SOC 2

Pentesting Requirements

A practical guide for IT leaders, auditors, and SaaS teams navigating SOC 2 Type 1 and Type 2 compliance requirements, with specific AICPA Trust Services Criteria control references.

Contents

01 Quick Summary

WHAT IT LEADERS NEED TO KNOW

If your organization is pursuing SOC 2 Type 1 or Type 2 attestation, penetration testing is a critical component of demonstrating operational security controls. Here is the simplified version:

AT A GLANCE

- Penetration testing is not explicitly mandated by AICPA, but is expected in practice by most auditors.
- SOC 2 Type 2 requires evidence of controls operating effectively over time - pentests provide that evidence.
- Vulnerability scanning alone is insufficient to satisfy auditor expectations.
- Both internal and external attack surfaces should be tested.
- Web applications, APIs, cloud infrastructure, and access controls are typically in scope.
- Retesting after remediation is expected before the audit period closes.
- Relevant controls span CC4, CC6, CC7, CC9, and A1 Trust Services Criteria.
- Password hygiene, access management, encryption, and network segmentation all have specific control mappings.

02 What Is SOC 2?

BACKGROUND AND CONTEXT

SOC 2 (Service Organization Control 2) is an auditing framework developed by the American Institute of Certified Public Accountants (AICPA). It evaluates whether a service organization's controls meet the Trust Services Criteria (TSC) across five categories:

Trust Services Category	Description
Security (CC)	Core category - required for all SOC 2 reports. Covers logical and physical access, change management, risk assessment, and monitoring.
Availability (A1)	System availability as committed or agreed. Relevant for SaaS uptime SLAs and DR testing.
Processing Integrity (PI)	Complete, valid, accurate, timely, and authorized processing.
Confidentiality (C)	Protection of confidential information.
Privacy (P)	Collection, use, retention, and disposal of personal information.

For most SaaS and cloud service providers, Security (the Common Criteria) is mandatory. The remaining categories are included based on the nature of the service and contractual obligations.

SOC 2 Type 1 vs. Type 2

Report Type	What It Means
SOC 2 Type 1	Point-in-time assessment. Confirms controls are suitably designed as of a specific date. Less demanding - a pentest conducted around the assessment date is typically sufficient.
SOC 2 Type 2	Period assessment (typically 6-12 months). Confirms controls operated effectively throughout the period. Requires ongoing evidence - annual pentesting and continuous monitoring are expected.

03 Required Controls and Pentest Mapping

AICPA TRUST SERVICES CRITERIA WITH PENTESTING RELEVANCE

The AICPA Trust Services Criteria (2017 with 2022 updates) do not use the term "penetration testing" explicitly. Instead, pentesting satisfies multiple points of focus across several criteria. The controls below are drawn directly from the AICPA TSC framework.

CC4 - Risk Assessment

CC4 governs how an organization identifies, analyzes, and responds to risk. Penetration testing is a direct method of operationalizing this requirement.

Control	Description	How Pentesting Satisfies This Control
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Penetration testing is a direct form of 'separate evaluation' that assesses whether security controls are functioning in a real attack scenario. Point of Focus: 'Considers Different Types of Ongoing and Separate Evaluations' - pentest qualifies as a separate evaluation. Auditors commonly cite pentesting as direct evidence for CC4.1.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action.	Pentest reports identify control deficiencies. The formal remediation and retest cycle directly satisfies the requirement to evaluate, communicate, and correct deficiencies.

CC4.1 - AICPA Point of Focus

"Considers Different Types of Ongoing and Separate Evaluations - Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, vulnerability assessments, and other procedures as relevant to identify control deficiencies."

Source: AICPA Trust Services Criteria (2017, with 2022 revisions), CC4.1 Points of Focus

CC6 - Logical and Physical Access Controls

CC6 is the most pentest-relevant criteria family. It covers access controls, authentication, encryption, network segmentation, and data protection.

Control	Description	Pentest Relevance
CC6.1	Logical access security software, infrastructure, and architectures are implemented to protect against threats from sources outside its system boundaries.	External pentest validates perimeter defenses. Tests firewall rules, WAF bypass, VPN weaknesses, exposed services, and authentication mechanisms at the boundary.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity.	Pentest validates access provisioning controls - tests for orphaned accounts, over-privileged users, insecure credential issuance, and unauthorized access paths.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on approved and documented access requests and authorization.	Tests privilege escalation paths, broken access control (IDOR, BOLA), and unauthorized modification of access rights. OWASP Broken Access Control is directly relevant.
CC6.6	Logical access security measures to protect against threats from persons acting outside of entity's system boundaries.	External pentest is the primary control validation method. Tests credential attacks, unauthorized remote access, exposed admin panels, and internet-facing vulnerabilities.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes.	Tests data exfiltration paths, insecure API endpoints, unauthorized data access, and weak authorization on data export functions.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software.	Pentest can include payload delivery simulation to test endpoint defenses, AV evasion, and detection capability for malicious code.

CC7 - System Operations and Monitoring

CC7 requires ongoing detection, response, and recovery capabilities. Pentest findings directly validate whether monitoring and response controls are working.

Control	Description	Pentest Relevance
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify changes to configurations or new vulnerabilities.	Vulnerability scanning and pentest findings surface undetected configuration drift and new attack vectors. Pentest validates that detection tools actually catch malicious activity.

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives.	Pentest simulates malicious activity - if SIEM/IDS alerts don't fire during a test, that's a CC7.2 finding. Red team exercises are particularly relevant here.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives and, if so, takes actions to prevent or address such failures.	Pentest report constitutes a formal security event evaluation. The remediation process maps directly to this control.

CC9 - Risk Mitigation

Control	Pentest Relevance
CC9.1 - Risk mitigation activities	Pentest is a core risk mitigation activity. The formal test-remediate-retest cycle directly demonstrates risk reduction to auditors.
CC9.2 - Vendor and business partner risk	Third-party component testing (APIs, SDKs, cloud services) validates that vendor risk is assessed through practical security testing, not just questionnaires.

A1 - Availability Criteria

Control	Pentest Relevance
A1.1 - Capacity planning	Infrastructure testing validates that capacity controls hold under simulated attack conditions (e.g., resource exhaustion testing).
A1.2 - Environmental protections	Testing of boundary controls and redundant paths supports availability assurance evidence.
A1.3 - Recovery testing	Disaster recovery and failover testing is distinct from pentesting but often scoped alongside it for SOC 2 Type 2 engagements.

04 Highlighted Control Areas

SPECIFIC SECURITY TOPICS WITH TSC CONTROL MAPPINGS

The following areas are specifically called out in the AICPA Trust Services Criteria with direct or indirect references to technical controls. Each maps to one or more points of focus that penetration testing or security assessments can satisfy.

Password Hygiene

RELEVANT CONTROLS: CC6.1, CC6.2, CC6.3

The AICPA Trust Services Criteria reference authentication strength under CC6.1 and CC6.2. Points of Focus include: 'Identifies and Authenticates Users' and 'Manages Credentials.' Pentesting validates: default credentials, weak password policies, password reuse, brute force protections, MFA bypass, session token weaknesses, and credential stuffing resistance.

Control Point	What Testers Should Validate
CC6.1 - Credential strength	Password complexity enforcement, lockout policies, MFA implementation, session expiry
CC6.2 - Credential issuance	Secure onboarding flows, temporary credential handling, password reset vulnerabilities
CC6.3 - Credential removal	Offboarding flows, orphaned accounts, stale service accounts with privileged access

Access Management

RELEVANT CONTROLS: CC6.2, CC6.3, CC6.6

The AICPA specifically identifies 'least privilege' and 'role-based access' as points of focus under CC6.2 and CC6.3. Access management testing is one of the most frequently cited pentest areas in SOC 2 audits. Pentesting validates: privilege escalation, horizontal/vertical access control bypass, IDOR vulnerabilities, over-privileged service accounts, and admin interface exposure.

Control Point	What Testers Should Validate
CC6.2 - Access provisioning	Role-based access control (RBAC), least privilege enforcement, access request validation
CC6.3 - Authorization controls	Broken access control (OWASP A01), IDOR, object-level authorization failures
CC6.6 - Remote access	VPN security, admin interface exposure, remote desktop protocols, cloud console access

Vulnerability Management

RELEVANT CONTROLS: CC4.1, CC7.1, CC7.2

CC4.1 explicitly mentions vulnerability assessments in its points of focus alongside penetration testing. CC7.1 requires ongoing detection of new vulnerabilities and configuration changes. Vulnerability scanning satisfies CC7.1 ongoing detection. Penetration testing satisfies CC4.1 separate evaluation. Both are required - scanning alone does not meet the separate evaluation standard.

Activity	Control Satisfied

Vulnerability scanning (monthly/quarterly)	CC7.1 - Ongoing monitoring and detection
Annual penetration test	CC4.1 - Separate evaluation; CC6.1, CC6.6 validation
Remediation tracking and retesting	CC4.2 - Deficiency communication and correction
Patch management evidence	CC7.1 - Timely remediation of identified vulnerabilities

Third-Party Assessments

RELEVANT CONTROLS: CC9.2, CC4.1

CC9.2 requires the entity to assess vendor and business partner risk. The AICPA points of focus under CC9.2 include: 'Considers the Significance of the Risk Posed' and 'Conducts Ongoing Monitoring.' Third-party pentesting satisfies both the independence requirement under CC4.1 and the vendor assessment program expectation under CC9.2. Using an independent pentesting firm is strongly preferred by auditors.

Scenario	Relevant Control
Internal team conducting their own pentest	Does NOT satisfy CC4.1 independence requirement for 'separate evaluation'
Third-party pentesting firm engaged annually	Satisfies CC4.1 (separate evaluation) and demonstrates vendor risk assessment maturity
Third-party SaaS APIs in scope	CC9.2 - Vendor components should be in scope where they handle or access sensitive data
Pentest firm's own SOC 2 report on file	Best practice - demonstrates due diligence on the tester themselves

Network Segmentation

RELEVANT CONTROLS: CC6.1, CC6.6, CC6.7

The AICPA points of focus under CC6.1 include: 'Restricts Access to Information Assets' and 'Manages Points of Access.' Network segmentation testing validates that internal boundaries actually prevent lateral movement between environments. Pentesting validates: VLAN hopping, inter-segment traffic controls, production vs. dev/test isolation, cloud VPC segmentation, and internal firewall rule effectiveness.

Testing Area	SOC 2 Relevance
Production vs. development network isolation	CC6.1, CC6.6 - boundary protection between environments
Cloud VPC and subnet controls (AWS/Azure/GCP)	CC6.1 - logical segmentation of cloud infrastructure
Lateral movement testing from compromised host	CC6.7 - restricts unauthorized movement of data/access
Internal firewall and ACL validation	CC6.6 - perimeter and internal boundary effectiveness

Data Segregation

RELEVANT CONTROLS: CC6.3, CC6.7, C1.1 (Confidentiality)

Data segregation - separating different tenants, customers, or data classifications - is tested under CC6.3 (authorization controls) and CC6.7 (information movement restrictions). For multi-tenant SaaS, this is a critical area of auditor scrutiny. Pentesting validates: tenant isolation (cross-tenant data access), customer data boundary controls, data classification enforcement, and unauthorized data access paths.

Testing Area	SOC 2 Relevance
Multi-tenant data isolation testing	CC6.3 - authorization ensures tenant A cannot access tenant B data
Database access control testing	CC6.7 - restricts unauthorized removal or access to stored data
API data boundary testing	CC6.3, C1.1 - API responses limited to authorized data only
Logging and audit trail segregation	CC7.2 - monitoring data integrity across tenants

Encryption

RELEVANT CONTROLS: CC6.1, CC6.7, C1.2 (Confidentiality)

The AICPA points of focus under CC6.1 include: 'Uses Encryption to Protect Data.' CC6.7 covers encryption of data in transit. The Confidentiality category (C1.2) explicitly requires encryption for confidential data. Pentesting validates: TLS configuration, cipher suite strength, certificate validity, data-in-transit encryption, encryption key exposure, insecure storage of sensitive data, and cleartext credential transmission.

Testing Area	SOC 2 Relevance
TLS/SSL configuration review	CC6.1, CC6.7 - validates transport encryption strength and configuration
Cleartext credential detection	CC6.1 - 'Uses Encryption to Protect Data' point of focus
Sensitive data in API responses	CC6.7, C1.2 - confidential data should not be unnecessarily exposed
Encryption key management testing	CC6.1 - key exposure or weak key management is a direct control failure
Database encryption validation	C1.2 - data at rest encryption for confidential information

Isolation (Environment and Compute)

RELEVANT CONTROLS: CC6.1, CC6.6, A1.1

Environment isolation - particularly between production and non-production systems - is referenced under CC6.1 as a boundary protection requirement. Compute isolation in containerized and cloud environments is increasingly in scope for SOC 2 Type 2 audits. Pentesting validates: container escape vulnerabilities, hypervisor isolation, cloud metadata service access, environment variable leakage, and production/staging boundary controls.

Testing Area	SOC 2 Relevance
Container escape testing (Docker/Kubernetes)	CC6.1 - boundary protection; CC6.6 - external threat protection
Cloud metadata service exposure (SSRF/IMDS)	CC6.6 - protects against external threats exploiting cloud misconfigurations
Staging/production environment separation	CC6.1 - restricts access; prevents dev credentials reaching production
Serverless function isolation	CC6.1 - function-level access control and isolation validation

05 Pentest Scope for SOC 2

WHAT SHOULD BE IN SCOPE?

SOC 2 scope is defined by the system boundary documented in the service organization's description of its system. In practice, any component that stores, processes, or transmits data covered by the Trust Services Criteria should be included.

Component	Typical Testing Focus	Relevant TSC
External Perimeter	Public-facing assets, IP ranges, DNS infrastructure, exposed services	CC6.1, CC6.6
Web Application and APIs	Authentication, authorization, business logic, data exposure, OWASP Top 10	CC6.1-6.3, CC6.6-6.7
Internal Network	Segmentation validation, lateral movement, internal service exposure	CC6.1, CC6.6, CC6.7
Cloud Infrastructure	AWS/Azure/GCP config review, IAM misconfigurations, storage exposure, metadata access	CC6.1, CC6.6
Authentication Systems	SSO, MFA, password policies, session management, OAuth/OIDC flows	CC6.1, CC6.2
Third-Party Integrations	API keys, webhook security, external service trust boundaries	CC9.2, CC6.7

Admin Interfaces	Admin panel exposure, privilege escalation, audit trail integrity	CC6.2, CC6.3, CC7.2

What SOC 2 Does Not Explicitly Require

The following are not directly mandated, though auditors may ask about them depending on scope:

- Mobile application pentesting (unless mobile apps are in scope).
- Source code review or SAST (though commonly recommended).
- Social engineering campaigns (relevant if CC1 culture controls are in scope).
- Physical security testing (unless physical access controls are in the system boundary).
- Formal red team exercises (recommended but not required for SOC 2, unlike FedRAMP).

06 Type 1 vs. Type 2: What Changes?

PENTEST REQUIREMENTS BY REPORT TYPE

Aspect	SOC 2 Type 1	SOC 2 Type 2
Pentest timing	Single pentest near assessment date sufficient.	Annual pentest covering the audit period. Evidence must be within the period.
Remediation evidence	Findings identified; remediation plan acceptable.	Evidence of remediation and retesting expected within the period.
Vulnerability scanning	Snapshot scan acceptable.	Ongoing scanning program with logs covering the period required.
Monitoring evidence	Controls designed to detect - described in system description.	Controls actually operated throughout the period - evidence required.
Report deliverable	Pentest report as point-in-time evidence.	Pentest report + remediation evidence + retest confirmation + scan logs.

KEY INSIGHT FOR TYPE 2

SOC 2 Type 2 covers an audit period - typically 6 to 12 months. A pentest conducted before the period begins or after it ends provides weak evidence. Auditors expect the pentest to fall within the period, with remediation evidence and retest confirmation also dated within the period. Best practice: Schedule your annual pentest in Q2 of your audit period to allow time for remediation and retesting before the period closes.

07 What Auditors Expect in Practice

COMMON EXPECTATIONS FROM SOC 2 AUDITORS

TYPICALLY EXPECTED	COMMONLY RECOMMENDED

- Annual penetration test (internal + external) - Web application and API pentest - Cloud configuration review (AWS / Azure / GCP) - Vulnerability scanning program with logs - Remediation retest before the period closes - Pentest conducted by independent third party - Formal pentest report with risk ratings and remediation guidance	- Regular segmentation validation testing - Encryption configuration review (TLS/cipher suites) - Access control testing including privilege escalation - Detection and response validation exercises - Third-party API security testing - Annual password policy and authentication review

What a Compliant Pentest Report Should Include

Auditors reviewing pentest evidence for SOC 2 will look for the following in the pentest report:

- Scope definition confirming all in-boundary systems were tested.
- Methodology description (black box, gray box, white box).
- Finding details with severity ratings (CVSS or equivalent).
- Proof of exploitation (screenshots, payloads, attack chains).
- Business impact per finding - not just technical severity.
- Remediation recommendations mapped to specific findings.
- Retest confirmation that critical and high findings were remediated.
- Tester independence statement (firm is not the service organization).

08 Do Pentesters Need to Be Independent?

INDEPENDENCE REQUIREMENTS FOR SOC 2 PENTESTING

Unlike FedRAMP, SOC 2 does not require the use of an AICPA-accredited third party for pentesting. However, the independence expectation is strong in practice.

SHORT ANSWER

Yes - in practice. The AICPA CC4.1 point of focus explicitly distinguishes between 'ongoing' evaluations (performed internally) and 'separate' evaluations (performed independently). Auditors view internal pentest teams as satisfying only the 'ongoing' evaluation standard. An independent third party is expected to satisfy the 'separate evaluation' requirement that most directly supports CC4.1 compliance.

What the Framework Requires

- The evaluator must be independent from the team that designed and operates the controls.
- Internal audit functions may qualify if sufficiently independent (separate reporting line).
- The assessment should be documented and provide objective evidence.
- No AICPA accreditation equivalent to FedRAMP's 3PAO requirement exists for SOC 2 pentesting.

Practical Guidance

Scenario	Auditor View
Internal security team performs pentest	Accepted as 'ongoing evaluation' only - does not fully satisfy CC4.1 separate evaluation expectation
Independent third-party firm performs annual pentest	Strongly preferred - satisfies CC4.1 separate evaluation; provides objective evidence
Bug bounty program results	Supplementary only - not a substitute for structured pentest with formal report
Automated scanner with no manual testing	Not accepted as penetration testing - scanning does not equal testing
Pentesting firm is offshore or non-U.S.-based	Acceptable for SOC 2 - no geographic restriction (unlike some FedRAMP agency requirements)

09 Resources

SOC 2 AND PENTESTING COMPLIANCE REFERENCES

AICPA: Trust Services Criteria (2017, 2022 revisions) aicpa-cima.com

Primary source for all Trust Services Criteria including CC4, CC6, CC7, CC9. Required reading before any SOC 2 pentest scoping discussion.

AICPA: SOC 2 Guide for Service Organizations aicpa-cima.com

Official practitioner guidance on implementing and evidencing controls for SOC 2. Covers what auditors look for in pentest evidence.

Software Secured: NIST SP 800-115 and Pentesting softwaresecured.com

Explains how the NIST SP 800-115 technical pentesting standard relates to compliance frameworks including SOC 2.

OWASP Testing Guide (v4.2) owasp.org

The most widely referenced methodology for web application and API pentesting. Directly relevant to CC6 control testing.

Cloud Security Alliance: SOC 2 and Cloud cloudsecurityalliance.org

Maps SOC 2 controls to cloud-specific risks. Useful for scoping AWS, Azure, and GCP pentests within SOC 2 boundaries.