

FREE RESOURCE — PENETRATION TESTING

Penetration Test Scoping Questionnaire

A fillable questionnaire to define what a penetration test should actually cover before you ask a provider for a quote. Capture the business drivers, your asset inventory, the accreditation you need, your constraints and who the final report is for — so every quote you receive is scoped against the same brief.

5

SCOPING
SECTIONS
TO COMPLETE

30+

FIELDS &
QUESTIONS
TO FILL IN

CREST

VS STANDARD —
DECISION AID
INCLUDED

Fillable

TICK & TYPE
IN ANY VIEWER

EXTERNAL

INTERNAL

WEB APPS

CLOUD & APIS

PREPARED FOR

Cloudswitched Knowledge
Library

PREPARED BY

Cloudswitched Ltd.

VERSION

2026 Edition

FORMAT

Interactive PDF

01

Business context & drivers

A scoping call goes twice as fast when you walk in with this filled out. Complete the fields below with whoever owns the decision to test — IT lead, CISO, compliance owner or the business owner directly.

Organisation details

COMPANY NAME

INDUSTRY SECTOR

EMPLOYEE COUNT

DATE OF LAST TEST (IF ANY)

PROVIDER USED PREVIOUSLY

TARGET START DATE

What is driving this test?

- ☐ **Client or partner requirement** — a customer, supply-chain partner or tender is asking for evidence of testing.
- ☐ **Cyber insurance requirement** — renewal terms or a proposal form ask for an annual test.
- ☐ **Compliance framework** — Cyber Essentials Plus, ISO 27001, PCI-DSS, SOC 2 or a sector regulator requires it.
- ☐ **Post-incident or post-change** — you have had an incident, a breach near-miss, or a major system change.
- ☐ **Peace of mind / due diligence** — no external trigger, but leadership wants independent assurance.

Accreditation decision aid — CREST vs standard

CHOOSE CREST (OR CHECK) WHEN...

Your insurer, a client contract, PCI-DSS, or a public-sector tender explicitly names CREST / CHECK as a requirement; you need the test methodology and tester competency independently accredited; or a regulator will ask to see the accreditation on the report cover page.

A STANDARD (NON-ACCREDITED) TEST IS FINE WHEN...

No contract or insurer names an accreditation body; the goal is genuine risk reduction rather than compliance evidence; and you have verified the tester's individual qualifications (CREST CRT/CCT, OSCP, OSCE) and read a sample report before booking.

- ☐ **CREST / CHECK accreditation required** — named explicitly in a contract, insurer questionnaire or tender document.
- ☐ **Standard test acceptable** — no named accreditation requirement identified.
- ☐ **Unsure** — check the insurer proposal form and any client security questionnaire before booking.

02

Asset inventory, constraints & audience

Every field below shrinks the gap between the quote you are given and the price you actually pay. Under-scoping is the single biggest cause of day-rate surprises once testing starts.

Asset inventory

EXTERNAL IP ADDRESSES / RANGES

APIS (REST/GRAPHQL — COUNT)

CLOUD TENANTS (M365 / AZURE / AWS / GCP)

OFFICE / SITE LOCATIONS IN SCOPE

PUBLIC WEB APPLICATIONS (COUNT & URLS)

MOBILE APPS (IOS / ANDROID)

INTERNAL HOSTS / SERVERS (APPROX. COUNT)

REMOTE ACCESS / VPN ENDPOINTS

Constraints

- ☐ **Test window agreed** — business hours, out-of-hours only, or a fixed change-freeze window. Dates: _____
- ☐ **Exclusions defined** — systems, third-party services or fragile legacy hosts explicitly out of scope.
- ☐ **Denial-of-service testing** — permitted, or explicitly excluded (default assumption: excluded).
- ☐ **Social engineering** — phishing simulation or physical access testing included, or scoped separately.

Report audience

- ☐ Technical (dev / IT team) ☐ Executive summary ☐ Board / insurer pack

THE MOST UNDER-SCOPED FIELD

API and mobile app counts are the fields most often left blank — and the ones that cause the biggest quote-to-invoice gap. If you are not sure, ask your developer or hosting provider for a count before the scoping call, not during it.



Sign-off & next steps

Attach this completed questionnaire to every provider RFQ you send. It ensures each quote is priced against the same scope, which is the only way to compare them fairly.

Additional notes for the scoping call

Completed by

NAME

ROLE / TITLE

DATE

Need a scope reviewed, or a test booked?

Cloudswitched runs external, internal and web application penetration tests for UK SMEs, with fixed-price quotes scoped against exactly this questionnaire.

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