

SOVEREIGN AI OPTIONS REPORT | MEDIUM ENTERPRISES, 501 TO 5,000 EMPLOYEES

Sovereign AI options for Example Engineering Ltd

Where your information goes today, three ways to run AI you control across your sites, the set-up we recommend and the waves to roll it out.

PREPARED FOR	PREPARED BY	DATE	STATUS
Example Engineering Ltd, Sheffield (fictional)	AI Assist	October 2026	Sample, version 1.0

Summary

THE QUESTION

Can Example Engineering give its 1,900 staff, across five sites, useful AI without sending customer drawings, bids and staff information somewhere it can't see or control?

OUR RECOMMENDATION

Yes. Run a private AI platform in Example Engineering's existing cloud tenancy, in a UK region, on an open-weight model, with sign-in through your identity provider. Prove it with 40 named users, then roll it out in three waves. Keep one enterprise public AI service for public content only, and retire unapproved AI tools as each wave lands.

38% of respondents

use AI tools the company hasn't approved, at all five sites. Some paste in customer drawings.

14 AI services

receive company data, found with your IT team in sign-in and network logs. Only one runs on terms anyone has reviewed.

2 customer contracts

require UK processing of their drawings; none requires on-site processing. A UK region in your own tenancy meets both.

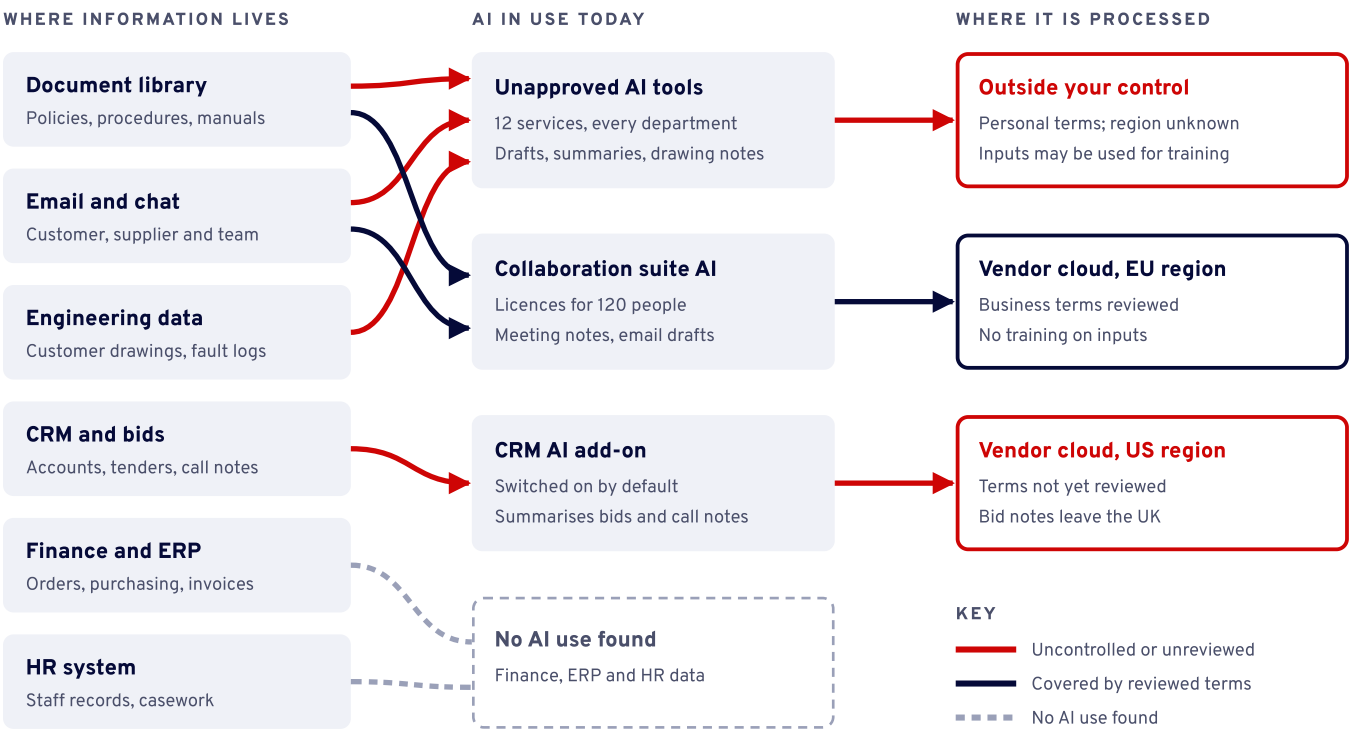
DECISIONS WE NEED FROM YOU

- 1 Approve the data boundary and the rule for each type of information**
AI governance group, before station 1 ends
- 2 Name a service owner, the platform team and department champions**
IT Director, before station 1 ends
- 3 Confirm the three waves and the 40 pilot users**
AI governance group, before station 2
- 4 Approve the AI use policy and the date unapproved tools are blocked**
Executive team, before station 4

1 | CURRENT STATE

Where your information lives, and where AI touches it

We interviewed 22 people in six departments across five sites, surveyed staff (1,140 of 1,900 replied) and, with your IT and security team, reviewed sign-in logs and the AI settings in nine systems. The map shows every route we found from company information to an AI service.



INFORMATION	LIVES IN	SENSITIVITY	AI USE TODAY	BOUNDARY RULE
Customer drawings and specifications	Engineering data	Confidential; two contracts UK-only	Unapproved tools	Must stay inside
Bids, tenders and call notes	CRM	Commercially sensitive	CRM add-on, US region	Must stay inside
Email, chat and meeting notes	Email and chat	Confidential	Suite AI, unapproved tools	Must stay inside
Policies, procedures and manuals	Document library	Internal	Suite AI, unapproved tools	Inside by choice
Staff records and HR casework	HR system	Personal, health data	None	Out of scope for now
Website copy and job adverts	Website	Public	Unapproved tools	Public service is fine

Unapproved use is everywhere

Over a third of respondents use AI tools nobody approved. Blocking them without an approved alternative would push the use out of sight.

Settings nobody chose

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

Value sits in three collections

Most of the help staff asked for draws on policies, engineering manuals and fault logs, and past bids. Those set the three waves.

2 | OPTIONS APPRAISAL

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

Each option was judged on the first two waves: answering staff questions from policies, procedures and engineering manuals, for up to 150 people at once, with answers that show their sources.

	OPTION A	OPTION B RECOMMENDED	OPTION C
	Public AI service on an enterprise account	Private AI in your existing cloud tenancy	AI on servers in your own data room
Where it runs	The vendor's cloud, in a region set by the vendor's plan	Your existing tenancy, in a UK region you choose	Servers in the head-office data room in Sheffield
Control over your data	Partial Settings and terms belong to the vendor	High Your tenancy, your keys, your identity provider	Highest Nothing needs to leave your network
Training on your data	Off, if set up right Enterprise 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 use policy	Medium Builds on your tenancy, sign-in and security tools	High Specialist hardware, power, cooling and space
Effort to run	Low The vendor runs it	Medium Your platform team, a runbook and monthly updates	High Hardware, patching, 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 data room; recovery depends on your own team
Showing where data goes	Limited Vendor audit logs, in the vendor's format and retention	Full Every flow recorded; logs feed your security monitoring	Full Every flow recorded; logs feed your security monitoring
Verdict	Use for public content only	Recommended for all three waves	Not needed now; revisit if a customer requires on-site processing

Key, for Example Engineering:

Favourable

Mixed

Unfavourable

Also considered: no new AI

Five of the 23 ideas departments raised need no AI at all. Holiday requests need one form in the HR system, and purchase approvals need a rule in the ERP. All five go to the IT team's normal backlog.

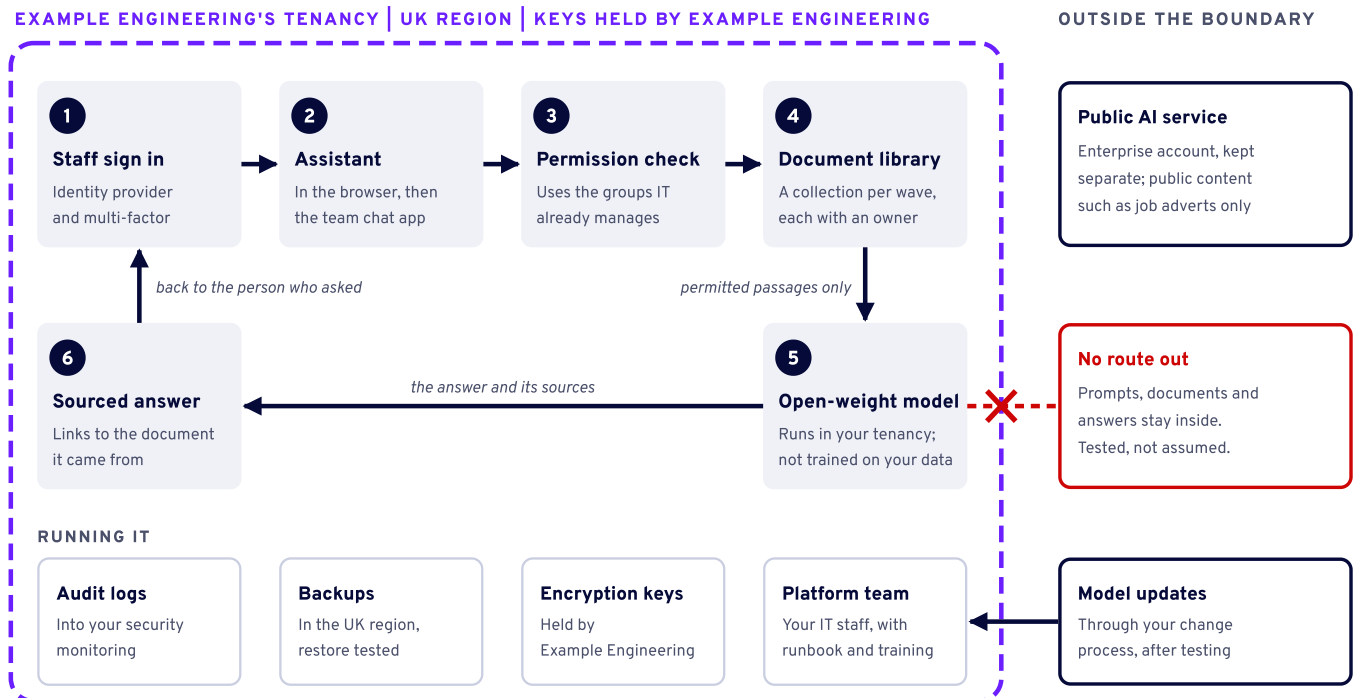
Why not on-premises?

It gives the most control, and it brings the most to run: specialist hardware, recovery, capacity and a person on call. A UK region in your own tenancy meets both UK-only contracts, so the extra work buys little. The governance group will revisit it at each quarterly review.

3 | RECOMMENDED ARCHITECTURE

A private AI platform inside your own cloud tenancy

Everything inside the purple line belongs to Example Engineering. This is how a question travels, and what your IT and security team see.



IN PLAIN ENGLISH

- Staff sign in through your identity provider. When someone changes role, their access changes with it.
- 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, logs and backups stay in the UK region. Audit logs feed your security monitoring.
- You decide what is logged and how long it is kept. Every data flow is mapped and recorded for your data protection lead.

HOW WE'LL PROVE IT IN THE PILOT

TEST	WHAT A PASS LOOKS LIKE
Data flows	A full day of pilot use at three sites, and nothing leaves the tenancy
Permissions	A shop-floor login asking for a customer's tender is refused
Quality	120 real staff questions, checked by the people who know the answers
Speed	150 people asking at once, within the agreed response time
Audit trail	Every pilot question traceable in your security monitoring
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 120 real questions.

How big

Sized from pilot use at three sites; grown wave by wave, on evidence.

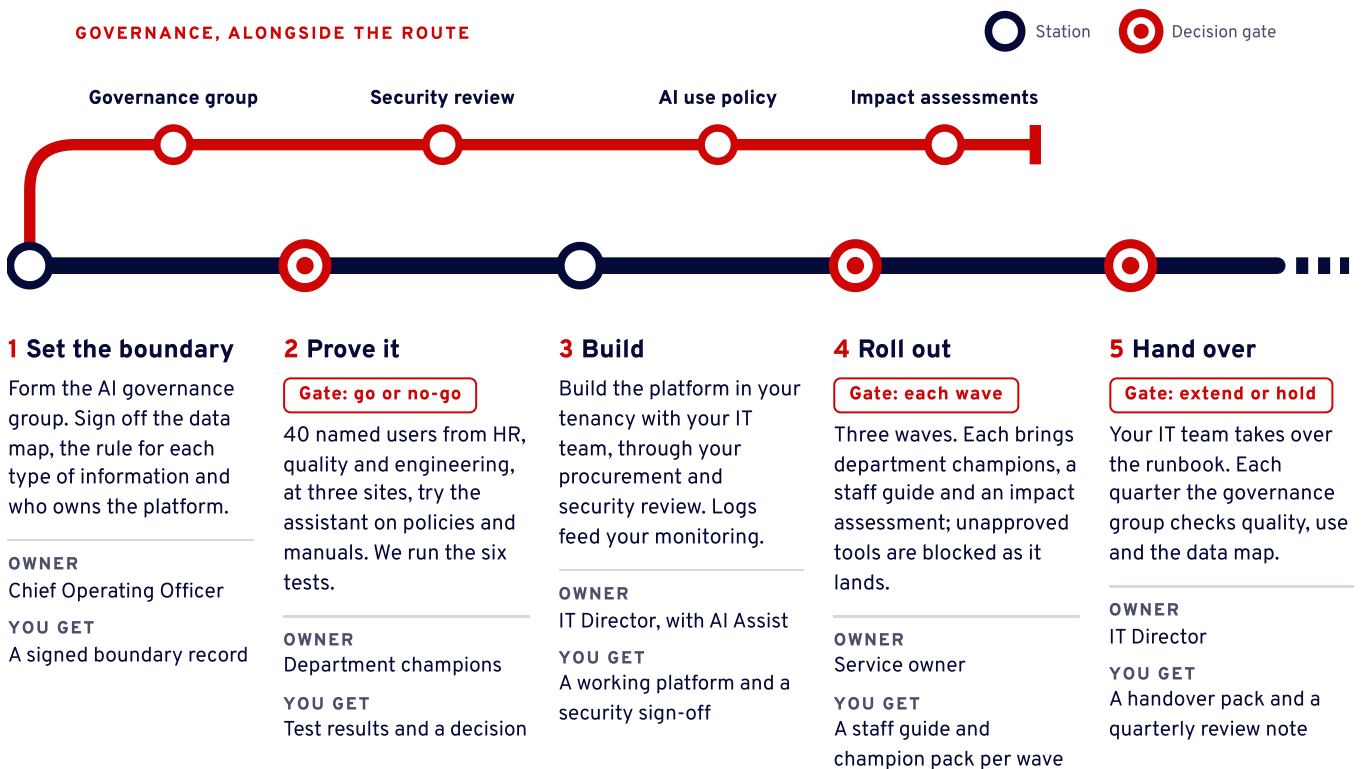
Where staff use it

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

4 | ROUTE

Five stations from today to a platform your IT team runs

Each station ends with something you can see and check. The red stations are decision gates: nothing moves on until your governance group says so. Governance runs alongside, so each wave arrives with its policy, its impact assessment and its security sign-off.



THE THREE WAVES

WAVE	WHO, AND WHAT IT DRAWS ON
1 Policies and procedures	Every department: HR, health and safety, quality and IT policies
2 Engineering knowledge	Plant engineers at four sites: maintenance manuals and fault logs
3 Bids and contracts	The commercial team: past bids, tenders and contract terms

RISKS WE'RE WATCHING

RISK	WHAT WE DO ABOUT IT
Unapproved tools stay in use	The approved assistant arrives first; each wave sets the date the old tools are blocked
Old documents give old answers	Only approved collections go in, each with an owner and a review date
Departments queue for IT	A champion in each department and one request route through the governance group

Not on this route

Buying hardware, retraining a model on your documents, HR casework, and anything that makes decisions about people. Each would need its own case, its own impact assessment and your governance group's 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 executive team 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 Medium Enterprises engagement, for organisations with 501 to 5,000 employees. Organisations with under 500 employees have their own offer, Sovereign AI for Small Businesses. Example Engineering 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.