01 / THE CASE FOR A GOOD TO GO DAY

AI is accelerating. Who is in control?

The safety debate has reached the frontier of AI development. For business leaders, it raises a nearer question: can organisational control keep pace with everyday adoption?

Capability and governance move at different speeds. A new model can reach employees overnight; agreeing data boundaries, testing decisions and assigning accountability takes deliberate work. Our argument is that this gap should be managed before it becomes embedded in the way a business operates.

ANTHROPIC / THE FRONTIER

“We must slow the pace at which we improve the capabilities of AI models.”

Dario Amodei, September 2026 [1]

His proposal seeks time for safeguards and independent evaluation to catch up. This concerns frontier development, not a call for SMEs to stop all AI use.

OPENAI / HUMAN CONTROL

“Human intervention is a critical safeguard”

A practical guide to building agents, p.31 [2]

OpenAI recommends escalation when agents exceed failure thresholds, and human oversight for sensitive, irreversible or high-stakes actions until reliability is established.

THE MANAGEMENT GAP IS ALREADY VISIBLE

71% of UK employees surveyed reported using unapproved consumer AI tools at work. Microsoft-commissioned Censuswide survey, October 2025; 2,003 employees, including large employers and the public sector. [4]

FROM PERSONAL EXPERIMENT TO BUSINESS PROCESS

A tool used to draft a paragraph may later be connected to customer records or allowed to take actions. Each change in data access or authority deserves a fresh risk decision.

OUR IMPLICATION FOR SMEs

AI adoption is already in motion. The practical response is to put steering, checks and a way to stop in place: know the tools, limit access, verify consequential outputs and name the person accountable. The longer unmanaged use spreads, the more there may be to untangle.

02 / THE RISKS INSIDE YOUR BUSINESS

Your team is using AI. Who is managing the risk?

Rules, oversight and training are not yet universal.
A missing written policy alone does not establish unsafe practice.

ONLY / A WRITTEN POLICY

17%

of UK small businesses using AI reported a formal written AI policy. 10-49 employees. [3]

UNAPPROVED AI USE

71%

of UK employees surveyed reported using unapproved consumer AI tools at work. [4]

ONLY / RECENT TRAINING

35%

of UK employers surveyed provided generative AI training and support in the preceding 12 months. [6]

WHAT THAT CAN MEAN FOR YOUR BUSINESS

- ✓ **Data leaves your control.** Client details, pricing or contracts enter tools without an approved data boundary.
- ✓ **Errors become decisions.** Unverified outputs can affect clients, hiring and financial decisions. People still need to verify what AI produces.
- ✓ **Nobody owns the response.** Without a named owner and escalation route, mistakes can go unreported and recur.

CUSTOMER COMMUNICATIONS

“AI gets it wrong quite a lot of times”

A micro retailer described AI errors affecting refunds and advertising. West Midlands. [5]

PROTECTING BUSINESS INFORMATION

“The main challenge has been security of data and intellectual property”

A large retailer discussed keeping data inside the organisation. London. [5]

Attributed excerpts from anonymous UK research interviews; not client testimonials.

EVIDENCE / SCOPE MATTERS

DSIT: small AI-using businesses, Oct 2025-Jan 2026. Microsoft/Censuswide: 2,003 UK employees, Oct 2025. CIPD: UK employers, autumn 2025. The latter two cover wider employer sizes, not SME-only samples. Sources [3, 4, 6] on page 4.

03 / THE FOUNDATIONS OF READINESS

Good governance. Human confidence.

A policy in a folder is only a start. Your people need clear boundaries, usable tools and the judgement to know when to stop and ask.

Informed by DSIT's voluntary AI Management Essentials guidance. [8]

SIX FOUNDATIONS TO PUT IN PLACE

- **Know your AI use.**
  Record tools, accounts, data and business use cases.
- **Set practical boundaries.**
  Approve tools and define permitted data, access and acceptable use.
- **Assess the risks.**
  Prioritise privacy, security, accuracy, IP and fairness risks; decide where to pause.
- **Make accountability visible.**
  Name decision owners, human review points and an incident escalation route.
- **Prepare your people.**
  Train staff to verify outputs, protect information and recognise unsafe requests.
- **Test, evidence and revisit.**
  Trial real use cases, resolve critical gaps and review new tools and changed uses.

GOOD TO GO READINESS CERTIFICATION

Our own programme assessment records whether agreed controls are evidenced and tested at handover. Certification requires the six foundations above, closure of critical gaps and leadership sign-off. The statement records scope, evidence, remaining risks and a review date.

A proprietary assessment, not accredited certification, legal clearance or a guarantee of risk-free AI.

THE GOOD TO GO PRINCIPLE

Enough governance to make AI safer. Not so much that nobody uses it.

Clear boundaries. Prepared people. Room to move.

Explore your programme and plan your next step.

Review from £5,000 | Governance from £13,500. Final pricing confirmed after scoping.

04 / TURN READINESS INTO A COMMITMENT

Set your GOOD TO GO Day.

A date for having the foundations in place.
A process for keeping them there.

Make readiness a leadership commitment with an owner, evidence and a review cycle. NIST treats AI risk management as a voluntary practice across design, development, use and evaluation; UK AI Management Essentials offers an SME-focused starting point. [7, 8]

MAKE THE DATE MEAN SOMETHING

01 **START NOW**

Appoint a senior owner. Establish the AI use register and address the highest-risk uses immediately.

02 **BUILD TOWARDS YOUR DATE**

Put the six foundations on page 3 into practice. Test the rules with real work, train the team and close critical gaps.

03 **SIGN OFF AND KEEP REVIEWING**

Record the scope, evidence and remaining risks. Agree the next review date and reassess when tools, access or use cases change.

THE GDPR PARALLEL: ACCOUNTABILITY

Know where data goes and who is responsible. Data protection duties already apply when AI processes personal data. This is an existing responsibility, not a future AI deadline. [9]

OUR RECOMMENDED TARGET

SUMMER 2027

Choose your date. Assign an owner. Address your highest-risk uses now, with us or another qualified provider.

This is GOOD TO GO's planning recommendation, not an official deadline or a point of no return. Readiness requires ongoing review; it does not remove all risk.

Set your date. Explore the GOOD TO GO programmes. ↗

1 Amodei, We Must Pace the Frontier (Sep 2026)
2 OpenAI, Building agents, p.31 (2025)
3 DSIT, UK Business Data Survey, section 3.4 (2026)
4 Microsoft / Censuswide, Shadow AI (Oct 2025)
5 DSIT, AI Adoption Research, section 6 (2026)
6 CIPD, GenAI training; autumn 2025 survey (Jan 2026)
7 NIST, AI Risk Management Framework
8 DSIT, AI Management Essentials (Feb 2026)
9 ICO, AI and data protection (under review)