SOC 2

Implementation & Assessment Capabilities

Independent. Auditor-Ready. Customer-Trusted.

Cybernion

www.cybernion.com | info@cybernion.com

What is SOC 2?

SOC 2 is an attestation report, defined by the AICPA, on the design and operating effectiveness of controls relevant to the Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. The report is issued by an independent CPA firm and is widely used to evidence security to customers.

Attestation Requirement

Service organisations handling customer data are frequently required to provide a SOC 2 report, issued by an independent CPA firm, before enterprise customers will contract with them.

A Type I report covers a point in time; a Type II report covers operating effectiveness over a period, typically three to twelve months.

1 **Effectiveness Over Time**

A Type II report tests whether controls operated effectively across the review period, not just on a single day.

2 **You Choose the Criteria**

Security is mandatory. Availability, Confidentiality, Processing Integrity, and Privacy are included only if in scope.

3 **Attestation, Not Certification**

SOC 2 results in an auditor's attestation report, not a pass or fail certificate. A CPA firm issues the opinion.

Why SOC 2?

Compliance & Risk

Provides independent assurance over controls relevant to the Trust Services Criteria

Market Access

Frequently required by enterprise and North American customers before contracting

Security Maturity

Structured uplift of Security, Availability, and Confidentiality controls

Sales Enablement

Shortens security reviews and unblocks stalled enterprise deals

Credibility & Trust

Independently demonstrates disciplined control over customer data

Our SOC 2 Services

A holistic service across Advisory, Readiness, and Assessment with independence between readiness and audit roles.

SOC 2 Advisory

- Readiness gap analysis
- Trust Services Criteria scoping
- Control design and guidance
- Auditor selection support
- Type I vs Type II strategy

SOC 2 Readiness

- Control implementation
- Evidence collection & management
- Documentation (policies, SOPs)
- Staff training and awareness
- Continuous control monitoring

SOC 2 Assessment

- Independent readiness assessment
- Control testing & verification
- Risk analysis across the criteria
- SOC 2 Readiness Report
- Controls Matrix

SOC 2 Readiness Process

Four stages, leading into an independent audit and periodic Type II reporting.

1 Plan & Prepare

- Define scope, criteria & timeline
- Identify key security personnel
- Establish communication process
- Review existing documentation

2 Scope Definition

- Map systems, services & data flows
- Select applicable Trust Services Criteria
- Agree control set & boundaries
- Define evidence requirements

3 Assess

- Control testing and walkthroughs
- Verification against the criteria
- Risk analysis across each service
- Evidence and gap review

4 Report

- SOC 2 Readiness Report
- Controls Matrix
- Detailed findings & recommendations
- Pathway to Type II attestation

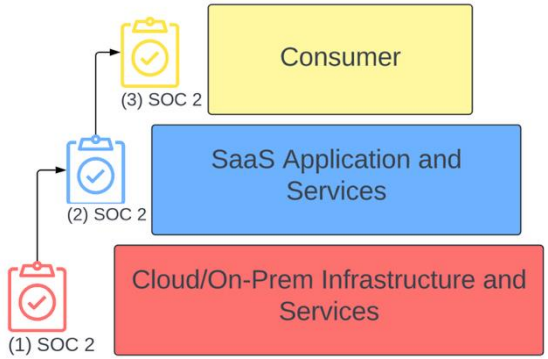
Case Study 1 - SOC 2 Assessment

A B2B fintech engaged us to conduct a SOC 2 readiness assessment ahead of its first Type II audit, covering its AWS-hosted platform, corporate systems, and customer onboarding operations.

Requirements

- Assess the design and operating effectiveness of controls across the AWS platform and corporate systems against the Security and Availability criteria
- Assess the security of customer onboarding operations that handle personal and financial data
- Provide recommendations to close gaps and improve readiness for the Type II audit

Our Solution



By testing controls against the Trust Services Criteria and reviewing real evidence, we gave the fintech a clear view of its readiness and a prioritised set of actions to close before its first Type II audit.

Key Highlights

- **Plan and Prepare:** Define clear objectives, timeline, and comms process
- **Define the Scope:** Scope the assessment to cover the AWS platform, corporate systems, and onboarding operations
- **Assess:** Conduct control walkthroughs, testing, and risk analysis against the selected criteria
- **Report:** A detailed readiness report and controls matrix highlighting strengths and gaps to close before the audit

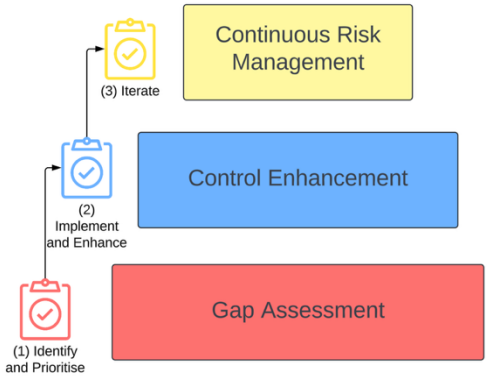
Case Study 1 - SOC 2 Readiness

A SaaS scale-up needed to achieve a SOC 2 Type II report to unblock enterprise deals, requiring it to design and operate a control environment across its product and corporate systems.

Requirements

- Design and operate a control environment aligned to the Security and Confidentiality criteria
- Ensure controls operate consistently across product and corporate systems over the review period
- Prepare for an independent Type II audit with robust, repeatable evidence
- Establish repeatable evidence collection and management to support recurring reports

Our Solution



A comprehensive gap analysis identified where practice fell short of the criteria, followed by control implementation and continuous monitoring so the scale-up could operate controls across the period and pass its Type II audit.

Key Highlights

- **Gap Analysis:** A comprehensive assessment to identify gaps between current practice and the Trust Services Criteria
- **Control Implementation:** Design and implement controls across product, infrastructure, and corporate systems
- **Continuous Monitoring:** Monitoring mechanisms to sustain control operation across the Type II review period
- **Documentation and Training:** Detailed documentation and staff training to support the new controls and audit

Important SOC 2 Artefacts

The documents your auditor will examine, and what you receive in return.

Input: What You Provide

SYS	System Description
TSC	Trust Services Criteria Mapping
RA	Risk Assessment
ISP	Information Security Policy
IRP	Incident Response Plan
BCP	Business Continuity Plan
SOPs	Standard Operating Procedures
VMP	Vendor Management Policy
CHG	Change Management Policy
ACP	Access Control Policy

+ Other policy and process documents as agreed during scoping.

Output: What You Receive

1 SOC 2 Readiness Report

A comprehensive evaluation of control design and operating effectiveness against the Trust Services Criteria, covering identified gaps and their severity, with remediation guidance.

2 Controls Matrix

A structured mapping of controls to the Trust Services Criteria, showing coverage and evidence, forming the backbone of the independent audit.

Thank You

Ready to start your SOC 2 journey? Let's talk.

Web www.cybernion.com

FAQs www.cybernion.com/insights

Email info@cybernion.com

Phone 0404 760 923

A Trusted Cyber Companion