Institute of Directors Ireland

KNOW YOUR EXPOSURE

TOOL 1.2 · AI GOVERNANCE TOOLKIT

Vendor Dependency Review

DIRECTOR'S GUIDE

Most organisations rent AI rather than build it. This review tells the board which AI vendors it now depends on, how much it would hurt if one of them changed or failed, and what has been done about it.

2	13	1
Questions place any vendor in a tier	Questions to put to a vendor, with what a good answer looks like	Page to the board, once a year and when something changes

WHAT IS IN THIS GUIDE

IOD AI GOVERNANCE TOOLKIT · TOOL 1.2 · VERSION 1.0 · SEPTEMBER 2026

Use this guide with the inventory from **Tool 1, the Shadow AI Audit**. The audit lists the AI in use; this review names the vendors behind it.

OVERVIEW

Why this, and why now

Every AI tool in your organisation is someone else's product, sold under terms nobody has read since the day they were accepted. This review is a once-a-year look at who those vendors are.

It answers one board question: *which AI vendors could hurt us if they changed their product, their price or their terms, or if they failed or were breached, and what have we done about it?*

THE SIMPLE RULE

A vendor you could replace in a month is a supplier. A vendor you could not replace in a year is a **dependency**, and dependencies are a board matter.

WHAT MAKES AI VENDORS DIFFERENT

THE PRODUCT MOVES

Models are retired, often at a few months' notice

The version your team learned is replaced by one that behaves differently. Prompts and workflows built on the old one stop working quietly.

IT ARRIVES UNINVITED

AI switched on inside tools you already pay for

Office suites, CRM, HR and finance platforms now ship AI features that staff turn on themselves. Nobody made a purchasing decision about them.

IT TAKES ACTION

Tools that take actions in your systems

The newer products send emails and raise invoices on your behalf. A vendor change is then an operational change.

THE PROVIDER UNDERNEATH

Most products run on a handful of model providers

Your small Irish supplier passes through the pricing and outages of a large provider you have no contract with. That provider is the real dependency.

WHO DOES WHAT

One named executive holds the register, usually the CIO, Head of Procurement or Company Secretary. The leadership team answers the two tiering questions for each vendor: half a day the first time, about an hour a year after that, with the vendors' answers gathered beforehand. The board sees one page a year, the Critical vendors by name, and asks the four questions on the back page.

WHERE IT SITS IN THE TOOLKIT

The **Shadow AI Audit** (Tool 1) gives you the inventory this review starts from. The register then feeds the **EU AI Act Readiness Check** (Tool 1.3), which needs the vendor's documentation, and the **AI Use Policy** (Tool 2.1), which names the approved vendors. A **Strategic Radar** signal (Tool 5.1) naming a vendor is tested against this register.

STEP 1

Build the register and tier it

Start from the Shadow AI Audit inventory. Every product on it has a vendor behind it. One row per vendor, with each product or use listed beneath, and seven things recorded about each.

RECORD	WHAT TO WRITE DOWN
Vendor and products	Who you contract with, what you use, and which model provider sits underneath.
What it does for us	The process, in one line: "drafts client letters in the claims team" rather than "generative AI".
Who owns it	The executive accountable for that process. IT owns it only when IT is the user.
Data it touches	Client, employee, commercial or none. Whether personal data is included, and whether it leaves the EU.
How it arrived	Procured, switched on inside a platform you already had, or adopted by staff without sanction.
Contract position	Term, renewal date, notice period, and whether there is a contract at all. Click-through terms count.
People who know it	How many staff could run it tomorrow if the current user left.

TWO QUESTIONS PLACE EVERY VENDOR IN A TIER

QUESTION 1 · DISRUPTION

If this vendor changed or stopped tomorrow, what breaks, and how long would a replacement take?

A process stops, a year to replace **3** · Slower or dearer, months to replace **2** · Nothing much, weeks to replace **1**

QUESTION 2 · EXPOSURE

What of ours do they hold?

Client or employee personal data, or commercially sensitive material **3** · Internal working data only **2** · Nothing we would miss **1**

Add the two scores. **Any 3 on Question 1 is Critical whatever the vendor holds.** If the leadership team cannot agree between Material and Critical, it is Critical until the answers say otherwise.

Convenience · 2 – 3

Replaceable and holds nothing sensitive. Read the terms once and review annually.

Material · 4

Would cost time or money to lose, or holds data that matters. Core six questions answered and filed, export route confirmed.

Critical · 5 – 6, or any 3 on Q1

All thirteen questions answered in writing, exit plan tested, named to the board.

STEP 2

The questions to ask a vendor

Critical vendors answer all thirteen, in writing. Material vendors answer the core six, marked ●, plus 4 and 5 wherever the output affects a person. The line in italics is what a good answer looks like, as a guide rather than a pass mark.

- ☐ ● 1 · **Training data.** Will our client, employee or commercial data be used to train your models, by default or via opt-out? *Written clause, default off, named jurisdiction.*
- ☐ ● 2 · **Model change.** How and when do you change the underlying model, and how will we know when behaviour changes? *Release notes, a notice period, a way to roll back.*
- ☐ 3 · **Output integrity.** How do you detect outputs that degrade, drift or hallucinate, and how is that surfaced to us? *Logging, and a review path on our side. Ask how accuracy is tested.*
- ☐ 4 · **Fairness and bias.** How do you test for unfair or discriminatory outputs in our kind of use, and what would you show us? *A named method, evidence on cases like ours, open to independent review.*
- ☐ 5 · **Explainability.** When the model produces a material outcome, can we explain it to the person affected? *Plain reasons and an audit trail, rather than "the model decided".*
- ☐ 6 · **Productivity claims.** What is the basis for the gains you are claiming, in an engagement like ours? *A named reference, a like-for-like baseline, a time window.*
- ☐ ● 7 · **Security and data residency.** Where is our data processed and stored, and which sub-processors touch it? *Named processors, EU or UK residency option, certification in date and in scope.*
- ☐ ● 8 · **IP and liability.** Who owns outputs, and where does liability sit if they harm a third party? *Ownership stated, IP indemnity, an adequate liability cap. Ask what the model was trained on.*
- ☐ ● 9 · **Regulatory posture.** How are you evidencing compliance with the EU AI Act, GDPR and our sector rules, and what will you give us as a deployer? *A named compliance owner. Instructions for use and the deployer information the Act provides for. See Tool 1.3.*
- ☐ 10 · **Workforce impact.** How does this change the work, particularly for junior staff? *An honest conversation with a reference customer.*
- ☐ 11 · **Environmental footprint.** What is the energy and resource cost of how we would use you? *A per-query or per-unit estimate. Disclosure on water and energy where material.*
- ☐ ● 12 · **Exit.** If we leave in eighteen months, what happens to our data, our configurations and what our team has built? *Export format, deletion timeline, portable prompts and fine-tunes.*
- ☐ 13 · **Incident track record.** Walk us through your most recent material incident: what happened, how it was disclosed, what changed. *Willing, specific answers and evidence of change afterwards.*

HOW TO READ THE ANSWERS

A good vendor answers in writing and volunteers its limits. **An evasive vendor offers adjectives where documents and names should be.** If a Critical vendor will not answer in writing, record the refusal on the register as its answer.

STEP 3

Concentration, exit and the board page

Tiering looks at vendors one at a time. Two further tests look at the register as a whole, and they are the two a board is best placed to ask.

> **THE CONCENTRATION QUESTION**
>
> Count how many Critical and Material processes run, directly or through a supplier, on the same model provider or cloud platform. **If one provider changed its terms, price or model tomorrow, how many of our processes move at once?** More than two, and the board should know that provider's name, even though you have no contract with it.

THE EXIT TEST, FOR EVERY CRITICAL VENDOR

- [ ] **Data.** Can we export what they hold in a usable format, and have we tried?
- [ ] **Deletion.** What is their deletion timeline after termination, in writing?
- [ ] **Configuration.** Are our prompts, templates, fine-tunes and integrations documented outside the vendor's product?
- [ ] **Alternative.** Is there a named alternative or a manual fallback, how long would the switch take, and does it depend on a document or on one person?

WHEN TO LOOK AGAIN

TRIGGER	WHAT TO DO
Ownership, model or terms change	Acquisition, insolvency, a retired model, new pricing or a revised training-data clause. Re-tier inside the month.
Scope creep	A tool adopted by one team is now used by four. Re-score Question 1.
Incident	A breach or outage at the vendor or the provider behind it. Same day: the exit plan starts, and GDPR or sector notification duties run on their own clocks.
Renewal	Refresh a Critical vendor's thirteen answers before the contract renews, while you still have leverage.

THE BOARD PAGE, ONCE A YEAR

Five blocks. **The register at a glance**: vendors by tier, and movement since last year. **Critical vendors by name**: the process, the owner, diligence status, exit-plan status. **Concentration**: the providers behind the register and how many processes each carries. **Open items**: unanswered questions, renewals in the next twelve months, and anything needing a decision to accept, reduce or exit a dependency. **Next review**: the date, and the triggers that would bring it forward.

Keep each year's register and board page as dated copies. The series shows what the board knew about its AI supply chain, when, and what it did: the evidence of care, skill and diligence under section 228(1)(g) of the Companies Act 2014.

QUICK REFERENCE

One page to keep

QUESTION 1 · DISRUPTION

If this vendor changed or stopped tomorrow, what breaks, and how long to replace?

A process stops, a year to replace **3** · Slower or dearer, months to replace **2** · Nothing much, weeks to replace **1**

QUESTION 2 · EXPOSURE

What of ours do they hold?

Personal or commercially sensitive data **3** · Internal working data **2** · Nothing we would miss **1**

Convenience · 2 – 3

Review annually.

Material · 4

Core six questions on file.

Critical · 5 – 6, or any 3 on Q1

Named to the board. Exit plan tested.

FOUR QUESTIONS FOR A DIRECTOR TO ASK

Which vendors are Critical, and who owns each? · How many of our processes sit on one provider? · Could we get our data out, and have we tried? · Which Critical vendor has not answered us in writing?

THE SIMPLE RULE

A vendor you could replace in a month is a supplier. A vendor you could not replace in a year is a dependency, and dependencies are a board matter.

THREE RULES THAT DO NOT BEND

Doubt moves a vendor up a tier. A refusal to answer in writing goes on the register as the answer. **An incident at a Critical vendor is acted on the same day.**

IOD AI GOVERNANCE TOOLKIT · TOOL 1.2 · CATEGORY: KNOW YOUR EXPOSURE · VERSION 1.0

Institute of Directors Ireland