Zero-Trust Readiness Assessment Checklist

Use this checklist to evaluate how much blind trust currently exists inside your organisation.

Identity Controls

☐ Multi-factor authentication is enforced across critical systems.
☐ Shared/generic accounts have been reduced significantly.
☐ Password management is standardized.
☐ Suspicious login behaviour is monitored.
☐ User identities are inventoried and reviewed.

Access Governance

☐ Least-privilege access is applied by role.
☐ Former employees are offboarded rapidly.
☐ Administrative rights are tightly restricted.
☐ Shared cloud folders are segmented by sensitivity.
☐ Dormant user permissions are reviewed periodically.

Device Trust

☐ Company devices follow minimum patch/security standards.
☐ Personal device access is governed.
☐ Lost/stolen devices trigger immediate response.
☐ Unsupported or risky software is restricted.

Monitoring and Visibility

☐ Login anomalies are reviewed regularly.
☐ Vendor accounts are logged and reviewed.
☐ Critical SaaS integrations are inventoried.
☐ Access logs are retained for investigation.

Human Verification Culture

☐ Employees are trained to verify unusual requests.
☐ Suspicious MFA prompts are reported immediately.
☐ Staff understand why access friction exists.
☐ Convenience-based sharing habits are discouraged.

Zero Trust Governance

☐ Vendor permissions are reviewed regularly.
☐ Zero Trust improvements are phased strategically.
☐ Leadership reviews trust exposure as an ongoing risk.
☐ Access assumptions are challenged at least annually.

SCORING YOUR RESULTS

20–24 boxes checked = STRONG MATURITY

Your organisation is actively reducing blind trust and building stronger access verification discipline.

12–19 boxes checked = MODERATE EXPOSURE

Some Zero Trust foundations exist, but significant automatic trust still remains embedded in systems, permissions, and employee routine.

0–11 boxes checked = HIGH VULNERABILITY

Your organisation is still operating with broad unverified trust relationships that could significantly amplify account compromise or insider mistakes.