

SOC 2 Pentest Checklist

What your auditor expects, and how to be ready. One page, no fluff.

1. DEFINE THE SCOPE

- ☐ **Map your SOC 2 system boundary:** web app, API, cloud infrastructure, admin panels
- ☐ List what is **out of scope** and why (your auditor will ask)
- ☐ Write down your **audit window dates** (Type II: test early in the observation period)
- ☐ Identify crown-jewel data flows: where customer data enters, moves, and is stored

2. WHAT THE AUDITOR EXPECTS

- ☐ **Independent manual testing** by an external party (CC4.1, CC7.1), not a scanner export
- ☐ A report where **every finding references the Trust Services Criterion** it affects
- ☐ **Remediation evidence:** findings fixed and confirmed by a retest (CC7.3)
- ☐ Testing that covers access control and tenant boundaries (CC6.1, CC6.6)

3. BEFORE THE TEST

- ☐ Decide: production or staging environment (and get it approved internally)
- ☐ Prepare **test accounts at every role level**, including admin
- ☐ Agree on rules of engagement: allowed hours, forbidden actions, escalation contact
- ☐ Freeze major releases during the testing window

4. AFTER THE TEST

- ☐ Assign every finding an owner and a fix date
- ☐ Get a **retest report** confirming each fix, this is your closure evidence
- ☐ File the report, retest confirmation and remediation tickets together for the auditor
- ☐ Set the next annual test date now

Timeline benchmark: a scoped manual pentest takes 2-4 weeks from kickoff to an audit-ready report, including remediation guidance and a free retest. Plan backwards from your audit date.