Pentest scoping checklist

The questions a serious vendor will ask you anyway, answered before the first call. A penetration test is priced from its scope: what's being tested, from what position, to produce what evidence. Fill this in with the team that owns each answer, and every quote you receive gets sharper, whoever you're evaluating.

01 Inventory the attack surface

Effort follows attack surface, so a real quote requires understanding yours. List what exists before deciding what's in scope.

- [ ] **Web applications and thick clients** in scope: names, URLs, and the environments they run in
- [ ] **APIs**: specifications or collections (e.g. Swagger/OpenAPI) you can share, plus any endpoints consumers use that aren't documented
- [ ] **Mobile apps**: platforms and builds, and where the app's backend boundary sits
- [ ] **Network scope**: external ranges, internal segments, and which perspective (outside, inside, or both) you need tested
- [ ] **Cloud estate**: accounts, services, and the data flows between them
- [ ] **Explicitly out of scope**: the systems a tester must not touch, written down

02 Roles, tenants, and access

Findings depend on the position the tester starts from. Decide what access you'll grant and which boundaries matter.

- [ ] **User roles to test**: which roles, and test accounts for each
- [ ] **Tenant boundaries**: if the product is multi-tenant, whether cross-tenant isolation is in scope
- [ ] **Environment under test**: production or a staging replica, and how test data is handled
- [ ] **Credentials and access method** the testers will receive, and for cloud, whether that's read-only credentials plus a set of agreed active tests

03 Compliance drivers and evidence

If an audit is behind the test, the framework shapes the scope. Know what evidence you need out before anyone quotes.

- [ ] **Which framework is driving the test** (SOC 2, PCI DSS, HIPAA, ISO 27001, GDPR) and the audit or deadline date
- [ ] **SOC 2**: whether you're facing a Type 1 (point in time) or Type 2 (review period); testing has to land accordingly
- [ ] **PCI DSS**: Requirement 11.4 expects external and internal testing at least annually and after significant changes, segmentation testing where segmentation shrinks your scope, and a tester independent of the systems under test
- [ ] **HIPAA**: where ePHI lives and moves, meaning the applications, APIs, integrations, and infrastructure your risk analysis answers for
- [ ] **The evidence you need out of the test**: what your auditor, customer, or security questionnaire actually asks for

04 Rules of engagement and logistics

Agree the ground rules in writing before testing begins; every serious vendor will expect these questions.

- [ ] **Exclusions**: e.g. denial of service, or phishing/social engineering unless explicitly agreed
- [ ] **Testing windows**: when testing may run, and any change-freeze periods to avoid
- [ ] **Escalation contacts**: who the testers call when something critical surfaces, and the channel for day-to-day contact
- [ ] **NDA and communication channels**: agreed before any testing starts
- [ ] **Who receives findings and the report**, and how long the vendor may retain them

05 Report and retest expectations

The report is the product. Set expectations for it, and for verification of fixes, before you compare quotes.

- [ ] **Report audiences**: an executive summary leadership can read, plus technical findings with reproduction steps and evidence
- [ ] **Severity model**: findings rated on a stated rubric (e.g. CVSS-based bands), with remediation guidance per finding
- [ ] **Retest**: included in the quoted price or extra, within what window, and whether the final report is updated to reflect verified fixes
- [ ] **Cadence**: one-time assessment or recurring cycles, and what triggers a re-test (releases, infrastructure change, annual baseline)
- [ ] **A sample report**: ask every vendor for a redacted sample before you sign

> **How to use this.** Work through the five sections with the people who own each answer: engineering for the surface and access, compliance for the drivers, security for the rules of engagement. A vendor that quotes without asking about most of this is pricing a scan, not a test. This checklist is published ungated at **virtuestech.com/pentest-scoping-checklist/**, alongside a guided walkthrough of a real (redacted) pentest report and a buyer's guide to choosing a vendor. We revise it as our published scoping guidance evolves; subscribe to “Updates from the practice” in the site footer for revisions.