Vendor Risk Management Readiness Assessment Checklist

Instructions

Use this checklist to evaluate your organisation's vendor governance maturity and third-party operational resilience readiness.

Score each item:

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

Vendor Visibility & Governance

☐ We maintain a complete inventory of critical vendors.

☐ Vendor ownership responsibilities are clearly assigned.

☐ Leadership receives visibility into major vendor risks.

☐ Vendor governance processes are documented.

☐ Critical vendor dependencies are operationally understood.

Cybersecurity Due Diligence

☐ Vendors undergo cybersecurity review before onboarding.

☐ MFA expectations are enforced for critical vendor access.

☐ Vendor backup and recovery practices are evaluated.

☐ Incident response expectations are documented.

☐ Vendor access permissions are reviewed regularly.

Operational Resilience

☐ Business continuity plans include vendor-related disruption scenarios.

☐ Critical SaaS and cloud dependencies are identified.

☐ Vendor outage recovery procedures exist.

☐ Operational concentration risk is evaluated.

☐ Vendor offboarding procedures are documented.

Compliance & Accountability

☐ Vendor contracts contain cybersecurity obligations.

☐ Breach notification procedures are clearly defined.

☐ Vendor compliance documentation is maintained.

☐ Third-party data handling practices are reviewed.

☐ Governance reporting includes vendor-related exposure.

Continuous Oversight & Strategic Planning

☐ Vendors are monitored continuously after onboarding.

☐ Vendor performance reviews occur regularly.

☐ Governance processes scale alongside business growth.

☐ AI and emerging technology vendors receive oversight.

☐ Vendor governance supports long-term resilience planning.

Scoring Results

40–50 Points — Strong Vendor Governance Maturity

Your organisation demonstrates strong vendor oversight, operational resilience, and governance accountability.

Continue refining:

- dependency visibility,
- operational coordination,
- and long-term resilience planning.

20–39 Points — Moderate Third-Party Exposure

Your organisation has foundational vendor governance practices but may still face:

- operational blind spots,
- dependency risk,
- or governance inconsistency.

Focus on:

- visibility,
- access control,
- incident preparedness,
- and governance maturity improvements.

0–19 Points — High Vendor Risk Vulnerability

Your organisation may face significant exposure involving:

- unmanaged vendor dependency,
- weak oversight,
- poor visibility,
- or insufficient operational resilience planning.

Immediate priorities should include:

- vendor inventory review,

- governance accountability,
- access management,

and operational dependency mapping.