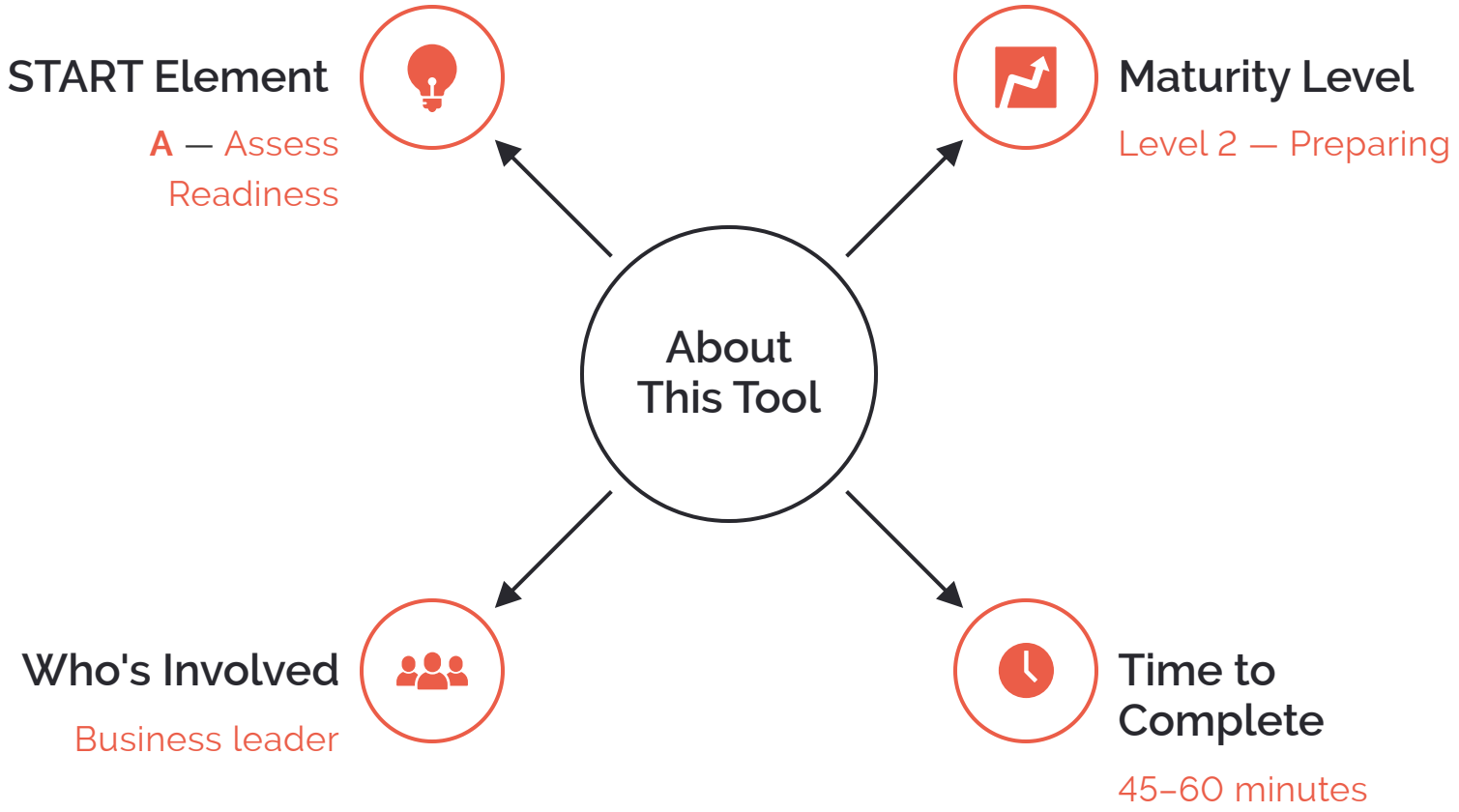
AI Governance Guardrails

Simple, practical rules for using AI responsibly in your business — whatever your size.

The Strategic Mind
START SMART. STAY STRATEGIC

AI Governance Guardrails

The practical rules every SME needs before AI goes anywhere near a pilot — or a client.



What you'll leave with: A clear set of practical AI rules for your business — and confidence that you're using AI responsibly.

AI Governance Guardrails

Practical rules for using AI responsibly in your business — whatever your size

What is it?

A plain English checklist of the minimum rules every SME should have in place before using AI in their business. No legal jargon. No complex frameworks. Just five practical guardrails — and a clear picture of where you stand..

Why Use it?

78% of SMEs are already using AI daily. Fewer than 23% have any governance in place. That gap is where data breaches, client incidents, and reputational damage happen. This closes it.

Benefits

Five clear guardrails that protect your business, your team, and your clients — without needing a compliance team, a legal budget, or a technical background.

The Strategic Mind
START SMART. STAY STRATEGIC

Governance isn't for large organizations.

It's for any business using AI.

You're probably already using it

ChatGPT, Copilot, Grammarly, CRM tools, accounting software. Most SMEs use five or more AI tools without any rules.

Small business doesn't mean small risk

A data breach or client incident can damage a small business as severely as a large one.

You don't need a compliance team

SMEs need practical plain English rules that can be implemented immediately, not enterprise frameworks.

The biggest risk isn't reckless AI use. It's thoughtless AI use — without any agreed rules at all.

Establish Your AI Inventory

Before you set rules — understand what you're setting rules for.

Build a simple AI inventory

List every AI tool your business uses, including tools with AI built in (e.g., accounting, email, CRM, design). Most businesses are surprised by how long the list is.

Ask three questions for each tool

For each tool, ask: What data goes in? Who uses it? What does it produce? These answers reveal your governance gaps.

Why this matters

You can't govern what you haven't mapped. An AI inventory is the first step every governance framework recommends. For an SME it takes 20 minutes.

You can't set rules for tools you don't know you're using. Start with the inventory.

Why AI Governance Matters for SMEs

Reputation is Everything

A single AI incident can severely damage relationships and brand trust.

Limited Safety Nets

Most SMEs lack extensive legal and compliance teams to navigate AI risks.

Team Culture

Clear governance provides direction, preventing ad-hoc judgments and aligning team behavior.

Client Trust

Transparent governance builds confidence as clients increasingly inquire about AI usage.

Governance isn't about slowing down. It's about not having to stop.

Your Five Guardrails for AI Use

Essential principles for every SME.

Five Simple Rules for Every SME and AI Use

1. Know AI Use Cases

Clearly define agreed-upon uses and explicitly state what is off-limits.

2. Data Sensitivity Awareness

Understand which data is safe to input and recognize the distinction between safe and unsafe data.

3. Mandatory Human Review

Always review AI-generated drafts before final use; humans are responsible for final outputs.

4. Incident Response Plan

Have a simple, clear plan for what actions to take when something goes wrong.

5. Continuous Updates

Regularly update your AI usage rules to keep pace with the evolving nature of AI technology.

THESE AREN'T OPTIONAL. THEY'RE THE MINIMUM.

The Strategic Mind
START SMART. STAY STRATEGIC

Guardrail 1: Know What AI Can Be Used For

Decide what's in — and what's out.

- **Approved Tools & Tasks**

  Clearly define which AI tools and tasks are permitted for use.

- **New Tool Approval Process**

  Establish a clear procedure for approving new AI tools.

- **Communication of Rules**

  Ensure all AI usage guidelines are effectively communicated to the team.

- **Examples**

  Provide concrete examples of acceptable and unacceptable AI usage (e.g., 'Use Claude for drafting,' 'No client-facing AI without senior review').

- **Policy Scaling**

  Adapt the AI policy based on business size, starting with simple guidelines for small businesses and evolving to more detailed policies for larger ones.

The goal is not to restrict AI, but to ensure everyone uses it the right way.

Guardrail 2: Know What Data Can Go In

Not all data is safe to share with an AI tool.

- **Free Tools May Store Inputs**
  Be aware that free AI tools might store the data you input.
- **Clear Rules for Input**
  Establish and follow clear rules on what data should never be shared.
- **Enterprise Tools for Sensitive Data**
  Utilize enterprise-level AI tools for handling sensitive information.
- **Check Privacy Settings**
  Always verify and adjust privacy settings before using any AI tool.
- **Data Sensitivity Guide**
  Use the Green-Amber-Red guide to classify data before sharing.

When in doubt, leave it out. Once data is in a public AI tool, you cannot take it back.

Guardrail 3: Always Review Before You Use

AI produces drafts. Humans produce finals.

- **AI Outputs as First Drafts**

  Treat all AI-generated content as preliminary and requiring human oversight.

- **Client-Facing Content Review**

  Ensure all external communications are thoroughly reviewed by a human before dissemination.

- **Recommendation Accuracy**

  Verify the accuracy and suitability of any AI-generated recommendations before implementation.

- **Awareness of AI Confidence**

  Understand that AI can present information confidently, even when incorrect.

- **Review Levels**

  Categorize review intensity based on content type: Full (Red), Spot Check (Amber), Light Touch (Green).

Your name goes on the output—not the AI's. Act accordingly.

Guardrail 4: What to do when something goes wrong

Plan for it now. Not after it happens.

- **Team knows who to tell**

  Ensure clear lines of communication for any issues or incidents.

- **Process to stop using a tool**

  Have a defined procedure for decommissioning or suspending tool usage.

- **Data exposure obligations understood**

  All team members understand their responsibilities regarding data privacy and security.

- **At least one scenario planned for**

  Develop contingency plans for at least one potential negative event.

A plan you never need is cheaper than a crisis you weren't prepared for

Keep it Updated

AI changes rapidly. Your rules need to keep up.

Review Date

Set a minimum review cadence of every six months for your AI rules, marked in your diary.

Update Process

Establish a clear process for updating rules whenever new AI tools are adopted.

Communication

Ensure rule changes are promptly communicated to the entire team.

Incident Review

Conduct a review of rules after any AI-related incident occurs.

Review Questions

New tools adopted? Privacy settings changed? Any incidents? Does the team know the rules?

Set the review date now. Before you leave this session.

Your Guardrails Summary

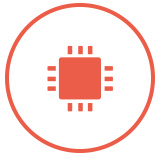
Map out where do you stand right now?

Guardrail 1: Approved uses

Status Pill: Green - In place, Amber - Partially, Red - Not yet.

Guardrail 2: Data rules

Status Pill: Green - In place, Amber - Partially, Red - Not yet.



Guardrail 3: Review process

Status Pill: Green - In place, Amber - Partially, Red - Not yet.

Guardrail 4: Incident plan

Status Pill: Green - In place, Amber - Partially, Red - Not yet.

Guardrail 5: Review date set

Status Pill: Green - In place, Amber - Partially, Red - Not yet.

Red statuses must be addressed before your pilot starts. Amber statuses have a 30-day deadline.

The Strategic Mind

START SMART. STAY STRATEGIC

"A few simple rules before you start protects your business, your clients, and your reputation. Governance isn't the obstacle. It's the insurance."

Peter Buckley, Senior Advisor, Technology & Cyber Risk · The Strategic Mind

A Note on Regulation

What regulatory obligations actually apply to your business.

Most regulation targets builders — not users

The EU AI Act and similar frameworks primarily target organisations that develop and deploy AI systems — not businesses using off-the-shelf tools like ChatGPT or Copilot for everyday tasks.

Data protection law always applies

GDPR in the UK and EU. PIPEDA in Canada. Regardless of how you use AI — if personal or client data goes into a tool, data protection rules follow it. This is the most immediate obligation for most SMEs.

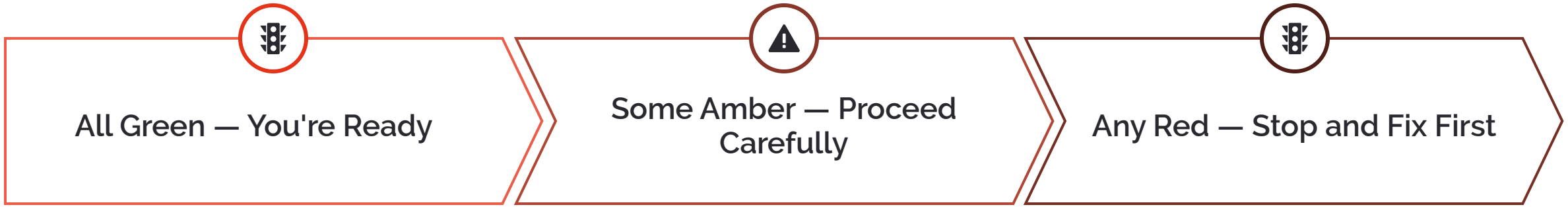
Sector-specific rules add another layer

Finance, healthcare, legal, and HR have additional obligations — particularly around automated decision-making and client data. If your use case touches these areas — seek advice before proceeding.

When in doubt — seek advice before you deploy. A short conversation with an expert is cheaper than the alternative.

What to Do Next

Guardrails in place. Ready to move forward.



Return to your Pilot Brief and confirm the governance section. Your pilot can begin.

Start your pilot but set a 30-day deadline to close the gaps. Don't let partial become permanent.

Address the gap, update your checklist, and come back when it's resolved.

Responsible AI isn't a constraint on ambition. It's the foundation for it.

The Strategic Mind

START SMART. STAY STRATEGIC