Tech Vendor Risk & Readiness Assessment Checklist

Use the following checklist to assess your organisation's current vendor management maturity and operational technology awareness.

Check each statement honestly.

Vendor Visibility & Documentation

☐ We maintain a documented list of critical vendors
☐ Vendor ownership is clearly assigned internally
☐ Renewal dates are tracked consistently
☐ Support contact details are documented
☐ Operational dependencies are understood

Security Awareness

☐ Vendors support multi-factor authentication
☐ Vendor security responsibilities are understood
☐ Backup responsibilities are clearly defined
☐ Access permissions are reviewed periodically
☐ Sensitive systems use strong authentication controls

Operational Resilience

☐ We understand what happens during vendor outages
☐ Business continuity risks involving vendors are reviewed
☐ Alternative operational procedures exist where appropriate
☐ Critical vendors are reviewed periodically
☐ Vendor support responsiveness is evaluated regularly

Contract & Dependency Awareness

☐ Contract renewal terms are understood clearly
☐ Exit and migration options are reviewed before purchasing
☐ Pricing escalation risks are considered
☐ Data ownership responsibilities are understood
☐ Vendor lock-in exposure is assessed periodically

AI & Emerging Technology Oversight

☐ AI tools used within the business are visible to management
☐ Employees understand acceptable AI usage expectations
☐ Sensitive data handling guidance exists for AI platforms
☐ Shadow IT risks are monitored operationally
☐ Vendor adoption decisions include cybersecurity considerations

---

Scoring Your Readiness

20–25 Checked

Strong Maturity

Your organisation demonstrates strong awareness of vendor dependency, operational resilience, and technology governance.

Continue refining:

- vendor reviews,
- documentation,
- cybersecurity evaluation,
- and operational continuity planning.

Maintaining visibility and discipline will support long-term resilience.

10–19 Checked

Moderate Exposure

Your organisation has some vendor management foundations in place but still faces meaningful operational and dependency risks.

Focus on:

- documentation,
- visibility,
- security questioning,
- and contract awareness.

Incremental improvements can significantly reduce long-term exposure.

0–9 Checked

High Vulnerability

Your organisation may face elevated exposure involving:

- vendor dependency,
- operational disruption,
- cybersecurity blind spots,
- and poor visibility into technology risk.

Immediate focus should include:

- vendor documentation,
- operational awareness,
- access management,
- and resilience planning.

Modern businesses cannot effectively manage technology they do not fully understand.