Annual Technology Audit Readiness Assessment Checklist

Instructions

Use this checklist to evaluate your organisation's operational visibility, cybersecurity audit maturity, and resilience preparedness.

Score each item:

- Yes = 2 points
- Partial/In Progress = 1 point
- No = 0 points

Cybersecurity & Access Visibility

☐ We maintain updated inventories of devices and systems.

☐ MFA is enforced consistently across critical accounts.

☐ Access permissions are reviewed regularly.

☐ Former employee accounts are removed promptly.

☐ Endpoint visibility is actively maintained.

Infrastructure & Operational Resilience

☐ Hardware lifecycle reviews are conducted annually.

☐ Unsupported systems are identified and addressed.

☐ Backup testing is performed regularly.

☐ Recovery procedures are documented clearly.

☐ Network visibility is maintained consistently.

Software & SaaS Governance

☐ SaaS applications are reviewed regularly.

☐ Unused software subscriptions are removed.

☐ Shadow IT exposure is monitored.

☐ Cloud application access is reviewed regularly.

☐ Operational complexity is actively reduced where possible.

Vendor & Third-Party Oversight

☐ Vendor inventories are maintained.

☐ Third-party access permissions are reviewed.

☐ Operational dependency risks are evaluated.

☐ MSP and cloud provider accountability is reviewed regularly.

☐ Vendor continuity exposure is considered during planning.

Governance & Continuous Improvement

☐ Leadership receives technology audit visibility.

☐ Audit findings are documented clearly.

☐ Cross-functional participation occurs during audits.

☐ AI and automation risks are reviewed operationally.

☐ Audit processes are continuously improved.

Scoring Results

40–50 Points — Strong Operational Technology Maturity

Your organisation demonstrates strong operational visibility, governance maturity, and resilience-focused audit discipline.

Continue strengthening:

- continuous improvement,
- recovery preparedness,
- and operational adaptability.

20–39 Points — Moderate Technology Exposure

Your organisation has foundational operational visibility but may still face:

- governance gaps,
- software sprawl,
- operational blind spots,
- or continuity weaknesses.

Focus on:

- access governance,
- SaaS visibility,
- recovery testing,
- and vendor oversight improvements.

0–19 Points — High Operational & Cybersecurity Risk

Your organisation may face significant exposure involving:

- weak visibility,
- unmanaged systems,
- unsupported infrastructure,
- operational fragmentation,
- or limited resilience preparedness.

Immediate priorities should include:

- inventory reviews,
- access cleanup,
- backup validation,
- governance strengthening,

and operational audit discipline improvements.