Human Firewall Readiness Audit Checklist

Use the following checklist to assess your organisation's current exposure to social engineering and human-cantered cyber threats.

Check each item honestly.

Employee Awareness & Training

1. ☐ Employees receive cybersecurity awareness training more than once per year.
2. ☐ Social engineering examples are included in employee education.
3. ☐ New hires receive cyber awareness onboarding immediately.
4. ☐ Phishing simulations or awareness drills are conducted regularly.
5. ☐ Training content is role-specific where appropriate.

Verification & Process Controls

6. ☐ Payment changes require independent confirmation.
7. ☐ Vendor bank detail updates are verbally verified.
8. ☐ Executive urgent requests are not exempt from verification.
9. ☐ Password or MFA resets require identity confirmation.
10. ☐ Sensitive data requests require approval procedures.

Reporting Culture

11. ☐ Employees know exactly how to report suspicious activity.
12. ☐ Reporting channels are simple and visible.
13. ☐ Employees are encouraged to report mistakes immediately.
14. ☐ Leadership avoids blame-first responses after incidents.

Leadership & Culture

15. ☐ Leadership actively reinforces cybersecurity expectations.
16. ☐ Managers support employees who question suspicious requests.
17. ☐ Verification is treated as professionalism, not delay.
18. ☐ Cybersecurity messaging is continuous, not annual only.

Remote & Operational Exposure

19. ☐ Remote workers receive dedicated social engineering guidance.
20. ☐ Collaboration platform threats are included in awareness training.
21. ☐ Personal device use is governed by security expectations.

22. ☐ Vendor communications are routinely validated.

Incident Readiness

23. ☐ Human-based cyber incident response steps are documented.
24. ☐ Financial fraud emergency contacts are pre-established.
25. ☐ Post-incident reviews are used to improve process discipline.

SCORING RESULTS

Strong Maturity (20–25 Checked)

Your organisation demonstrates a healthy human firewall culture with strong operational awareness and above-average resilience against social engineering threats.

Moderate Exposure (12–19 Checked)

Your organisation has partial controls in place, but meaningful behavioural and process vulnerabilities remain exploitable.

High Vulnerability (0–11 Checked)

Your organisation currently faces significant human-cantered cyber risk and should prioritise awareness, verification, and reporting improvements immediately.