Penetration Testing Services

Request for Information

Issued by:

Reference number:

Date issued:

Response required by:

Primary contact:

Email:

For the buyer: Section 01 takes about 10 minutes. Required questions sit in 1.1 to 1.5. The optional 1.6 (technical context) helps vendors quote more accurately but can be left for the scoping call.
For the vendor: Complete sections 02 through 08 and return as a single PDF to the contact above. Flag any unanswered question in writing rather than leaving it blank.

Section 01: Engagement Scope

Completed by the issuing company - five required subsections, about 10 minutes

Required: 1.1 to 1.5 (about 10 minutes - everything a vendor needs to quote). **Optional: 1.6** shortens the scoping call; skip what you do not have.

1.1 Contact

Company name:

Primary contact:

Email:

1.2 Systems in scope

List every asset to be tested - URLs, IP ranges, application names. One per line.

Also in scope:

- ☐ Mobile applications
- ☐ Cloud infrastructure (IAM, storage, compute)
- ☐ Internal network or Active Directory

1.3 Test parameters

Test type:

- ☐ White box - *source code, architecture, and credentials provided*
- ☐ Gray box - *authenticated user access provided*
- ☐ Black box - *external attacker view only, no credentials*

Test environment:

- ☐ Production
- ☐ Staging
- ☐ Both

Compliance to satisfy:

(e.g. PCI DSS v4.0, SOC 2, NIS2, ISO 27001 - or 'none')

1.4 Timeline

Preferred start date:

Required completion date:

1.5 Rules of engagement

Denial-of-service style payloads:

- ☐ Excluded entirely
- ☐ Permitted with prior written approval

1.6 Optional - technical context

Skip what you do not have. Anything left blank, the vendor will raise during the scoping call. Filling these in usually shortens that call by half.

Business goal of this test:

(what success looks like, what risk this engagement is buying down)

Architecture and tech stack:

(modules, microservices, languages, frameworks, third-party integrations)

Hosting model:

(e.g. AWS eu-west-1, Azure West Europe, on-prem, hybrid)

Roles and permissions in scope:

(list every role; mark which are in test scope vs out of scope)

Section 02: Company Information

Vendor completes

Company name:

Registered address:

Company registration number:

Website:

This response prepared by:

(name and title)

Email:

Phone:

Insurance and accreditations

Professional indemnity / errors and omissions insurance:

☐ Yes ☐ No

If yes - coverage limit:

If yes - insurance provider:

ISO 27001 certified:

☐ Yes ☐ No

Other relevant accreditations:

Section 03: Team for This Engagement

Vendor completes

Name the specific individuals who will perform testing on this engagement. Certifications listed must be held by the named individual, not the company overall.

Tester 1

Name:

Role on this engagement:

Certifications personally held:

Tester 2

Name:

Role on this engagement:

Certifications personally held:

Tester 3

Name:

Role on this engagement:

Certifications personally held:

Tester 4

Name:

Role on this engagement:

Certifications personally held:

Will any work be performed by freelancers?

☐ Yes ☐ No

If yes - provide details:

Will any testing be performed offshore?

☐ Yes ☐ No

If yes - provide details:

Section 04: Methodology

Vendor completes

Describe your approach to each asset type in scope. Be specific - generic answers such as 'we follow all major frameworks' are not acceptable.

Web application testing approach

Which OWASP WSTG categories will you cover? List any you will not cover and explain why.

API testing approach

Network and infrastructure approach

Manual to automated ratio:

(e.g. 80% manual, 20% tool-assisted)

Tools

List the commercial and open-source tools you use for this scope type:

Out-of-scope discovery

If you find a critical vulnerability outside the agreed scope during testing, what do you do?

Critical finding escalation

What is your procedure if you discover a CVSS 9.0+ issue mid-engagement?

Section 05: Reporting and Retest

Vendor completes

Business days after testing concludes until final report is delivered:

Will findings be mapped to the compliance specified in Section 1.3?

☐ Yes ☐ No

Sample report

☐ I will provide a sample redacted report from a comparable engagement
☐ I can offer a walkthrough on a call where NDA prevents sharing a document
☐ I cannot provide a sample report or offer a walkthrough

Retest policy

Retest of the following severities is included at no additional charge:

☐ Critical ☐ High ☐ Medium ☐ None included - retest scoped separately

Retest is available within:

(days of report delivery date)

Describe your retest process (how findings are verified as resolved, what the addendum contains):

Section 06: Data Handling and Legal

Vendor completes

Data retention:

(how long do you retain test artifacts - screenshots, logs, captured credentials, exploit code - after the engagement concludes?)

Destruction procedure:

(how are retained artifacts destroyed at end of retention period?)

Data processing location:

(country or region where artifacts are stored)

Data residency restrictions honoured:

(e.g. EU-only, UK-only)

Sub-processors used during this engagement:

(any third party that touches client data - cloud storage, transcription, AI assistants - or 'none')

Will you sign our non-disclosure agreement?

☐ Yes ☐ No

Standard clauses you typically negotiate or flag:

Cyber liability cap stated in your standard terms:

Cap amount:

Currency:

Service disruption procedure

If your testing causes unintended service disruption, describe your response procedure:

Section 07: References

Vendor completes

Please provide three references from engagements in a comparable sector or scope type. We may contact references directly. A sector description is acceptable where the client name is subject to NDA.

Reference 1

Client:

(or sector if NDA applies)

Contact name and title:

Email:

Phone:

Engagement type and approximate date:

Reference 2

Client:

(or sector if NDA applies)

Contact name and title:

Email:

Phone:

Engagement type and approximate date:

Reference 3

Client:

(or sector if NDA applies)

Contact name and title:

Email:

Phone:

Engagement type and approximate date:

Section 08: Pricing

Vendor completes

Complete this section if pricing has not been submitted separately.

Day rate (excluding VAT/tax):

Estimated days for this scope:

Total quote (excluding VAT/tax):

Quote valid until:

What is included in the above quote:

What is excluded or quoted separately:

Information confirmed accurate; named testers available subject to contract.

Signature and date:

Printed name and title: