WHITE PAPER

What is SOC 2?

A Complete Guide

Understand SOC 2: its origin, the five Trust Service Criteria, Type I vs. Type II distinctions, how to prepare for an audit, and why SOC 2 compliance is now a de facto requirement for SaaS companies serving enterprise customers.

Version 1.0

Prepared By Lorikeet Security

lorikeetsecurity.com

OVERVIEW

1. Executive Overview

SOC 2 (System and Organization Controls 2) is a reporting framework developed by the American Institute of CPAs (AICPA) that evaluates whether a service organization's controls effectively protect the security, availability, processing integrity, confidentiality, and privacy of customer data. For SaaS companies, fintech providers, and technology service organizations, SOC 2 has become the de facto security attestation required by enterprise buyers during vendor due diligence.

> **Key Distinction: SOC 2 is an Attestation, Not a Certification**
>
> SOC 2 is not a certification — it is an auditor attestation. A licensed CPA firm reviews your controls and issues a formal opinion. The report itself is what customers and prospects receive.

HISTORY

2. Background and History

SOC 2 was developed by the AICPA as part of the Service Organization Controls reporting suite. It replaced the older SAS 70 standard and was designed specifically for technology and cloud service providers where traditional financial auditing frameworks were insufficient.

Year	Milestone
Pre-2010	SAS 70 used as a general-purpose service organization report. Not designed for IT controls or cloud services.
2010	AICPA introduces the SOC framework. SOC 1 replaces SAS 70 for financial reporting controls. SOC 2 introduced for service organizations with security-relevant controls.
2011	SOC 2 reporting framework formally available. Trust Services Criteria (TSC) published.
2016	SOC 2 + criteria updated. AICPA revises the Trust Services Criteria to align with COSO 2013 Internal Control Framework.
2017	Updated Trust Services Criteria become effective for reports covering periods beginning on or after December 15, 2018.
Present	SOC 2 Type II is the standard expectation for SaaS companies in enterprise sales cycles. Security criteria mandatory; others optional.

TSC

3. The Five Trust Service Criteria

SOC 2 is built around five Trust Service Criteria (TSC). Security is the only mandatory category. Organizations select additional categories based on customer commitments and service type.

Criteria	Required?	Description
Security (CC)	MANDATORY	Protection of system resources against unauthorized access. Covers logical access, encryption, monitoring, incident response, and change management. Mapped across 9 Common Criteria (CC1–CC9).
Availability (A)	Optional	System availability meets committed service levels. Covers performance monitoring, capacity planning, disaster recovery, and backup procedures.
Processing Integrity (PI)	Optional	System processing is complete, accurate, timely, and authorized. Relevant for transaction processing systems, financial platforms, and data pipelines.
Confidentiality (C)	Optional	Information designated as confidential is protected. Covers data classification, encryption, and access restrictions on confidential data.
Privacy (P)	Optional	Personal information is collected, used, retained, and disclosed according to commitments and privacy notice. Aligned to the AICPA Privacy Management Framework.

TYPE I VS II

4. SOC 2 Type I vs. Type II

Attribute	Type I	Type II
What It Covers	Controls are suitably designed at a point in time.	Controls are suitably designed AND operating effectively o
Audit Period	Single point in time (no testing period).	Minimum 6 months; typically 6–12 months.
Time to Obtain	6–12 weeks after controls are in place.	6–12 months from program start.
Customer Value	Demonstrates control design. Useful for early-stage.	Demonstrates operating effectiveness. Enterprise standard
Cost	Lower audit cost; less evidence collection.	Higher audit cost; continuous evidence required.
Use Case	New programs, early-stage companies, immediate sales need.	Mature security programs, enterprise procurement, establis

COMMON CRITERIA

5. The Security Common Criteria (CC1–CC9)

Criteria	Focus Area
CC1	Control Environment: Board oversight, organizational structure, competence, accountability, and ethical values.
CC2	Communication and Information: Internal and external communications about security responsibilities and incidents.
CC3	Risk Assessment: Identification and analysis of risks to achieving security commitments and requirements.
CC4	Monitoring Activities: Ongoing and separate evaluations to determine whether controls are present and functioning.
CC5	Control Activities: Actions taken to address risks, including policies, procedures, and technology controls.
CC6	Logical and Physical Access Controls: Restricts access to systems, data, and facilities. Includes MFA, privilege management, and encryption.
CC7	System Operations: Monitors for security events, responds to incidents, and remediates vulnerabilities.
CC8	Change Management: Controls changes to systems and applications, including testing, approval, and documentation.
CC9	Risk Mitigation: Manages risks from vendors, business partners, and other external parties.

PENTEST ROLE

6. The Role of Penetration Testing in SOC 2

Penetration testing is not explicitly mandated by SOC 2, but it provides critical evidence for multiple Trust Service Criteria — particularly CC7 (System Operations) and CC6 (Logical Access). Auditors from Accorp Partners CPA and other qualified firms expect to see documented evidence of vulnerability testing as part of a mature SOC 2 program.

TSC Reference	How Penetration Testing Provides Evidence
CC7.1	Detects security events: penetration testing identifies exploitable vulnerabilities, demonstrating systematic detection capability.
CC7.2	Responds to vulnerabilities: documented remediation of pentest findings demonstrates an operational vulnerability response process.
CC6.6	Boundary protection testing: external network and web application testing validates perimeter controls.

TSC Reference	How Penetration Testing Provides Evidence
CC4.1	Ongoing monitoring: recurring annual testing demonstrates continuous security evaluation as a monitoring activity.
CC9.2	Vendor risk: if third-party APIs or integrations are in scope, testing demonstrates vendor-connected risk assessment.

PREPARATION

7. Preparing for a SOC 2 Audit

- Define scope: Identify which systems, services, and data are in-scope for the audit. Narrower scope = lower cost and faster timeline.
- Select Trust Service Criteria: Most SaaS companies start with Security (CC) only. Add Availability or Confidentiality based on customer commitments.
- Implement required controls: Address CC6 (access management, MFA, encryption), CC7 (monitoring, incident response), and CC8 (change management) first.
- Use a compliance automation platform: Tools like Vanta or Drata (Lorikeet is a partner of both) automate evidence collection across 35+ frameworks.
- Commission a penetration test: Obtain a current penetration test report before the audit window. Remediate findings and get an attestation letter.
- Engage your auditor early: Work with your CPA firm (such as Accorp Partners CPA, Lorikeet's audit partner) to define the audit timeline and evidence requirements.

BUSINESS VALUE

8. Business Value of SOC 2

Benefit	Description
Enterprise Sales Unlock	SOC 2 Type II is a prerequisite for enterprise deals in financial services, healthcare, and SaaS. Without it, deals stall in security review.
Vendor Qualification	Procurement teams use SOC 2 to qualify vendors without running custom security assessments, accelerating onboarding.
Trust Demonstration	Customers share a SOC 2 report in lieu of answering security questionnaires, reducing friction in the sales process.
Regulatory Alignment	SOC 2 controls overlap significantly with HIPAA, PCI DSS, ISO 27001, and GDPR, making multi-framework compliance more efficient.

Benefit	Description
Cyber Insurance	SOC 2 Type II is increasingly used as a positive underwriting signal by cyber insurers, contributing to lower premiums.

HOW WE HELP

9. How Lorikeet Security Supports SOC 2

Lorikeet Security is purpose-built for SOC 2 penetration testing. Our reports are specifically formatted for compliance auditors, with executive summaries and risk ratings mapped to Trust Service Criteria. We partner with Accorp Partners CPA for combined pentest + audit engagements and Vanta/Drata for compliance automation integration.

- SOC 2-mapped reports: Findings annotated with CC references accepted by auditors on the first submission.
- Pentest + Audit bundle: Lorikeet handles testing. Accorp Partners CPA delivers attestation. One intake call, unified timeline.
- Compliance platform integration: Works directly with Vanta and Drata evidence workflows.
- Free retest included: Fix the issues, we verify and update the report — no additional cost within 30 days.

Get Started with SOC 2

Contact Lorikeet Security at lorikeetsecurity.com or call (689) 202-3940 to discuss SOC 2 penetration testing, the pentest + audit bundle with Accorp Partners CPA, or compliance automation with Vanta and Drata.