Boardroom Digital Risk Readiness Assessment Checklist

Instructions

Use this assessment to evaluate your organisation's board-level digital risk governance and resilience maturity.

Score each item:

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

Governance & Oversight

☐ The board receives regular cybersecurity and digital risk updates.

☐ Digital risk responsibilities are clearly assigned.

☐ Executive leadership maintains visibility into operational cyber exposure.

☐ Governance committees oversee resilience and cybersecurity planning.

☐ Digital risk is discussed during strategic planning sessions.

Operational Resilience

☐ Critical operational systems and dependencies are documented.

☐ Incident response procedures are tested regularly.

☐ Backup and recovery processes are validated operationally.

☐ Crisis communication procedures are documented.

☐ Business continuity plans include cyber disruption scenarios.

Vendor & Third-Party Governance

☐ Third-party vendors undergo cybersecurity due diligence.

☐ Cloud provider dependencies are reviewed regularly.

☐ Vendor contracts address security and resilience obligations.

☐ Supply chain cybersecurity exposure is assessed periodically.

☐ Vendor oversight continues after procurement approval.

Human Risk & Organisational Culture

☐ Employees receive ongoing cybersecurity awareness training.

☐ Leadership actively supports cybersecurity governance initiatives.

☐ Reporting culture encourages rapid escalation of suspicious activity.

☐ Insider risk is addressed operationally.

☐ Governance communication remains clear and consistent.

Compliance & Strategic Readiness

☐ Digital compliance obligations are reviewed regularly.

☐ Governance documentation is maintained consistently.

☐ AI governance and emerging technology risks are evaluated.

☐ Cybersecurity metrics are reviewed at the board level.

☐ Continuous resilience improvement initiatives exist.

Scoring Results

40–50 Points — Strong Governance Maturity

Your organisation demonstrates strong digital risk governance, operational resilience, and leadership accountability.

Continue refining:

- governance visibility,
- vendor oversight,
- operational preparedness,
- and long-term resilience planning.

20–39 Points — Moderate Digital Risk Exposure

Your organisation has foundational governance practices but may still face operational and resilience gaps.

Focus on:

- strengthening oversight,
- improving preparedness,
- clarifying accountability,
- and enhancing operational visibility.

0–19 Points — High Governance Vulnerability

Your organisation may face significant operational exposure involving:

- weak governance,
- limited resilience planning,
- insufficient oversight,
- or poor operational visibility.

Immediate priorities should include:

- governance improvement,
- resilience planning,
- vendor oversight,

and executive accountability strengthening.