual
SAMPLE-SIZE / OBSERVATION WINDOW: 1 artifact

Continue the SOC 2 Readiness Journey

This checklist is a companion to the SOC 2 framework hub on cyberstackhub.ai. The hub walks through CC1–CC9 + Availability mappings, the 6-step SMB roadmap, and the Sprinto / Drata / Defendify / Vanta / Secureframe platform comparison. Start with the free Compliance Gap Analysis to pre-score your readiness before paying for a platform.

/soc-2-checklist
The full framework hub — CC1–CC9 + Availability for SMBs

/soc2-compliance-guide
Practical SOC 2 readiness guide (Type I vs Type II, 5 TSCs)

/soc2-gap-analysis
Free 25-item gap analysis with SMB audit-failure patterns

/assess
5-minute SOC 2 / NIST CSF maturity score with top-5 gaps

Sources: AICPA Trust Services Criteria (2017, rev. 2022) — aicpa-cica.com; AICPA SOC 2 Reporting Standard (SSAE 18) — aicpa.org.