CHECKLIST 12 REVIEW POINTS 9 MIN REVIEWED 11/08/2026

# Prepare penetration tests sensibly

Determine the test objective, systems, access, test rules and results path before a penetration test.

FOR WHOM

IT managers, product teams, management and information security before an external security test.

WHEN TO USE IT

Before the offer and order and again immediately before the start of the active examination.

THE SHORT ANSWER

A penetration test is well prepared when the test objective, system boundaries, roles, permitted methods, test access, emergency contacts, report recipients and follow-up test are clearly agreed upon before the first active test.

**Important boundary:** Active security checks can impact systems and data. Scope, release and demolition route must be agreed in writing.

## 01 Target and test area

A test needs a specific security question and clearly stated limits.

- [ ] **Define the test objective in one sentence**
  Describe which risks, roles or business processes should be assessed.
- [ ] **Inventory systems and interfaces**
  Mention domains, APIs, mobile applications, networks, identities and external dependencies.
- [ ] **Document exceptions visibly**
  Systems and methods that cannot be verified receive a technical justification and risk assessment.
- [ ] **Decide test model**
  Black Box, Gray Box or White Box are chosen to suit the goal, time and available insight.

## 02 Safe test operation

Contacts, time windows and rules protect operations, evidence and test quality.

- [ ] **Identify responsible persons and emergency contacts**

  Technology, departments and test teams must be available during the test.

- [ ] **Agree on permitted methods and limits**

  Load testing, social engineering, data access and productive changes are explicitly regulated.

- [ ] **Prepare test accounts and data**

  Roles, multi-factor access and data-efficient test data are checked in advance.

- [ ] **Define termination criteria**

  Disruption, data risk or unexpected impact need a decision-making path that can be used immediately.

## 03 Result and resolution

Value only arises when discoveries are understood, prioritized and verifiably closed.

- [ ] **Specify report recipients**

  Technical teams and management require different levels of detail, but the same understandable risk basis.

- [ ] **Regulate critical reporting during the test**

  Finds that can be exploited are not withheld until the final report.

- [ ] **Prepare action process**

  Every relevant find is given responsibility, priority, deadline and technical consultation.

- [ ] **Arrange a follow-up test**

  The scope, deadline and expected proof of remediation are included in the original order.

## Result of the joint review

- A written test order
- A secure test and escalation path
- Usable reports for technology and management
- An agreed remediation and retesting process

## Related guidance

- Penetration test in detail →
- Cybersecurity →
- Web and API penetration testing →

---

## Sources and professional basis

This working aid translates general recommendations into a compact initial review. The primary sources and your specific context remain decisive.

- BSI: Practical guide for IS penetration testing →
- OWASP: Web Security Testing Guide →

# Frequently asked questions

## Is an automatic vulnerability scan enough?

## Should testing be carried out directly in production?

Browser checkmarks are not stored or transmitted to sudo/PORT.