PENTESTERRA

SOC 2 GAP ASSESSMENT

Would Your SOC 2 Report Hold Up to a US Client?

Gap assessment across 51 SOC 2 controls - Common Criteria CC1-CC9 plus the additional categories - for SaaS and B2B service providers selling to enterprise clients.

IN SHORT

Covers all Common Criteria CC1-CC9 (33 controls, always in scope) plus the 4 additional categories - Availability, Confidentiality, Processing Integrity, Privacy - included only where your service commitment covers them.

51
SOC 2 controls covered (CC1-CC9 + additional categories)

33
Common Criteria always in scope

US / Global
Standard demanded by US enterprise clients

THE SITUATION TODAY

WHO YOU ARE
You're the CISO or security lead of a SaaS or B2B service provider selling - or trying to sell - to enterprise clients that require a SOC 2 report before signing.

WHAT HAPPENED
An enterprise prospect has made SOC 2 Type II a contractual condition, and the audit with the external auditor is coming up.

WHY IT HURTS
Without evidence ready across all 51 controls, the external auditor finds gaps during the audit itself - the most expensive and visible moment to discover them.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME	You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.
THE SOLUTION	Pentesterra's SOC 2 Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.
WHY IT'S DIFFERENT	You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.
CONCRETE PROOF	The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of SOC 2, grouped the way you'll see them in the platform.

CC1-CC5: Environment and risk assessment

The foundations of the internal control system.

- Control environment and organizational culture
- Communication and information
- Risk assessment and control activities

CC6-CC9: Access, operations, change

The day-to-day operational controls most technically verifiable.

- Logical and physical access to systems
- System operations and monitoring
- Change management and risk mitigation

Additional category: Availability and Confidentiality

Included only where your service commitment covers them.

- System availability per SLA commitments
- Protection of confidential information

Additional category: Processing Integrity and Privacy

The categories most relevant to SaaS platforms with sensitive data.

- Data processing integrity (complete, accurate, timely)
- Privacy principles P1-P8

PENTESTERRA

SOC 2 GAP ASSESSMENT

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for SOC 2

A complete report, ready to present to clients, auditors, or your board.

Request your SOC 2 Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance