The SMB AI Governance Checklist

25 Questions to Assess Whether Your Business Is Using AI Responsibly

Most small and medium businesses have adopted AI tools faster than they've developed policies to govern them. This checklist helps you identify gaps before they become problems—whether that means regulatory fines, data breaches, reputational damage, or operational failures.

How to Use This Checklist

Work through each question honestly. For any "No" or "Unsure" answer, note it as an area to address. At the end, you'll have a clear picture of where your AI governance stands and what needs attention. This assessment typically takes 15-20 minutes to complete thoroughly.

Prepared by

SAFETY PINNACLE

AI Governance for Growing Businesses

Section 1: Visibility and Inventory

You can't govern what you don't know exists.

#	Question	Yes	No	Unsure
1	Do you have a complete inventory of all AI tools currently used in your business (including tools employees may have adopted independently)?			
2	For each AI tool, do you know what data it has access to?			
3	Do you know which employees are using AI tools and for what purposes?			
4	Are you aware of any AI features embedded in software you already use (e.g., AI in your CRM, email platform, or analytics tools)?			
5	Do you have a process for employees to report or request approval for new AI tools?			

> ***Why this matters:*** *Many businesses discover AI is being used in ways they weren't aware of—often involving sensitive customer or business data. Shadow AI (unauthorised tool adoption) is one of the most common sources of risk.*

Section 2: Data Handling and Privacy

AI tools often process, store, or learn from your data in ways that may surprise you.

#	Question	Yes	No	Unsure
6	Have you reviewed the data retention and usage policies of each AI tool you use?			
7	Do you know whether the AI tools you use train their models on your inputs?			
8	Have you assessed whether your AI use complies with GDPR (or other applicable data protection regulations)?			
9	Do you have controls preventing employees from inputting personal customer data into AI tools?			

#	Question	Yes	No	Unsure
10	If you process data from EU citizens, have you evaluated your AI tools against EU AI Act requirements?			

Why this matters: *Many AI tools (particularly free tiers) use customer inputs to train models, meaning your confidential data could influence outputs shown to competitors. Data protection regulators are increasingly scrutinising AI-related processing.*

Section 3: Policies and Governance

Clear policies prevent well-meaning employees from creating risks accidentally.

#	Question	Yes	No	Unsure
11	Do you have a written AI acceptable use policy that employees have acknowledged?			
12	Does your policy clearly state what types of data can and cannot be entered into AI tools?			
13	Do you have guidelines for how AI-generated outputs should be reviewed before use?			
14	Is there a clear process for evaluating and approving new AI tools before adoption?			
15	Have you designated someone responsible for AI governance in your organisation?			

Why this matters: *Without clear policies, employees make individual judgments about appropriate AI use—often with good intentions but incomplete understanding of risks. "I didn't know I wasn't supposed to" is not a defence regulators accept.*

Section 4: Quality and Reliability

AI tools can fail, hallucinate, or produce biased outputs—often confidently.

#	Question	Yes	No	Unsure
16	Do you have processes to verify AI outputs before they're used in decisions or shared externally?			
17	Have you tested your AI tools for accuracy in your specific use cases?			
18	Do you have fallback procedures if AI tools become unavailable or produce unreliable results?			
19	If AI is involved in decisions affecting people (hiring, lending, customer service), do you have human oversight built in?			

#	Question	Yes	No	Unsure
20	Are employees trained to recognise and handle AI errors or hallucinations?			

Why this matters: *AI systems can generate plausible-sounding but entirely false information. Businesses have faced legal and reputational consequences for acting on AI outputs without verification—including a law firm sanctioned for citing non-existent cases generated by ChatGPT.*

Section 5: Transparency and Accountability

Regulators, customers, and partners increasingly expect clarity about AI use.

#	Question	Yes	No	Unsure
21	Do customers know when they're interacting with AI rather than humans?			
22	Could you explain to a regulator or auditor how AI-assisted decisions in your business are made?			
23	Do your contracts with customers and suppliers address AI use where relevant?			
24	Have you reviewed your insurance policies to understand coverage (or exclusions) related to AI?			
25	Do you have documentation that would demonstrate responsible AI governance if questioned?			

Why this matters: *Regulatory frameworks globally are moving toward requiring transparency about AI use. The EU AI Act, for instance, mandates disclosure in many contexts. Being unable to explain your AI governance is increasingly a liability.*

Scoring Your Results

Count your "No" and "Unsure" responses to determine where your organisation stands:

Score Range	Assessment	Recommendation
0-5	**Strong foundation**	You're ahead of most SMBs. Focus on continuous improvement and staying current as regulations evolve.
6-12	**Moderate gaps**	You have some governance in place but meaningful blind spots that warrant attention before they become problems.
13-19	**Significant exposure**	Your business likely has material risks that should be addressed promptly. Consider prioritising an AI governance review.

Score Range	Assessment	Recommendation
20-25	**Urgent attention needed**	Your AI use may be exposing your business to substantial legal, financial, and reputational risks. Professional guidance is strongly recommended.

Your Score: ______ No responses + ______ Unsure responses = ______ Total

Common Gaps We See

Based on working with SMBs on AI governance, these are the issues that surface most frequently:

No inventory of AI tools in use. Most businesses significantly undercount their AI exposure because they don't think of embedded AI features (like Microsoft Copilot, AI in their CRM, or AI-powered analytics) as "AI tools."

Employees using AI with sensitive data. Staff often input customer information, financial data, or strategic documents into AI tools without realising the privacy implications.

No written policies. Verbal guidance like "be sensible" doesn't protect you when something goes wrong. Regulators and courts look for documented policies and training.

Over-reliance on AI outputs. Speed gains from AI often come with reduced scrutiny of outputs, leading to errors that wouldn't have happened with traditional processes.

No human oversight on consequential decisions. When AI influences decisions about people—hiring, credit, customer treatment—lack of human review creates both ethical and legal exposure.

Next Steps

If this checklist has identified gaps you'd like to address, you have several options:

Self-service

Many governance improvements can be implemented internally. Start with creating an AI inventory and drafting a basic acceptable use policy. Resources are available online, though quality varies significantly.

Professional guidance

For a comprehensive assessment and implementation support, consider working with an AI governance specialist who understands SMB constraints and can help you prioritise effectively.

Free Consultation

I offer a limited number of complimentary 25-minute AI risk assessments each month. In this session, we'll review your checklist responses, identify your highest-priority risks, and discuss practical next steps—whether that involves working together or not.

To schedule your free assessment:
Email: [your email]
Website: [your website]
LinkedIn: [your LinkedIn URL]

—

SAFETY PINNACLE

AI Governance for Growing Businesses

Helping small and medium businesses use AI confidently—
without the legal, financial, or reputational risks that come from getting it wrong.