Network Security Maturity Audit Checklist

Score each item:

- Yes = 2 points
- Partially = 1 point
- No = 0 points

Core Infrastructure

☐ 1. All major routers, firewalls, and gateways are documented.
☐ 2. Network hardware firmware is updated on a scheduled basis.
☐ 3. Default credentials on network devices have been changed.
☐ 4. Unsupported legacy networking hardware has been phased out.

Internal Trust & Segmentation

☐ 5. Guest devices are separated from internal business systems.
☐ 6. Critical systems are segmented from ordinary employee devices.
☐ 7. Vendor access is restricted to only necessary resources.
☐ 8. Lateral movement opportunities have been reviewed internally.

Wireless & Remote Access

☐ 9. Business Wi-Fi uses strong authentication and controlled passwords.
☐ 10. Guest Wi-Fi is isolated from corporate traffic.
☐ 11. VPN or remote access requires MFA.
☐ 12. Dormant remote access accounts are reviewed regularly.

Device & Endpoint Control

☐ 13. The organisation maintains a current inventory of connected devices.
☐ 14. BYOD usage is governed by policy.
☐ 15. Unknown or decommissioned devices are removed promptly.

Monitoring & Detection

☐ 16. Firewall logs are reviewed routinely.
☐ 17. Suspicious remote login patterns are monitored.
☐ 18. Network anomalies trigger assigned investigation.
☐ 19. Critical logs are centrally retained.

Governance & Incident Readiness

☐ 20. Firewall and access rule changes are documented.
☐ 21. Network vendors and contractors are reviewed periodically.
☐ 22. Network incident response contacts are clearly assigned.
☐ 23. Leadership receives periodic network risk visibility.
☐ 24. The network undergoes recurring security audits.
☐ 25. Network security ownership is assigned beyond informal IT support.

SCORING RESULTS

40–50 Points — Strong Maturity

Your organisation demonstrates disciplined network control and above-average infrastructure resilience.

22–39 Points — Moderate Exposure

Important protections exist, but unmanaged growth or inconsistent oversight still creates avoidable gaps.

0–21 Points — High Vulnerability

Your business network may be operationally functional but remains materially exposed to preventable compromise, rapid malware spread, and weak incident containment.