

## Eight Questions Every SME Board Should Ask About AI Risk

01

### QUESTION 01

#### What AI tools are already in use across your business, and who actually knows?

Most businesses that have not formally adopted AI are still using it. Staff use ChatGPT to draft documents, Copilot to summarise emails, AI writing tools to produce content, and AI-assisted features built into standard software they already have. The question is not whether AI is present, it almost certainly is. The question is whether leadership knows which tools, used by whom, and handling what data. An AI audit does not need to be complex, a brief staff survey will typically surface the tools in use within days. What most businesses find surprises them.

**Why it matters:** You cannot govern what you cannot see.

02

### QUESTION 02

#### What data is your business sending to AI tools, and where does it go?

When a member of staff pastes a client contract into ChatGPT or uploads a customer list to an AI tool, they are sending that data to a third-party system. In many cases, that data may be used to train the AI model, stored on servers outside the UK, or processed in ways the business has not consented to or disclosed to its clients. This is not hypothetical risk, it is the day-to-day behaviour in many businesses, with real implications under UK GDPR and real reputational consequences if a client discovers their data was handled this way.

**Why it matters:** Data sent to an AI tool may never truly come back.

03

### QUESTION 03

#### Do you have an AI acceptable use policy, and does it actually work?

Many businesses have responded to the AI question by writing a policy. Fewer have a policy that staff have read, understood, and are genuinely following. A policy buried in a staff handbook or issued as a one-time email is not governance, it is documentation that gives the appearance of governance without the substance. An effective AI acceptable use policy is short enough to be read, specific enough to be followed, and reinforced through team discussions and periodic reminders. It should tell staff clearly what they may and may not use AI for, and what to do if they are unsure.

**Why it matters:** A policy nobody follows is not a policy. It is a liability.

04

### QUESTION 04

#### What are your obligations under UK GDPR when staff use AI with personal data?

Under UK GDPR, your business is responsible for how personal data is processed, including when that processing is carried out by a third-party AI tool your staff are using. If a member of staff submits personal data to an AI system that processes it outside the UK or uses it for model training, your business may be in breach of its data protection obligations, even if it was not aware of the submission. Boards should understand the basics: what constitutes personal data, what a data processing agreement is and when one is needed, and what the ICO's current guidance on AI says.

**Why it matters:** Ignorance of the rules does not protect you from the consequences.

## Eight Questions Every SME Board Should Ask About AI Risk

05

QUESTION 05

### What is your exposure to reputational or legal risk from AI-generated content?

AI-generated content (documents, emails, proposals, marketing copy) can contain errors that a human author would not make: factual inaccuracies, invented references, confident claims that are simply wrong. When that content goes out under your business's name, the reputational consequence is yours, regardless of how it was produced. There is also a question of originality. AI tools generate content by drawing on their training data, which in some cases may be substantially similar to copyrighted material, creating potential IP exposure. For businesses in regulated sectors, AI-generated content may need additional scrutiny before publication or submission.

**Why it matters:** Your business is responsible for everything it publishes, whatever produced it.

06

QUESTION 06

### Does your AI governance match the actual scale of your AI use?

Governance does not mean complexity. For most SMEs, proportionate AI governance is three things: a clear policy that staff understand and follow; a named individual with responsibility for keeping that policy current; and a simple process for reviewing and approving AI tools before they are adopted. It does not require a dedicated AI team or expensive software. It requires deliberate decisions made by leadership, communicated clearly, and revisited regularly as the landscape evolves. The businesses that get this right are typically the ones that treat AI governance as a leadership question, not a technical one.

**Why it matters:** Under-governed AI use creates compounding risk that is hard to unwind once embedded.

07

QUESTION 07

### Which AI opportunities are actually relevant to your business, and have you evaluated them?

The AI conversation is often framed around large enterprises and complex implementations. For most SMEs, the practical opportunities are more modest and more immediate: automating repetitive tasks, improving the quality and speed of written communication, handling customer enquiries, analysing data that currently sits unread in spreadsheets. The question is not whether AI is relevant to your business, it almost certainly is. The question is which applications will actually deliver value, and how to adopt them in a way that does not create the risks covered in this guide. An honest assessment of where time is currently wasted is usually the best place to start.

**Why it matters:** Businesses that ignore AI entirely are also falling behind. The goal is informed adoption, not avoidance.

08

QUESTION 08

### Who is accountable for AI risk at board or leadership level in your business?

This is the question that most directly predicts whether a business will manage AI well or poorly. When nobody owns AI risk at leadership level, policy does not get written, tools do not get reviewed, and the business discovers its exposure only after something goes wrong. AI accountability at board level does not require a technical expert. It requires a leader who takes the question seriously, ensures the right conversations happen, and is prepared to be the named individual when a client, auditor, or regulator asks who is responsible. In most SMEs, this will be the MD, CEO, or a non-executive director with a relevant background.

**Why it matters:** When everyone is responsible for AI risk, nobody is.

## Eight Questions Every SME Board Should Ask About AI Risk

### If these questions are difficult to answer, you are not alone.

Most SME boards have not yet had a structured conversation about AI risk. The tools are being used, the data is being shared, and the exposure is growing, but the governance conversation has not kept pace. Northstar works with SME boards and leadership teams to close that gap: understanding current AI exposure, building proportionate governance, and identifying the AI opportunities that will actually deliver value.

#### 01 **AI Readiness & Advisory**

An independent review of your current AI exposure, policy gaps, and quick wins, delivered as a clear, prioritised report for leadership.

#### 02 **AI Governance & Policy**

A proportionate AI governance framework built for your business, covering policy, accountability, tool approvals, and staff communication.

#### 03 **Fractional IT & Cyber Director**

Ongoing independent IT and cyber leadership, including AI governance, for businesses that do not have a CTO or IT director.

#### **Get in touch**

[northstaritadvisory.com](https://northstaritadvisory.com)

[cs@northstaritadvisory.com](mailto:cs@northstaritadvisory.com)

0333 577 1714