

Penetration Test Readiness Checklist

A little preparation gets you far more value from the same engagement: fewer delays, deeper coverage and a report your auditors will accept first time. Tick off each item as you go. This checklist works whoever you test with.

1. Define the goal

4–6 weeks before testing

- ☐ **Know why you are testing**
Compliance (PCI DSS, HIPAA, SOC 2, ISO 27001), a customer or investor request, cyber insurance, a major release, or after an incident. The reason shapes the scope and the report format.
- ☐ **Confirm any deadlines**
Audit dates, contract renewals or launch dates. Allow time to fix findings and retest before them.
- ☐ **Check what your auditor or customer expects**
Some require specific test types (e.g. PCI DSS 11.4 internal, external and segmentation testing), a tester with recognised certifications, or a summary letter they can keep on file.

2. Define the scope

3–4 weeks before

- ☐ **List every target**
Web applications and URLs, APIs, external IP ranges, internal subnets, wireless networks, and AI/LLM features such as chatbots, RAG pipelines and agents.
- ☐ **Decide what is out of scope**
Fragile legacy systems, third-party services you do not own, and any techniques you do not want used (e.g. denial of service). Write it down.
- ☐ **Choose production or staging**
Staging is safer, but it must match production closely or the results will not reflect real risk.
- ☐ **Get permission for hosted and third-party systems**
Confirm you own or are authorised to test every target. Cloud providers such as AWS, Azure and Google Cloud allow testing of your own resources but have published policies to follow.

3. Paperwork and contacts

2 weeks before

- ☐ **Sign the authorization and rules of engagement**
Covers targets, testing windows, permitted techniques, and how data is handled and destroyed.
- ☐ **Name a technical point of contact**
Someone who can answer questions quickly and fix access issues during testing.
- ☐ **Set up an emergency contact**
Available during testing hours (and after hours if testing then) in case a critical finding needs immediate action or a system behaves unexpectedly.
- ☐ **Agree testing windows**
Business hours, after hours, or around change freezes and peak trading periods.

4. Access and accounts

1 week before

- ☐ **Create test accounts for each user role**
e.g. customer, staff and admin. Testing every role is how access-control and privilege flaws are found.

☐ **Provide API documentation**

An OpenAPI/Swagger file or Postman collection makes API testing faster and more thorough.

☐ **Arrange internal access**

VPN credentials, a jump host, or space on the network for a testing VM, plus any NAC exceptions needed.

☐ **Decide on allow-listing**

Allow-listing the tester's IP addresses in your WAF or IPS tests the application itself; leaving controls on tests your defences too. Agree which you want.

5. Prepare your environment

Days before

☐ **Take backups**

Testing is non-destructive, but recent backups are good practice for any change to normal traffic.

☐ **Tell the people who watch your alerts**

Your IT team, MSSP or SOC should know testing dates and source IPs, unless detection is part of the test.

☐ **Pause risky changes**

Avoid major deployments to in-scope systems during the test so results stay consistent.

6. After the test

Weeks after

☐ **Hold a report readout**

Walk through the findings with the tester so your developers understand each issue and the fix.

☐ **Assign owners and deadlines**

Prioritise by risk: critical and high findings first. Track them like any other engineering work.

☐ **Schedule the retest**

A retest confirms the fixes worked and gives auditors and customers a clean, updated result.

☐ **Plan the next test**

At least annually, and after significant changes. PCI DSS requires both.

Ready to scope your penetration test?

CREST CRT & OSCP certified testing with a fixed price agreed up front and a free retest.

Book a free scoping call: zerodaysecurity.net/book-a-free-scoping-call