# Data, build and operations

*Which data it is built on and how it is kept alive in production.*

> *"An AI system can fail without going down. It is built on data with an owner and permission to use, monitored in production for quality, drift and cost, and there is always a tested way to roll back."*

WHAT IT IS

## Data with an owner and permission to use

Every dataset or knowledge source used by AI has a business owner, quality measured for its use and a legal basis for that purpose. Availability and quality are checked with real data during feasibility, before design: a data problem discovered at delivery costs the whole build.

**Implication:** How many of your use cases passed the feasibility gate with real data, rather than with descriptions of what the data should contain?

**Risk:** Without an owner or a legal basis, the use case stops late or cannot be defended before an auditor or a regulator.

WHAT IT PROPOSES

## Operate, change and roll back

Each system in production has a reachable AI Operations Owner, an operations manual and alerts with an owner. Each change is classified before it is applied: minor, significant or substantial; a substantial change returns to a decision gate. The rollback plan is tested and agents have a kill switch.

**Implication:** Who is accountable today for each AI system in production, and when was the ability to roll back last tested?

**Risk:** An unvalidated change of model or instructions alters behaviour without anyone having decided it.

HOW IT IS CHECKED

## Monitoring and continuity review

Monitoring looks at more than availability: input data, drift, quality of responses, agent actions, security, cost and value. The continuity review, quarterly at Enterprise and half-yearly at Lite, decides to continue, continue with conditions or bring forward the decision to scale or retire.

**Implication:** Does each system in production have its continuity review up to date, with the value, cost and incidents of the period?

**Risk:** Without a periodic review, a system that no longer adds value keeps consuming budget and accumulating risk.

## FOUR QUESTIONS FOR THE BOARD

1. **Do we know what data each system uses and whether we can use it?**
   Each dataset catalogued with an owner, measured quality, legal basis and retention, and linked to its use cases.
2. **What happens if the model provider fails?**
   For each critical case, a planned degraded mode (fallback model, another provider or non-AI alternative) and a tested recovery time.
3. **Are there substantial changes applied without returning to a gate?**
   None: every change is recorded with its class and substantial ones return to the corresponding decision gate.
4. **What do we do if the consumption budget runs out?**
   A defined degradation cascade: optimise, validated fallback model, reduced scope or non-AI alternative, without touching the controls.

## WHAT FAILS IF IT IS NOT GOVERNED

| WHAT FAILS | LEVEL | WHAT TO DO |
|---|---|---|
| Data used for AI with no owner or legal basis | HIGH | Catalogue each dataset with its owner |
| Feasibility assessed with descriptions, not real data | HIGH | Assess the data with a real sample before design |
| Systems in production with no AI Operations Owner | HIGH | Appoint an AI Operations Owner for each system |
| Changes of model or instructions not classified | MEDIUM | Classify each change before applying it |
| A rollback plan that has never been tested | MEDIUM | Test the rollback plan of each system |
| Consumption cost with no limit or planned degradation | MEDIUM | Define the cost-driven degradation cascade |
| Out-of-date knowledge sources in assistants | LOW | Set a review date and owner for each source |

## FURTHER READING

**Data and knowledge**
Document 51 · ownership, quality and legal basis

**Building solutions with AI**
Document 53 · requirements for AI-generated work

**AI operations manual**
Document 52 · monitoring, changes and rollback

**General Data Protection Regulation (EU) 2016/679**
European Parliament and Council of the EU · 27-04-2016



Fernando García Varela · CC BY 4.0 · Version 0.x, under review

*Generic help offered free of charge, with no legal review for any specific case: each organisation adapts it, identifies the regulation that applies to it and is responsible for its own compliance. It is neither advice nor certification. To the maximum extent permitted by law, the author accepts no liability for the effects of its application.*