Insider Threat Readiness Audit Checklist

Use this checklist to assess whether your organisation is overexposed to trusted-user cyber risk.

User Access Governance

☐ All active employee accounts are inventoried.
☐ Former employee accounts are removed rapidly.
☐ Shared/generic accounts are minimised.
☐ Least-privilege access is applied by role.
☐ Administrative rights are tightly controlled.

Sensitive Data Protection

☐ Sensitive business data locations are clearly identified.
☐ Large export/download permissions are role-limited.
☐ Personal cloud uploads are restricted.
☐ USB/local transfer handling is governed.
☐ Broad anonymous share links are discouraged.

Contractor and Vendor Controls

☐ Contractor accounts are reviewed regularly.
☐ Vendor access has named internal ownership.
☐ Temporary external permissions expire deliberately.
☐ Third-party login activity is visible.

Monitoring and Reporting

☐ High-risk internal activity is logged.
☐ Employees know what internal mistakes to report.
☐ Suspicious MFA/login prompts are escalated quickly.
☐ Managers reinforce cyber accountability consistently.

Growth Governance

☐ Role changes trigger access review.
☐ New SaaS platforms are reviewed before broad rollout.
☐ Insider risk policies are documented.
☐ Leadership reviews internal trust exposure annually.

☐ Sensitive folders are segmented by business need.
☐ Data handling expectations are part of employee awareness training.

SCORING YOUR RESULTS

20–24 boxes checked = STRONG MATURITY

Your organisation is actively controlling internal trust relationships and reducing preventable insider-driven cyber exposure.

12–19 boxes checked = MODERATE EXPOSURE

Some internal controls exist, but growth has likely created permission, data handling, or visibility gaps that still leave meaningful insider risk.

0–11 boxes checked = HIGH VULNERABILITY

Your organisation is relying heavily on informal trust and may be significantly exposed to costly employee, contractor, or dormant-account cyber incidents.