Penetration Testing Maturity & Readiness Assessment Checklist

Mark each item:

- Yes
- No
- Needs Review

Governance & Scope

1. We maintain an updated inventory of public-facing digital assets.
2. We know which systems are most critical for pentest prioritisation.
3. Security testing objectives are defined in business terms, not vague technical terms.

Visibility & Enumeration

4. We routinely review exposed login portals, domains, and remote interfaces.
5. Forgotten subdomains, staging systems, and retired tools are actively decommissioned.
6. Public employee identity exposure is understood and monitored.

Vulnerability Discipline

7. Patch responsibilities are clearly assigned.
8. Cloud permissions are reviewed regularly.
9. Administrative interfaces are restricted and strongly authenticated.
10. SaaS integrations are reviewed for ongoing necessity.

Credential & Access Security

11. MFA is enforced consistently without broad exemptions.
12. Former employee and contractor accounts are removed quickly.
13. Password reuse is actively discouraged and managed.
14. Privilege levels are reviewed against job necessity.

Human Security Resilience

15. Staff receive recurring phishing/social engineering awareness.
16. Payment and account change requests require secondary verification.

17. Helpdesk/support identity verification is documented.

Pentest Response Readiness

18. We assign ownership for remediation after security findings.
19. Findings are prioritized by business impact.
20. We conduct retesting after major remediation work.

Continuous Improvement

21. Pentesting is scheduled periodically, not only after incidents.
22. Pentest reports influence policy and workflow updates.
23. Vendor-managed systems are included in assessment planning.
24. Remote access environments are tested regularly.
25. Leadership reviews pentest findings at management level.

SCORING GUIDE

Strong Maturity (20–25 Yes Answers)

Your organisation demonstrates disciplined security testing governance and meaningful resilience follow-through.

Moderate Exposure (11–19 Yes Answers)

You have security controls in place but testing maturity and remediation consistency still leave practical attacker opportunities.

High Vulnerability (0–10 Yes Answers)

Your organisation likely relies on untested assumptions and may contain multiple unvalidated exposure pathways requiring immediate structured assessment.