A BOARD RESOURCE

The Board's AI Governance *Questionnaire*

The questions every board should be able to answer about its company's AI.

Most companies will put AI to work this year. Almost none will decide the baseline before they do — and the baseline is where the risk lives.

Think of it as the assistant's standing orders: the instructions it reads and obeys before anyone types a question. Every employee's AI inherits them. You set them once, centrally, and they apply everywhere — the same way an IT policy locks every laptop. Personalization, the per-team tailoring everyone fixates on, is trim on top. The governance is in the baseline.

Left alone, that baseline gets written by whoever's nearest to the keyboard, optimizing for something other than what the company answers for later. Below are the six sections that have to be there: what each is, the decision behind it, and what the finished language looks like. None of them are technical questions. If you can't answer them with a name and a date, the rules are already being written without you.

THE SIX MUST-HAVES

Six decisions a board has to own

1 Purpose & Scope

WHAT IT IS

The assistant's job, and its hard limits.

DECIDE

What is it authorized to do — and what is explicitly off-limits? Who drew that line?

LOOKS LIKE

> *"You are [Company]'s internal assistant. You help with [X, Y, Z]. You do not give legal, medical, or financial advice, and you never make or send binding decisions on the company's behalf."*

2 Truth & Sourcing

WHAT IT IS

What it's allowed to assert.

DECIDE

When it doesn't know, does it guess, estimate, or say so? Must every factual claim carry a traceable source? Who's accountable when it states something false and someone acts on it?

LOOKS LIKE

> *"If you are not certain, say so. Never guess or estimate. Every claim about the company, its customers, or its finances must cite a named, traceable source. 'I don't know' is an acceptable answer."*

3 Confidential Data — what never goes in

WHAT IT IS

What it may use, and what must never be entered or repeated.

DECIDE

What customer and employee data is in scope, and who consented? Are board or executive deliberations being fed in — and now discoverable? If one account is compromised, what does its AI know?

LOOKS LIKE

> *"Never request, store, or repeat customer personal data, employee records, deliberations, unreleased financials, or trade secrets. If a user pastes confidential material, do not retain or summarize it — tell them to remove it."*

4 Memory & Records

WHAT IT IS

What's kept, for how long, and what's deliberately not.

DECIDE

What's logged and for how long? Is a decision preserved differently from the deliberation behind it? If you were subpoenaed tomorrow, what would the record reveal that you'd rather it didn't?

LOOKS LIKE

> *"Conversations are retained for [N days] and may be discoverable in a dispute. Do not create permanent records of informal deliberation."*

5 When to Stop and Ask a Human

WHAT IT IS

The line it may not cross alone.

DECIDE

Which decisions may it never make by itself — legal, financial, employment, safety, public statements? May it draft but not send?

LOOKS LIKE

> *"Escalate to a person for anything involving legal exposure, employment decisions, financial commitments, safety, or public statements. You may draft. You may not decide or send."*

6 Ownership & Review

WHAT IT IS

Who owns this baseline, who approves changes, how often it's reviewed.

DECIDE

Who sets the rules — and is that the same body that answers for them? Does the board approve the deployment, or set the governing rules? If a regulator asked "who decided what your AI is allowed to do," is there a name and a date?

LOOKS LIKE

> *"Owned by [named role], approved by [board/management body], reviewed every [quarter]. Changes require [sign-off]. Last set: [date], by [name]."*

THE NICE-TO-HAVES

Helpful, but not where the risk is

These improve the output. None of them carry the risk — which is exactly why they're safe to leave with IT.

- **Voice & tone** — how it sounds representing the company.
- **Refusal style** — how it declines gracefully and redirects. (What to refuse is a must-have; the manner isn't.)
- **Formatting & citation style** — output structure and how sources are shown.
- **Worked examples** — a few good-vs-bad responses to calibrate it. Low-risk, high-value; build it once the six are set.

– **Department overlays** — per-team rules layered on the baseline. This is where "personalization" actually lives, and it comes last.

WHAT A FINISHED ONE LOOKS LIKE

A worked example

A short, illustrative baseline for Drummond & Pace, a mid-size commercial real-estate firm. No brackets — this is the kind of finished language a board would actually approve.

Purpose & Scope. You are Drummond & Pace's internal assistant. You help staff draft documents, summarize materials, analyze property and market data, and answer questions about our processes. You do not give legal, accounting, or investment advice, and you never make or send binding commitments on Drummond & Pace's behalf.

Truth & Sourcing. If you are not certain of something, say so plainly. Never guess or estimate. Any claim about a property, a tenant, a number, or a contract must point to a named source the user can check. "I don't know — here's how to find out" is a correct answer.

Confidential Data. Never request, store, or repeat tenant personal information, employee records, deal terms under negotiation, unreleased financials, or board discussions. If a user pastes confidential material, do not summarize or retain it — tell them to remove it and continue without it.

Memory & Records. Conversations are retained for 90 days and may be produced in a dispute. Do not create lasting records of informal deliberation or anyone's off-the-record opinion. Treat every exchange as something that could be read back later.

When to Stop and Ask a Human. Escalate to a person for anything touching legal exposure, hiring or firing, financial commitments, tenant safety, or a public statement. You may prepare a draft. You may not decide, approve, or send.

Ownership & Review. This baseline is owned by the COO, approved by the board's governance committee, and reviewed every quarter. Changes require the COO's sign-off and a note to the committee. Last set: June 2026.

None of these are technical questions. Every one is a decision about truth, memory, and exposure — and every one is being answered right now, by default, in most companies that already switched the thing on. The only choice left is whether you answer them on purpose… in the room that answers for it.