Ethical Hacking Readiness & Exposure Assessment Checklist

Use this checklist to evaluate your organisation's current maturity in attacker-awareness and practical exposure reduction.

Mark each item:

- Yes
- No
- Needs Review

External Visibility & Recon

1. We know what public information about our company is easily discoverable online.
2. We routinely review public-facing domains, subdomains, and exposed portals.
3. Staff social media and public business listings are reviewed for oversharing risk.

Website & Application Security

4. Our website software, plugins, and forms are reviewed and updated consistently.
5. Administrative website login areas are protected with strong authentication.
6. File upload/download features have been security reviewed.

Credential Discipline

7. Multi-factor authentication is enforced across critical systems.
8. Former employee accounts are removed promptly.
9. Shared admin credentials are prohibited or tightly controlled.
10. Password reuse risk is addressed through policy and password manager adoption.

Cloud & Access Control

11. Shared cloud folders are reviewed for unnecessary public exposure.
12. Third-party SaaS tools are inventoried and monitored.
13. User permissions are reviewed at scheduled intervals.

Human Security Readiness

14. Employees receive phishing and social engineering awareness training.
15. Payment or bank detail changes require secondary verification.
16. Staff are trained to challenge urgent executive-style requests.

Infrastructure & Remote Exposure

17. Wi-Fi infrastructure is segmented and regularly updated.
18. VPN and remote access accounts are reviewed for necessity and security.
19. Company devices used remotely are governed by security policy.
20. Peripheral connected devices are included in security oversight.

Vulnerability Management

21. We perform regular vulnerability reviews rather than waiting for incidents.
22. Software and firmware patching responsibilities are clearly assigned.
23. Old digital tools, unused accounts, and abandoned services are routinely removed.

Response & Improvement

24. Security findings are prioritized by business impact, not just technical severity.
25. We retest important fixes to ensure vulnerabilities are actually closed.

SCORING GUIDE

Strong Maturity (20–25 Yes Answers)

Your organisation shows healthy attacker-awareness and disciplined cyber governance. Continue refining review cycles and verification culture.

Moderate Exposure (11–19 Yes Answers)

You have meaningful protections in place, but operational blind spots still create exploitable attacker opportunities.

High Vulnerability (0–10 Yes Answers)

Your organisation likely relies too heavily on assumed safety and may contain multiple overlooked compromise pathways requiring immediate review.