CLOUDSWITCHED

FREE RESOURCE — PENETRATION TESTING

Penetration Testing Buyer's Guide

How to buy a penetration test without overpaying, under-scoping, or ending up with a glorified vulnerability scan wearing a CREST logo. Covers the questions to ask providers, CREST vs standard explained, the red flags that predict a bad engagement, what a good report actually contains, and a scorecard to compare quotes fairly.

12	6	5	Fillable
PROVIDER SCOPING QUESTIONS	RED FLAGS TO WATCH FOR	REPORT QUALITY CRITERIA	SCORE SHEET INCLUDED

CREST · FIXED PRICE · REPORT QUALITY · RED FLAGS

PREPARED FOR
Cloudswitched Knowledge Library

PREPARED BY
Cloudswitched Ltd.

VERSION
2026 Edition

FORMAT
Interactive PDF

01

Questions to ask before you sign

A good provider answers every question below without hedging. Vague answers to specific questions are themselves a signal.

- **Who exactly will perform the test?** Named individual(s), their qualifications (CREST CRT/CCT, OSCP, OSCE), and years of relevant experience — not just the company's accreditation.
- **Is this manual testing or an automated scan with a human name attached?** Ask what proportion of the engagement is manual exploitation versus tool output.
- **What methodology do you follow?** OWASP Testing Guide, PTES, NCSC CHECK or CREST methodology — a named standard, not "our own process".
- **Can I see a sample report (redacted)?** This is the single most revealing question — see the report checklist opposite.
- **What is included in the price, and what is billed extra?** Retest, report walkthrough call, out-of-hours testing, additional scope added mid-engagement.
- **How many findings are typically retested for free?** Some providers include one free retest cycle; others charge per retest.
- **What happens if you find something critical mid-test?** Expect same-day notification for anything exploitable and high-impact, not a wait for the final report.
- **Do you carry professional indemnity and cyber insurance?** Ask for the coverage level, particularly for anything approaching live production systems.
- **How long until the report is delivered after testing ends?** 5–10 working days is typical; anything over three weeks should be queried.
- **Will you support us during Cyber Essentials Plus / insurer evidence requests?** Confirm the report format is accepted by the accreditation body or insurer you need it for.

CREST vs standard, explained

> **WHAT CREST ACCREDITATION ACTUALLY CERTIFIES**
>
> CREST accredits the *company* and individually examines *testers* against a defined methodology and code of conduct. It does not guarantee a better report than a non-accredited firm — it guarantees a minimum, independently verified standard of process and tester competency. Ask for it when a contract, insurer or regulator names it explicitly; otherwise, verify individual tester qualifications and a sample report instead.

02

Red flags, report quality & scorecard

Red flags

- ☐ **Day-rate ambiguity** — no fixed price, vague scope, “we’ll bill as we go”. Fixed-price against a written scope is the industry norm.
- ☐ **Scan-only “tests”** — an automated vulnerability scan re-badged as a penetration test, with no manual exploitation or chaining of findings.
- ☐ **No retest included or offered** — a provider with no view on verifying fixes has no interest in whether the engagement actually reduced risk.
- ☐ **Cannot name the tester or show qualifications** — a red flag regardless of company-level accreditation.
- ☐ **Report sample refused** — a redacted sample report is standard practice; refusal usually means the real thing is thin.
- ☐ **Pressure to skip scoping** — “just give us the IP range, we’ll work it out” leads directly to the day-rate surprises this guide exists to prevent.

What a good report contains

- **Executive summary** in plain English, written for a non-technical board or insurer audience, with an overall risk rating.
- **Each finding individually** with severity (CVSS or equivalent), technical detail, evidence (screenshots/output), business impact, and a specific remediation step — not a generic link.
- **An attack narrative** showing how findings chain together into a realistic compromise path, not just a flat list.
- **A methodology and scope appendix** stating exactly what was and was not tested, and any constraints encountered.
- **Retest results** as a follow-up appendix once remediation is verified, referencing the original finding IDs.

Evaluation scorecard

CRITERIA	PROVIDER A	PROVIDER B	PROVIDER C
Manual testing depth	___/5	___/5	___/5
Tester qualifications	___/5	___/5	___/5
Sample report quality	___/5	___/5	___/5
Price clarity & inclusions	___/5	___/5	___/5
Retest policy	___/5	___/5	___/5

Fixed-price expectations & next steps

For most UK SMEs, a scoped, fixed-price engagement is the right commercial model — it removes the risk of an open-ended day-rate bill and forces the provider to commit to a defined outcome.

WHAT "FIXED PRICE" SHOULD INCLUDE

The agreed scope, manual testing to a named methodology, a full written report with an executive summary, one retest cycle for Critical and High findings, and a report walkthrough call. Anything outside this — scope creep, additional retests, out-of-hours work — should be a clearly priced add-on, not a surprise invoice line.

Notes on shortlisted providers

Want a fixed-price quote to compare against?

Cloudswitched runs external, internal and web application penetration tests for UK SMEs at a fixed price, with one retest cycle and a full written report included as standard.

info@cloudswitched.com

cloudswitched.com/services/penetration-testing

CLOUDSWITCHED

OPTIMIZE YOUR IT AND THRIVE

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom