SOC 2 Audit Evidence Package Checklist

What to Give Your Auditor - Across All Five Trust Services Criteria

Prepared by Software Secured

How to Use This Checklist

SOC 2 auditors don't just want to know that you ran a pentest. They want to see that your controls are operating - and that when gaps were found, you fixed them. This checklist maps the evidence your auditor will ask for to the specific Trust Services Criteria (TSC) it satisfies.

Work through each section before your audit window closes. Items marked * are the ones auditors most commonly flag as missing.

Before You Start: Scope Confirmation

Before presenting any evidence, confirm your system boundary is documented. Auditors will ask.

- ☐ System description document is current and signed off by management
- ☐ All in-scope components are listed: web application, APIs, cloud infrastructure, authentication systems, third-party integrations
- ☐ The pentest scope document matches the system description (same URLs, IP ranges, environments)
- ☐ * **The pentest was conducted within the audit period (not before it started or after it closed)**
- ☐ * **Testing was performed by an independent third party (satisfies CC4.1 'separate evaluation' requirement)**

Why this matters:

CC4.1 explicitly distinguishes between ongoing evaluations (internal) and separate evaluations (independent third party). An internal team's pentest does not fully satisfy CC4.1. Your auditor will ask whether the firm that tested you is independent of your operations.

1 Security (Common Criteria / CC Series)

Required for all SOC 2 reports. Covers logical access, change management, risk assessment, and monitoring.

CC4 - Monitoring Activities

These controls require you to demonstrate that you actively evaluate whether your security controls are working.

Evidence Item	TSC Control	Status
* Final pentest report (complete, with scope, methodology, findings, and severity ratings)	CC4.1	[ ]
* Retest report or retest attestation confirming critical and high findings were remediated	CC4.1, CC4.2	[ ]
Remediation tracking log showing each finding, assigned owner, remediation date, and retest date	CC4.2	[ ]
Vulnerability scan logs covering the full audit period (not just a point-in-time scan)	CC4.1	[ ]
Documentation that scan and pentest results were communicated to responsible parties	CC4.2	[ ]

Common gap:

Auditors frequently see a pentest report with findings but no retest evidence. The retest attestation - a written confirmation that critical and high vulnerabilities were retested after remediation - is separate from the original report and must be dated within the audit period.

Software Secured note:

Our reports include control mappings and are accompanied by a retest attestation for every engagement. Retesting is available for 12 months after delivery.

CC6 - Logical and Physical Access Controls

These controls require evidence that access to your systems is restricted, monitored, and managed.

Evidence Item	TSC Control	Status
Pentest findings specifically testing authentication controls (MFA, session management, password policies)	CC6.1, CC6.2	[ ]
Evidence of RBAC enforcement - pentest tested privilege escalation and horizontal access control	CC6.3	[ ]
External network pentest report validating perimeter defenses (firewall, WAF, exposed services)	CC6.6	[ ]
Pentest tested for unauthorized data transmission paths or API data exposure	CC6.7	[ ]

Evidence Item	TSC Control	Status
Access provisioning and deprovisioning logs for the audit period	CC6.2	[ ]
Annual access review documentation	CC6.3	[ ]
MFA enforcement evidence (configuration screenshots or policy documentation)	CC6.1	[ ]
TLS configuration review or evidence of encryption in transit	CC6.7	[ ]

> **Common gap:**
> Teams document that MFA is policy but can't show it was tested. Your pentest report should include findings or a pass confirmation on MFA bypass attempts, session token weaknesses, and credential handling.

CC7 - System Operations

These controls require evidence that you monitor for anomalies and respond to security events.

Evidence Item	TSC Control	Status
Vulnerability scan logs showing ongoing scanning (not just the annual pentest)	CC7.1	[ ]
SIEM or IDS/IPS logs showing detection activity during the audit period	CC7.2	[ ]
Evidence that security events were reviewed and acted on	CC7.3	[ ]
Incident response log (even if no incidents occurred, document that the process was tested)	CC7.4	[ ]
Patch management records showing timely remediation of identified vulnerabilities	CC7.1	[ ]

> **Pentest contribution to CC7:**
> If your SIEM or IDS did not generate alerts during the pentest, that is itself a CC7.2 finding - your detection capability did not catch simulated malicious activity. Your pentest report should note whether detection tools fired or not. If they didn't, you need remediation evidence for this control.

CC8 - Change Management

Evidence Item	TSC Control	Status
Change management log or ticketing system records for the audit period	CC8.1	[ ]
Evidence that security testing was included in the SDLC (pre-deployment testing, code review)	CC8.1	[ ]

Evidence Item	TSC Control	Status
Configuration baseline documentation	CC8.1	[ ]

CC9 - Risk Mitigation

Evidence Item	TSC Control	Status
Risk assessment documentation updated within the audit period	CC9.1	[ ]
Vendor security questionnaires or assessments for any third parties with access to your systems	CC9.2	[ ]
Third-party pentesting firm's own SOC 2 report (best practice - demonstrates you assessed your tester)	CC9.2	[ ]
Pentest scope explicitly covered third-party API integrations where they handle or access sensitive data	CC9.2	[ ]

Software Secured note:

We are SOC 2 Type 2 attested. Our report is available on request and can serve as vendor evidence for your CC9.2 documentation.

2 Availability (A1 Series)

Required only if Availability is in scope. Relevant for SaaS companies with uptime SLAs.

Evidence Item	TSC Control	Status
Uptime monitoring logs for the audit period	A1.1	[ ]
Capacity planning documentation	A1.1	[ ]
Backup and recovery procedure documentation	A1.2	[ ]
Backup integrity test results (showing backups were tested, not just created)	A1.2	[ ]
Business continuity / disaster recovery plan	A1.3	[ ]
BCP/DR test results from the audit period	A1.3	[ ]
Pentest included infrastructure testing that validates boundary controls under simulated attack	A1.1, A1.2	[ ]

Common gap:

Most companies have backup procedures documented but cannot show the backups were tested. A1.2 requires evidence of integrity and completeness testing, not just backup creation.

3 Confidentiality (C1 Series)

Required if Confidentiality is in scope. Relevant if you process trade secrets, customer data under NDA, or proprietary business information.

Evidence Item	TSC Control	Status
Data classification policy (defines what is confidential and how it is labelled)	C1.1	[ ]
Data retention schedule with defined retention periods per data type	C1.1	[ ]
Secure disposal procedures (how confidential data is deleted or destroyed at end of retention)	C1.2	[ ]
Pentest tested for unauthorized access to confidential data (IDOR, API data exposure, privilege escalation to confidential records)	CC6.3, C1.1	[ ]
Encryption at rest evidence for confidential data stores	CC6.1, C1.1	[ ]
NDA or confidentiality agreements with vendors who access confidential data	CC9.2	[ ]
Evidence that access to confidential information is restricted to identified purposes	CC6.1	[ ]

Common gap for multi-tenant SaaS:

Auditors will look specifically at whether tenant A can access tenant B's data. Your pentest report should include explicit multi-tenancy isolation testing findings. If it doesn't, flag this to your pentesting vendor before the audit.

4 Processing Integrity (PI Series)

Required if Processing Integrity is in scope. Most relevant for data processing, payments, or analytics services where accuracy of outputs matters.

Evidence Item	TSC Control	Status
Input validation controls documentation (how does the system reject malformed or unauthorized inputs?)	PI1.2	[ ]
Error handling and logging evidence - system records and flags processing errors	PI1.3	[ ]

Evidence Item	TSC Control	Status
Output validation evidence - controls confirming outputs are complete, accurate, and authorized	PI1.4	[ ]
Data integrity testing results (showing that processing produces correct outputs under test conditions)	PI1.3	[ ]
Pentest included business logic testing relevant to processing integrity (e.g., transaction manipulation, race conditions, parameter tampering)	PI1.3	[ ]

Pentest contribution:

Standard web app pentests include input validation testing (injection attacks, parameter tampering) that directly supports PI1.2 and PI1.3. Ensure your pentest report explicitly covers these areas if Processing Integrity is in scope.

5 Privacy (P Series)

Required if Privacy is in scope. Relevant for companies that collect, process, or store personal information.

Evidence Item	TSC Control	Status
Current privacy notice (publicly posted, dated, written in plain language)	P1.1	[ ]
Consent mechanism documentation (how is consent collected and recorded?)	P2.1	[ ]
Data inventory: what personal information is collected, from whom, and for what purpose	P3.1, P6.7	[ ]
Data retention and disposal schedule for personal information	P4.2, P4.3	[ ]
Process for handling data subject access requests (DSARs)	P5.1	[ ]
Vendor/third-party privacy commitments (data processing agreements or DPAs)	P6.4	[ ]
Breach response procedure documentation	P6.6	[ ]
Pentest tested for unauthorized access to personal information (API data leakage, IDOR on user records, PII in logs)	CC6.3, P4.1	[ ]
Privacy training records for personnel with access to personal information	CC2.2	[ ]

Common gap:

Companies collect consent but can't demonstrate what happens to a data subject access request. Auditors want to see a documented process, not just a policy statement.

The Pentest Report Itself: What Auditors Check

Your pentest report is the anchor document for multiple controls. Before submitting it as evidence, confirm it contains:

- [ ] * **Scope definition - confirms all in-boundary systems were tested**
- [ ] * **Methodology description - black box, gray box, or white box; frameworks referenced (OWASP, NIST, ASVS)**
- [ ] * **Finding list with severity ratings (CVSS or equivalent) for every finding**
- [ ] Proof of exploitation for critical and high findings (screenshots, payloads, or attack chain descriptions)
- [ ] Business impact per finding - not just technical severity
- [ ] Remediation recommendations mapped to specific findings
- [ ] * **Retest confirmation - written attestation that critical and high findings were retested after remediation**
- [ ] Tester independence statement - confirms the firm is independent of your operations
- [ ] Control mappings - ideally mapped to SOC 2 TSC controls (CC4.1, CC6.x, CC7.x)

If your report is missing any * items:

Contact your pentesting vendor before submitting to your auditor. Missing retest attestation and scope documentation are the two most common reasons audit evidence is rejected on first submission.

Timing Reference

Activity	Recommended Timing
Schedule annual pentest	Q2 of audit period (leaves time for remediation and retest)
Complete remediation of critical findings	Within 15 days of report delivery
Complete remediation of high findings	Within 30 days of report delivery
Obtain retest attestation	Before audit period closes
Submit evidence package to auditor	At least 2 weeks before audit window closes

What's Not Covered Here

This checklist focuses on penetration testing evidence and directly related controls. The following are also required for SOC 2 but are outside the scope of this document:

- [ ] HR onboarding/offboarding documentation (CC1 controls)
- [ ] Security awareness training records (CC2.2)
- [ ] Board-level risk oversight documentation (CC1.2)
- [ ] Physical access controls and badge logs (CC6.4)
- [ ] Full vendor management programme (CC9.2 - beyond pentest scope)

Ready to Build Your Evidence Package?

If you're preparing for a SOC 2 audit and want to ensure your pentest report will satisfy auditor requirements, our team can help you scope and execute an engagement that produces audit-ready evidence - including control mappings, retest attestation, and Vanta/Drata integration.

Book a consultation: softwaresecured.com/book-a-consultation

Already working with us? Your report and retest evidence are available in the Portal. Your auditor can be granted read-only access directly.