SOC 2: Demonstrating Trust in Service Organizations

SOC 2 (System and Organization Controls) is a framework developed and maintained by the American Institute of Certified Public Accountants (AICPA). The framework establishes controls designed to help service organizations protect the security, availability, processing integrity, confidentiality, and privacy of sensitive information.

SOC 2 Compliance and Pentesting

While SOC 2 is a voluntary framework and never a legal requirement, certification has become widely regarded as proof that a company has taken appropriate measures to protect customer data. Many security-conscious companies, especially those providing cloud or Software-as-a-Service (SaaS), require SOC 2 compliance from their partners' accountants.

SOC 2 requires companies to have a formal process to identify, track, and resolve security vulnerabilities. Pentesting plays a vital role in validating this process:

- **Independent evaluation:** SOC 2 specifically mentions pentesting under CC4.1 COSO Principle 16, which states that management should use "a variety of different types of ongoing and separate evaluations, including penetration testing ... and internal audit assessments."
- **Key audit artifact:** A pentest report is considered a key artifact for demonstrating due diligence to auditors, proving that process controls are rigorously tested.
- **Comprehensive findings:** Since compliance requires identifying security vulnerabilities, manual pentesting is essential for discovering more complex issues, such as business logic or chained exploits, that automated scanners typically miss.

Type I vs. Type II Audits

When pursuing SOC 2 compliance, organizations must choose between a Type I and a Type II audit, which determines how controls are evaluated:

- **SOC 2 Type I Audit:** Attests to the design and implementation of controls at a single point in time.
- **SOC 2 Type II Audit:** Attests to the design, implementation, and operating effectiveness of controls over a period of time, usually three to 12 months.

A Type II audit generally provides a greater level of trust to customers because it verifies that controls operated effectively over a duration. Integrating continuous pentesting into the development lifecycle ensures organizations maintain the strong compliance posture needed to satisfy the scrutiny of a Type II audit.

See how Cobalt helps Labforward comply with SOC 2

READ CASE STUDY

About Cobalt

Cobalt is the pioneer in pentesting as a service (PTaaS) and a leader in offensive security services.

We are focused on combining talent and technology with speed, scalability, and expertise. Thousands of customers and hundreds of partners rely on the Cobalt Offensive Security Platform, along with the industry's largest exclusive community of 450+ trusted pentesters and security experts, to find and fix vulnerabilities across their environments. By enabling faster pentest launches, real-time collaboration with testers, continuous scanning, and seamless integration with remediation workflows, we help organizations identify critical issues and accelerate risk mitigation so they can operate fearlessly and innovate securely.

Book a demo to see how Cobalt can help you achieve compliance and build your offensive security program.

BOOK A DEMO