

SOVEREIGN AI OPTIONS REPORT | SMALL BUSINESSES, UNDER 500 EMPLOYEES

Sovereign AI options for Example Trading Ltd

Where your information goes today, three ways to run AI you control, the set-up we recommend and the route to get there.

PREPARED FOR
Example Trading Ltd, Leeds
(fictional)

PREPARED BY
AI Assist

DATE
October 2026

STATUS
Sample, version 1.0

Summary

THE QUESTION

Can Example Trading give its 46 staff useful AI without sending customer and supplier information somewhere it can't see or control?

OUR RECOMMENDATION

Yes. Run a private assistant in Example Trading's own cloud tenancy, in a UK region, on an open-weight model. Prove it with eight named users before building more. Keep a business-account public AI service for public content only, and stop using personal AI accounts for work.

9 of 31 staff

who answered our survey use personal AI accounts for work, some of them with supplier contracts pasted in.

3 AI services

already receive company data. Only one of them runs on terms anyone at Example Trading has reviewed.

0 contracts

require on-site processing today. A private cloud tenancy gives the control needed, with far less to run.

DECISIONS WE NEED FROM YOU

1 Approve the data boundary and the rule for each type of information
Managing Director, before station 1 ends

2 Name a service owner and an operator
Operations Director, before station 1 ends

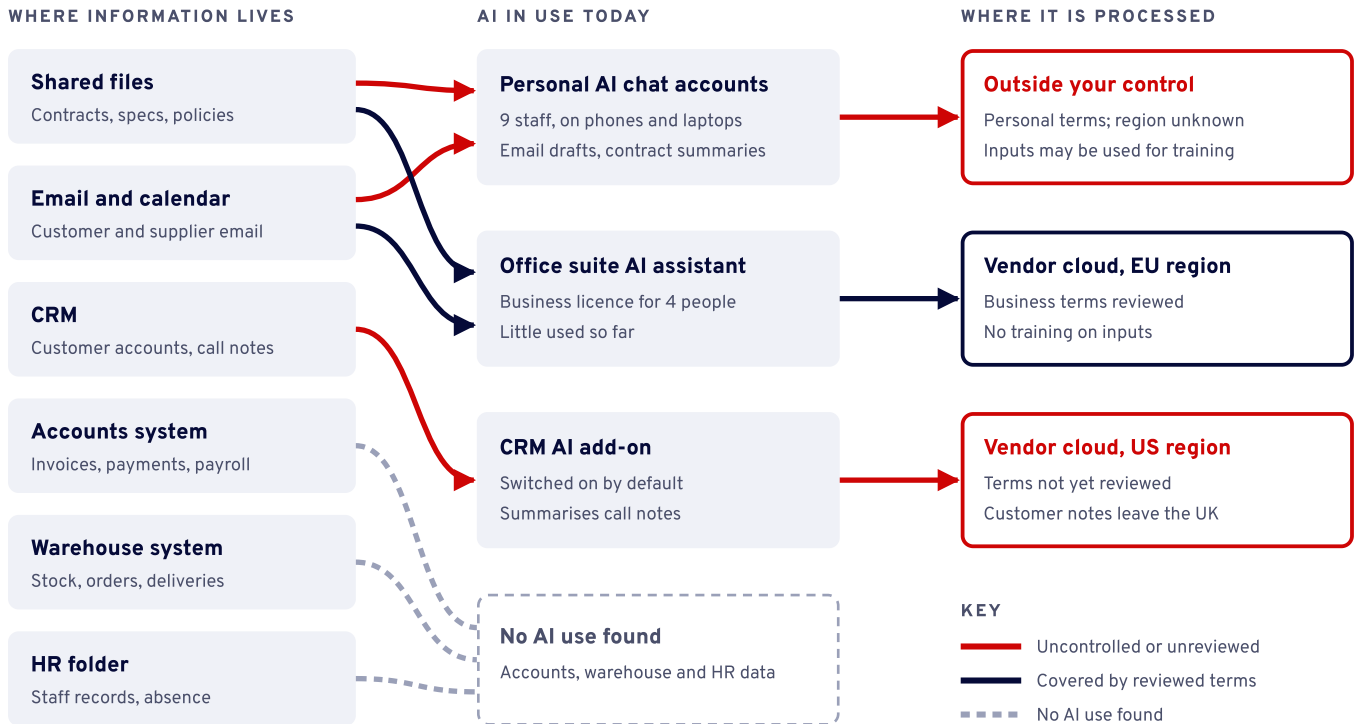
3 Choose the eight pilot users
Sales and Customer Service leads, before station 2

4 Set the date personal AI accounts stop being used for work
Managing Director, before station 4

1 | CURRENT STATE

Where your information lives, and where AI touches it

We interviewed six people, surveyed staff (31 of 46 replied) and reviewed the AI settings in five systems. The map shows every route we found from company information to an AI service.



INFORMATION	LIVES IN	SENSITIVITY	AI USE TODAY	BOUNDARY RULE
Supplier contracts	Shared files	Commercially sensitive	Personal accounts, office AI	Must stay inside
Customer accounts and call notes	CRM	Personal data	CRM add-on, US region	Must stay inside
Customer and supplier email	Email	Confidential	Personal accounts, office AI	Must stay inside
Product specifications and manuals	Shared files	Internal	Personal accounts, office AI	Inside by choice
Staff records	HR folder	Personal, health data	None	Out of scope for now
Website and brochure copy	Website	Public	Personal accounts	Public service is fine

Personal accounts fill a gap

People use them because they're quick and nobody offered an alternative. Banning them without a replacement would push the use out of sight.

Settings nobody chose

The CRM add-on was switched on by default. Nobody at Example Trading decided to send call notes to a US region.

Value sits in two collections

Most of the help staff asked for draws on product specifications and supplier contracts. That is where the pilot should start.

2 | OPTIONS APPRAISAL

Three ways to run AI you control, judged on the same work

Each option was judged on one job: answering staff questions from product specifications, supplier contracts and policies, for up to 12 people at once, with answers that show their sources.

	OPTION A	OPTION B RECOMMENDED	OPTION C
	Public AI service on a business account	Private AI in your own cloud tenancy	AI on a server at your own premises
Where it runs	The vendor's cloud, in a region set by the vendor's plan	Your own tenancy, in a UK region you choose	A server in the Leeds office
Control over your data	Partial Settings and terms belong to the vendor	High Your tenancy, your keys, your rules	Highest Nothing needs to leave the building
Training on your data	Off, if set up right Business terms only; personal accounts differ	None An open-weight model you run	None An open-weight model you run
Effort to set up	Low Accounts, settings and a usage policy	Medium Tenancy, sign-in, document library and tests	High Hardware, power, cooling and physical security
Effort to run	Low The vendor runs it	Medium A named operator and monthly updates	High Patching, backups, spares and capacity are all yours
Residual risk	Medium Depends on vendor terms and on settings staying right	Low Boundary tested; the cloud platform handles resilience	Medium One site; recovery depends on your own team
Showing where data goes	Limited You see what the vendor chooses to report	Full Every flow mapped and recorded; you set logging and retention	Full Every flow on your own network; you set logging and retention
Verdict	Use for public content only	Recommended for the document assistant	Not needed now; revisit if a contract requires on-site processing

Key, for Example Trading:

Favourable

Mixed

Unfavourable

Also considered: no new AI

Two of the seven ideas staff raised need no AI at all. Order-status emails need a template in the warehouse system, and duplicate customer records need a merge rule in the CRM. Both are on the route as quick fixes.

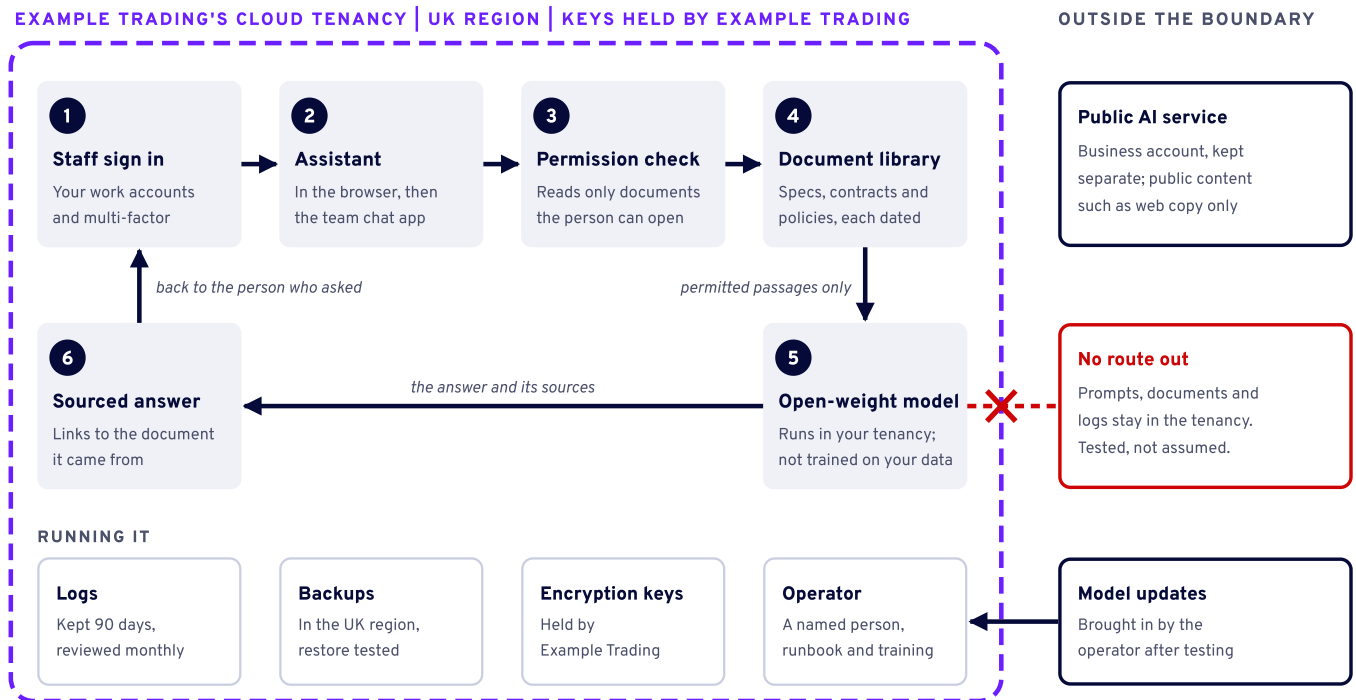
Why not on-premises?

It gives the most control, and it brings the most to run: hardware, recovery, capacity and a person on call. Nothing in Example Trading's contracts asks for on-site processing today, so the extra work buys little. We'll revisit it at each quarterly review.

3 | RECOMMENDED ARCHITECTURE

A private assistant inside your own cloud tenancy

Everything inside the purple line belongs to Example Trading. This is how a question travels.



IN PLAIN ENGLISH

- Staff sign in with the accounts they already have. When someone leaves, their access goes with their account.
- The assistant reads only the documents the person asking could already open.
- Every answer shows the document it came from, so people can check it.
- Nothing anyone types or uploads is used to train a model, here or anywhere else.
- Your documents, the logs and the backups stay in the UK region.
- You decide what is logged and how long it is kept. Every data flow is mapped and recorded, so you can show where your information goes.

HOW WE'LL PROVE IT IN THE PILOT

TEST	WHAT A PASS LOOKS LIKE
Data flows	A full day of pilot use, and nothing leaves the tenancy
Permissions	A warehouse login asking about a supplier contract is refused
Quality	40 real staff questions, checked by the people who know the answers
Speed	12 people asking at once, within the agreed response time
Restore	The service rebuilt from backup, in the UK region
Retention	Logs deleted on the schedule you set, and the deletion confirmed

CHOICES WE'LL SETTLE IN THE PILOT, ON EVIDENCE

Which model

Two or three open-weight models, tested on the same 40 real questions.

How big

Sized from real pilot use; grown only when a quarterly review says so.

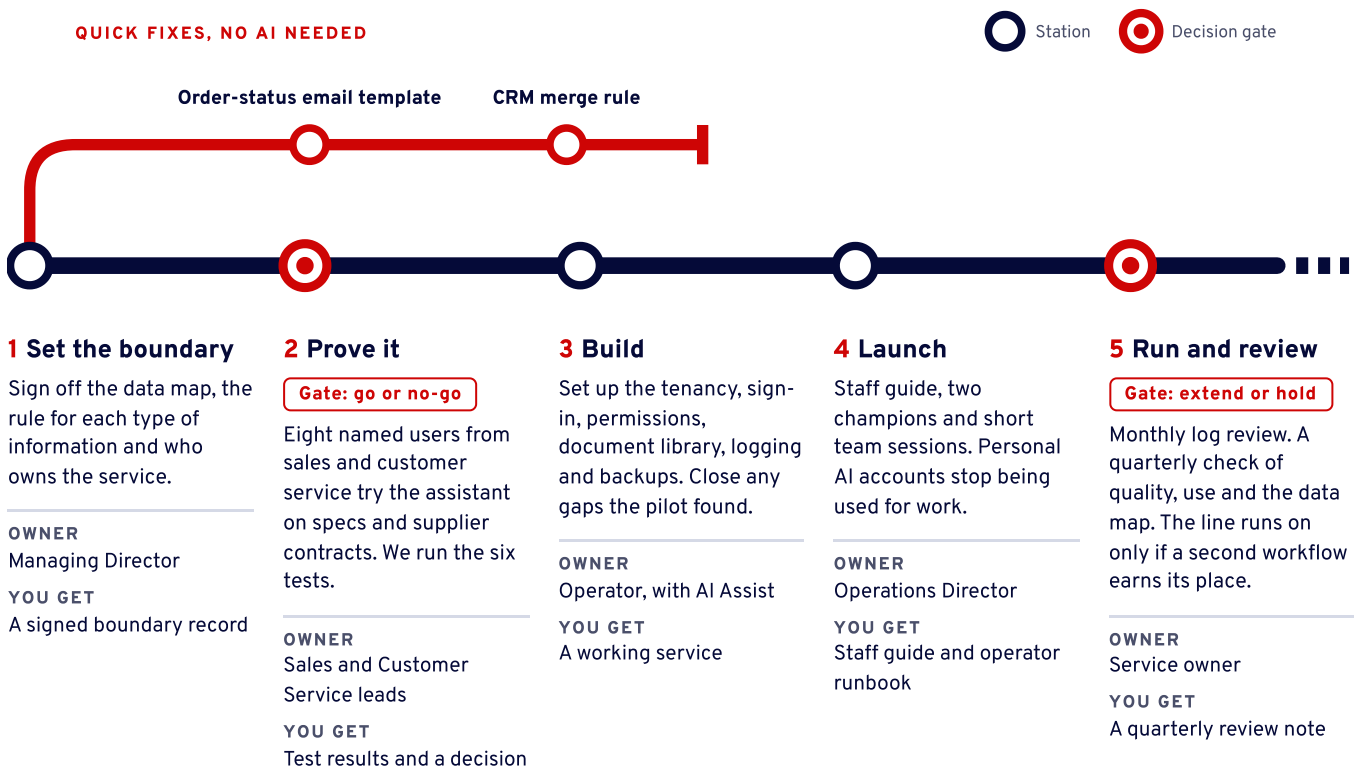
Where staff use it

The browser first; the team chat app once the pilot shows people want it.

4 | ROUTE

Five stations from today to a service you run yourselves

Each station ends with something you can see and check. The red stations are decision gates: nothing moves on until you say so. The quick fixes run alongside, because they need no AI at all.



WHAT THE STAFF GUIDE WILL SAY

RULE	EXAMPLE
Use the private assistant for	Product questions, supplier contract terms, policy look-ups
Check with your manager first	Anything you will send to a customer word for word
Keep out of every AI tool	Staff records, bank details, anything marked confidential by a customer
Public AI service, business account	Web copy and brochure drafts only

RISKS WE'RE WATCHING

RISK	WHAT WE DO ABOUT IT
It feels slower than the public tools people use at home	Speed tested in the pilot and fixed before launch; results shared with staff
Old documents give old answers	Only approved collections go in, each with an owner and a review date
Nobody owns it after launch	Owner and operator named at station 1; runbook and training before launch

Not on this route

Buying hardware, retraining a model on your documents, and anything that makes decisions about people. Each would need its own case, its own tests and your explicit go-ahead.



ABOUT AI ASSIST

AI that works for people

AI Assist is the ethical-AI consultancy in Cloud Assist Group. We help organisations use AI with clarity, ethics and practical sense. Sometimes the answer is AI. Sometimes it's better process, or better use of the tools you already have. Our job is to tell you which, honestly.

Human-centric

Technology serves people. If it doesn't make someone's work better or clearer, we don't recommend it.

Transparent

No black boxes and no jargon. You'll understand what we recommend and why, in plain English.

Practical

Real answers for real businesses. We design for how your team works, not for a slide.

You own your data

It stays inside a boundary you control, in the UK or EU, and is never used to train models.

Every data flow on the record

We map and record where your data goes, so you can show anyone who asks.

Ethics as standard

Bias checks, governance and transparency in every engagement.

Plain English, always

If your managing director can't follow the recommendation, we haven't done our job.

WHAT WE DO

AI Readiness Assessment

Ethical AI Strategy

HR Transformation Advisory

Compliance and Risk Management

Custom AI Solutions

Schools AI Readiness

Sovereign AI for Small Businesses

Sovereign AI for Medium Enterprises

About this sample. It shows the format and depth of the report we produce in a Sovereign AI for Small Businesses engagement, for organisations with under 500 employees. Organisations with 501 to 5,000 employees have their own offer, Sovereign AI for Medium Enterprises. Example Trading Ltd is fictional; its people, systems, figures and findings are illustrative. Your report would reflect your own data, systems and decisions.

Talk to us about sovereign AI

Thirty minutes on where your information goes today and what control you actually need. If a simpler answer will do, we'll say so.

ai-assist.cloud

AI Assist is part of **Cloud Assist Group**: Cloud Assist, AI Assist, WD Assist, DF Assist and NOW Assist.