



Remote Work Security Maturity Checklist

Score each item:

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

Connectivity & Access

- 1. All remote business access uses secure approved entry points.
 - 2. VPN or Zero Trust access is protected with MFA.
 - 3. Dormant remote access accounts are reviewed regularly.
 - 4. Remote users receive only necessary system visibility.
-

Endpoint Security

- 5. Remote laptops are managed and patched.
 - 6. Devices are encrypted.
 - 7. Endpoint protection is centrally monitored.
 - 8. Personal unmanaged devices are restricted by policy.
-

Identity Governance

- 9. MFA is enforced across critical cloud applications.
 - 10. Shared departmental logins are prohibited.
 - 11. Dormant users are reviewed after role changes and exits.
 - 12. Conditional login anomalies are monitored.
-

SaaS & Data Control

- 13. Shared cloud folders are permission-reviewed.
- 14. Third-party SaaS integrations are assessed.
- 15. Leadership knows where major business data repositories exist.
- 16. Oversharing and public links are restricted.

Environmental Awareness

- 17. Employees receive home Wi-Fi and public network security guidance.
- 18. Public Wi-Fi use is governed by VPN policy.
- 19. Remote device loss procedures are documented.

Lifecycle & Vendor Trust

- 20. HR and IT share a formal remote onboarding/offboarding checklist.
- 21. Contractor access is time-bound and named.
- 22. Vendor remote sessions are reviewed periodically.

Monitoring & Response

- 23. Remote access logs are centrally retained.
- 24. Devices/accounts can be remotely disabled quickly.
- 25. Leadership receives recurring distributed security visibility.

SCORING RESULTS

40–50 Points — Strong Maturity

Your organisation demonstrates disciplined secure remote work governance and resilient distributed trust management.

22–39 Points — Moderate Exposure

Remote operations are functioning, but inconsistent controls leave meaningful avoidable gaps.

0–21 Points — High Vulnerability

Your distributed workforce may be productive, but current infrastructure trust is materially under-governed.