Template: Third-Party Cyber Risk Review

Purpose

To support board-level oversight of third-party and vendor cyber risk by providing a structured review template that helps identify material exposures, assess controls, and track assurance activities across the supply chain.

Intended Users

Boards, Audit & Risk Committees, CISOs, procurement leads, and any executives responsible for managing third-party relationships or cyber risk assurance.

Section 1: Key Vendor Inventory

List your critical third parties — those with access to sensitive data, system control, or core business continuity roles.

Vendor Name	Critical Function	Data Access Level	Geographic Risk (Yes/No)	Internal Owner

Section 2: Risk Assessment Summary

- What is the vendor's security posture (based on questionnaire, certification, or due diligence)?
- Any known breaches in the past 3 years?
- Do they subcontract key functions to others? Are those parties assessed?

Section 3: Controls and Assurance

Tick if the following are in place for each critical vendor:

- ☐ Cybersecurity clause in contract
- ☐ Right to audit
- ☐ Incident notification obligation
- ☐ Up-to-date third-party risk assessment
- ☐ Independent assurance (e.g. SOC 2, ISO 27001)

Section 4: Board-Level Questions

- Which vendors pose the greatest operational or reputational risk if breached?
- How does third-party risk integrate into our risk management framework?
- What assurance do we have that vendor controls are current and effective?
- How would we respond if one of these vendors suffered a material cyber incident?

Section 5: Actions and Follow-Ups

Track next steps to address third-party risks.

Action Item	Owner	Due Date	Status

Optional: AI Support Prompts

Use these prompts in your AI co-pilot to summarise or extend your vendor risk review:

- Summarise top 5 vendor-related risks based on risk register and contract data.
- Generate a board briefing note on our third-party cyber risk exposure.
- List vendors by data access level and recommend review priorities.
- Suggest follow-up actions for vendors lacking up-to-date assurance.