Professional Hybrid Office Cybersecurity Readiness Audit Checklist

Distributed Workforce Security Self-Assessment

Score each item:

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

Workforce Visibility

☐ We maintain a current inventory of all hybrid/remote users and their access roles.
☐ Devices used for business work are documented, including mobile dependencies.
☐ Core cloud applications and data movement paths are mapped.

Endpoint Protection

☐ All work laptops use managed endpoint protection and enforced updates.
☐ Device encryption is enabled on all company-issued endpoints.
☐ Remote wipe or rapid disable procedures exist for lost devices.

Identity Security

☐ MFA is enforced across all critical business systems.
☐ Password governance is standardized across cloud applications.
☐ Ex-employee and stale accounts are removed promptly.

Remote Connectivity

☐ VPN or secure access controls are consistently used where required.
☐ Browser/cloud sessions use timeout or conditional access controls.
☐ Employees receive guidance on public Wi-Fi and home router risk.

Collaboration Security

☐ Cloud document sharing permissions are reviewed regularly.
☐ Meeting confidentiality practices are communicated clearly.
☐ Messaging/file sharing tools are governed by approved-use standards.

Employee Behaviour

☐ Staff receive recurring phishing and remote security awareness training.
☐ Shadow IT and personal file-sharing shortcuts are actively discouraged.
☐ Home office confidentiality expectations are defined.

Incident & Continuity

☐ Remote incident response instructions exist for non-technical staff.
☐ Backup communication methods exist if primary collaboration tools fail.
☐ Key business roles have alternate access continuity plans.

Governance Maturity

☐ Hybrid security reviews are performed on a scheduled cadence.
☐ Managers participate in reinforcing secure remote work discipline.

SCORING RESULTS

38–46 Points — STRONG MATURITY

Your organisation demonstrates strong distributed workforce cyber discipline and resilient hybrid operational readiness.

20–37 Points — MODERATE EXPOSURE

Important controls exist, but employee inconsistency and distributed trust gaps may still create avoidable disruption risk.

0–19 Points — HIGH VULNERABILITY

Your hybrid workforce likely operates with fragmented security practices, limited continuity readiness, and elevated cyber exposure.