

One-page short version

If there is no time for the full questionnaire, start with these 12 questions. The text after “Good” says what a good answer looks like. Tick an item only if the provider answered that way in writing. Items marked [stop] are mandatory.

- ☐ **[stop] Team.** Who exactly will test? Good: names and certificates with numbers.
- ☐ **[stop] Subcontractors.** Anyone else involved? Good: “no”, or only with our consent.
- ☐ **Method.** Which methodology? Good: PTES, OWASP or NIST, manual days listed separately.
- ☐ **Scope.** What will you test? Good: a written list of systems, roles and exclusions.
- ☐ **Rules.** How will you avoid breaking production? Good: bans, IP addresses, hours, who stops it.
- ☐ **[stop] Critical.** When will you tell us? Good: immediately, without waiting for the report.
- ☐ **[stop] Data.** What about evidence? Good: NDA first, encryption, deletion with confirmation.
- ☐ **[stop] AI.** Does our data go into AI services? Good: only with our written consent.
- ☐ **[stop] Report.** Is there a sample? Good: sanitised report, CVSS version, executive summary.
- ☐ **Retest.** Is it in the price? Good: number of retests and deadlines in the contract.
- ☐ **Liability.** Who is liable for an outage? Good: a contract clause, a cap, insurance.
- ☐ **Price.** What is included? Good: separate lines, scope changes only in writing.

Want to go through this checklist together? Write to us and we will review your scope.
veiltrack.io/en/contact