AI Platforms as a Secure Business Foundation

Erik Jan de Vries

2026-03-03 VSAE Actuarial Congress

AI Platforms as a Secure Business Foundation

2026-03-03 VSAE Actuarial Congress

- Introduction
- Scenario: Mortgage lending
- Framework: Secure business foundation
- Role of actuaries
- Competition
- What to do next

Introduction

Erik Jan de Vries

Award-winning AI & MLOps Consultant, freelance

Strategist

Architect

Engineer

Trainer

> 15 yrs experience

AI & MLOps platforms

Azure ML — Van Oord (Marine ingenuity)

GCP Vertex AI — Liberty Global

On-prem — Swift, vodafone, Ziggo

PhD

Mathematical Physics

Amateur Pianist

Next Best Action Marketing

Azure — Eneco, cda customer data awards

https://linkedin.com/in/erikjandevries

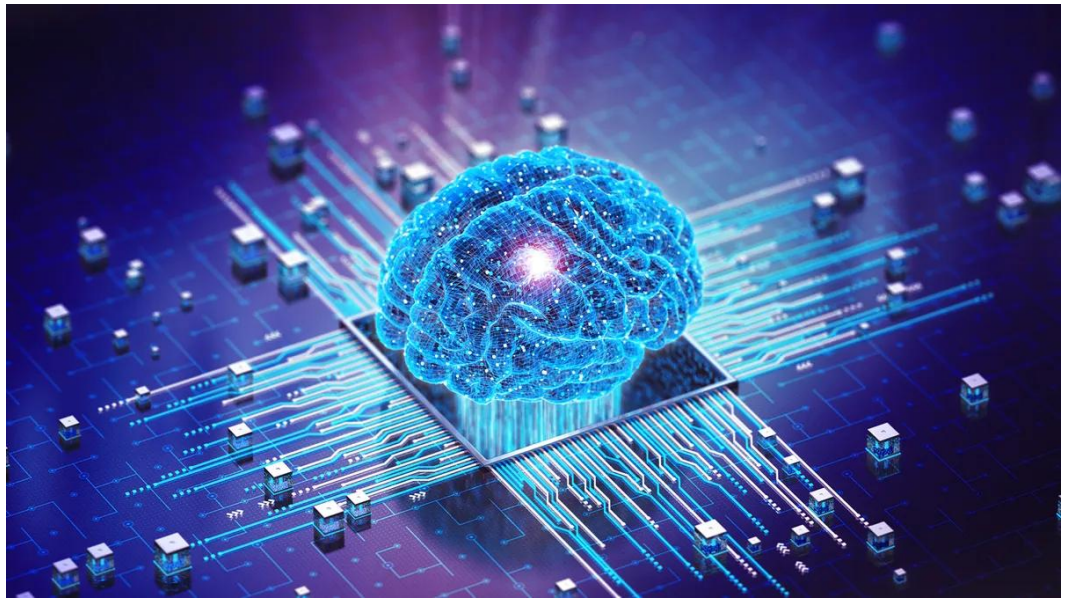
http://youtube.com/watch?v=UsnGprFRa8

My framework for successfully navigating digital transformations

Integrating Business, Organisation and Technology

	Strategic • Vision • Ambition • Strategy • Roadmap	**Tactical** • Planning • Resource allocation • Project management	**Operational** • Execution • Maintenance • Support
Business • Business model (canvas) • Use cases			
Organisation • Culture • Structure • Governance • Processes • People			
Technology • Architecture • Information & Data • Artificial Intelligence • Security			

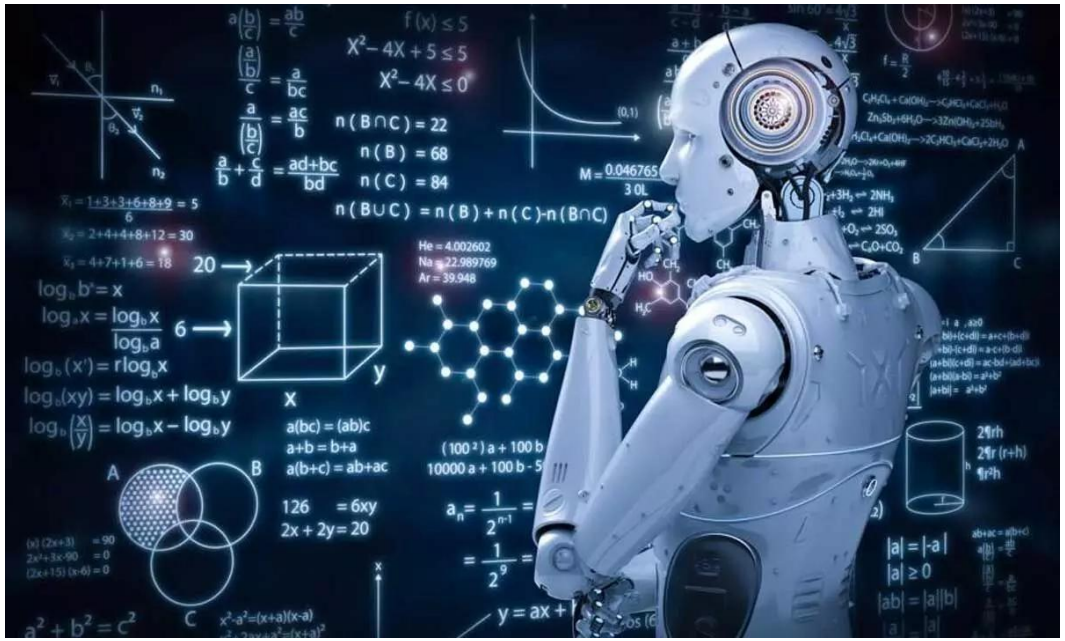
Artificial Intelligence (AI)



- Intelligence in machines
- Intelligence is the ability
  - to perceive information, and
  - to use it to drive behaviour and decisions
  - resulting in progress towards goals

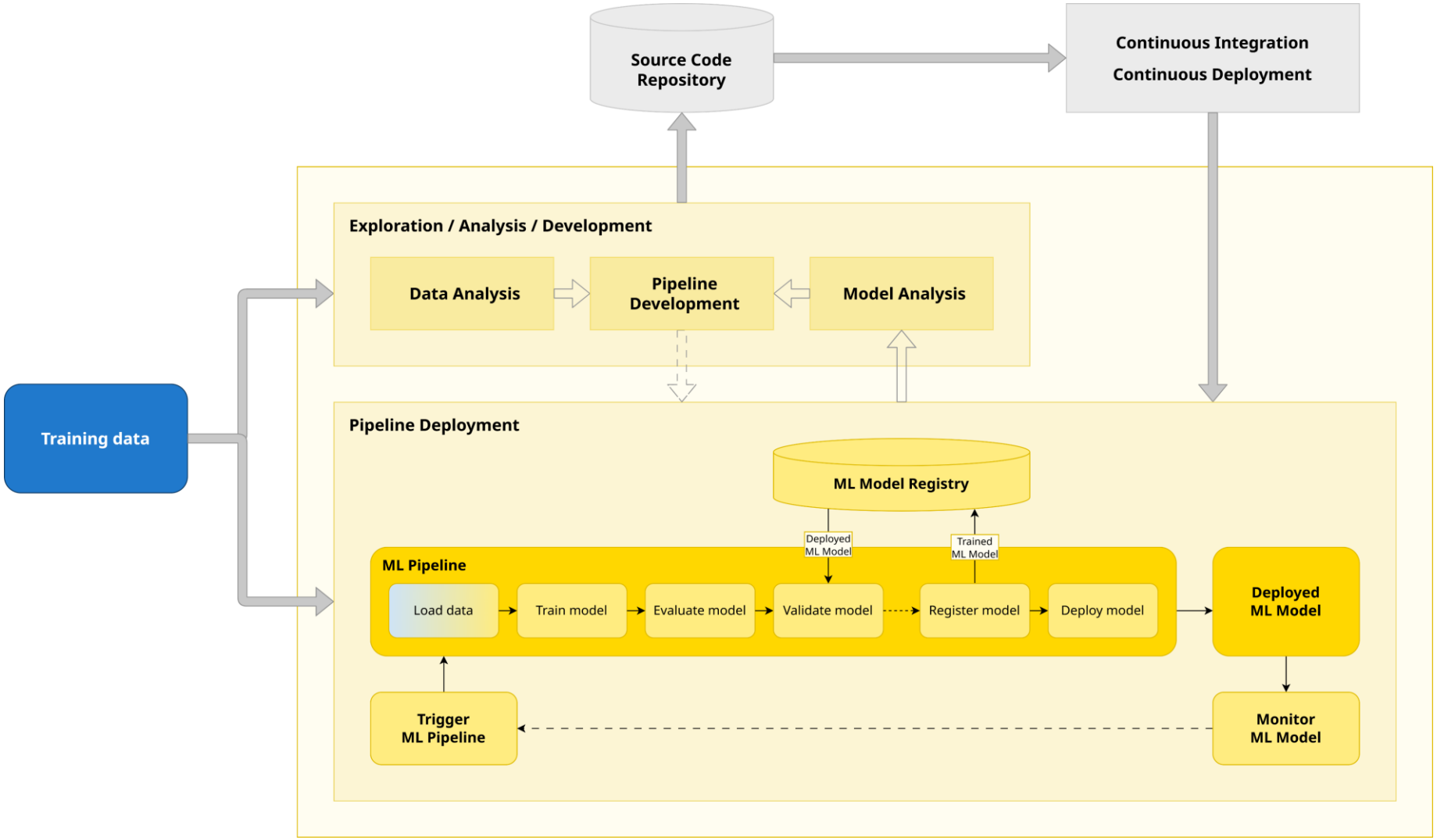
Machine Learning (ML)

- Technique for developing algorithms without coding explicit instructions
- Computers derive the algorithm by observing training data



MLOps = DevOps for ML

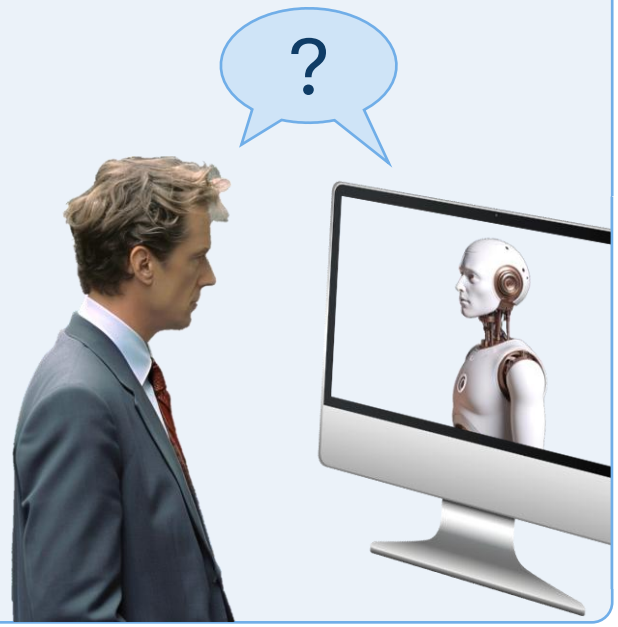
A methodology to develop and deploy ML models, through automated ML Pipelines



Generative AI

Q&A

- AI chat bots
- Challenge:
  - How do you talk to an AI?



Gen AI Systems

- AI embedded in an application
- Capable of specific actions
- For example:
  - RAG: let an AI access your knowledge (documents)

Gen AI Agents

- Versatile digital assistant
- Plans and acts independently
- For example:
  - Computer use
  - Personalised financial advisor

Scenario: Mortgage lending

YOUR AI MODELS WILL FAIL!

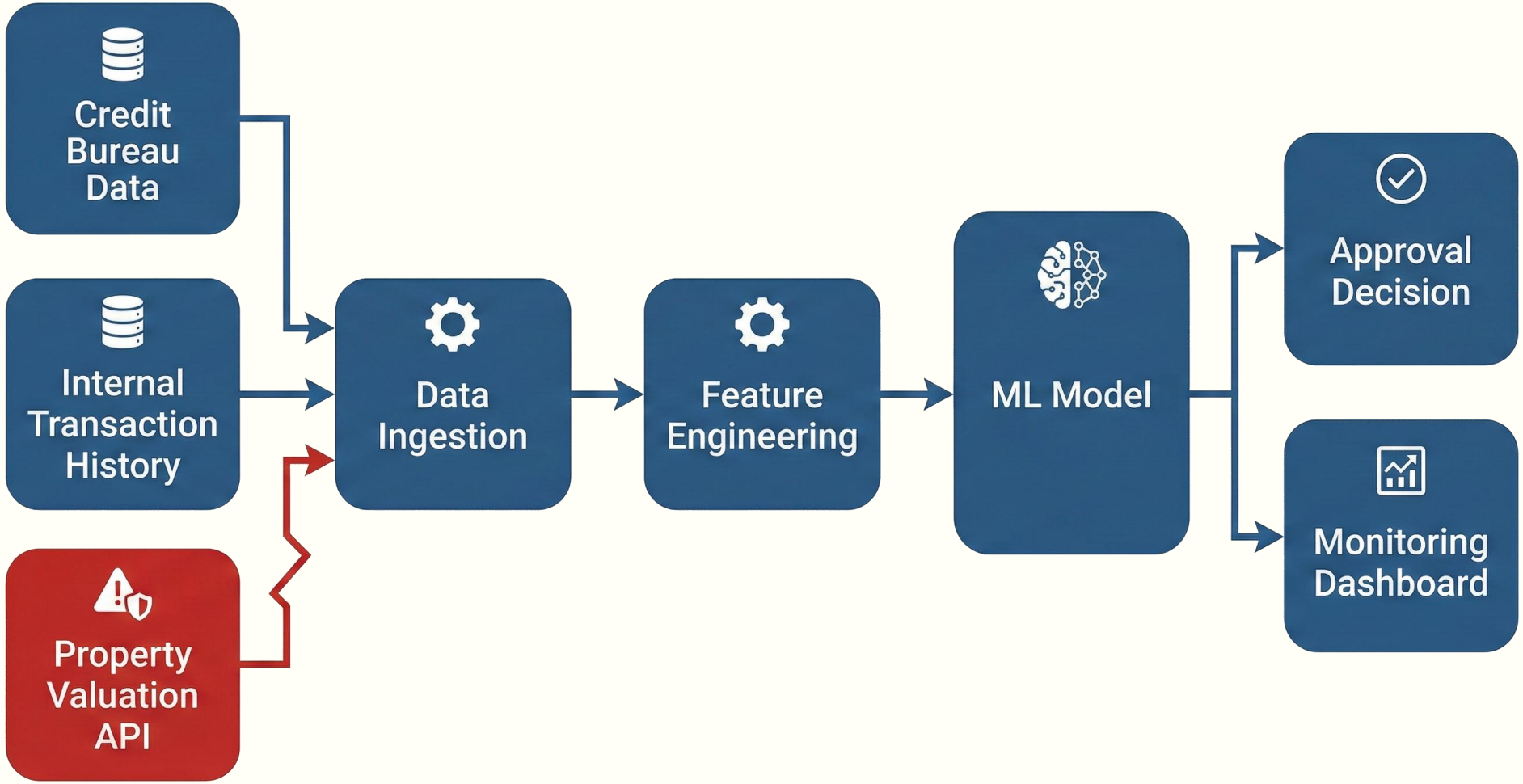
WILL YOU KNOW WHY?

WILL ANYONE BE ACCOUNTABLE?

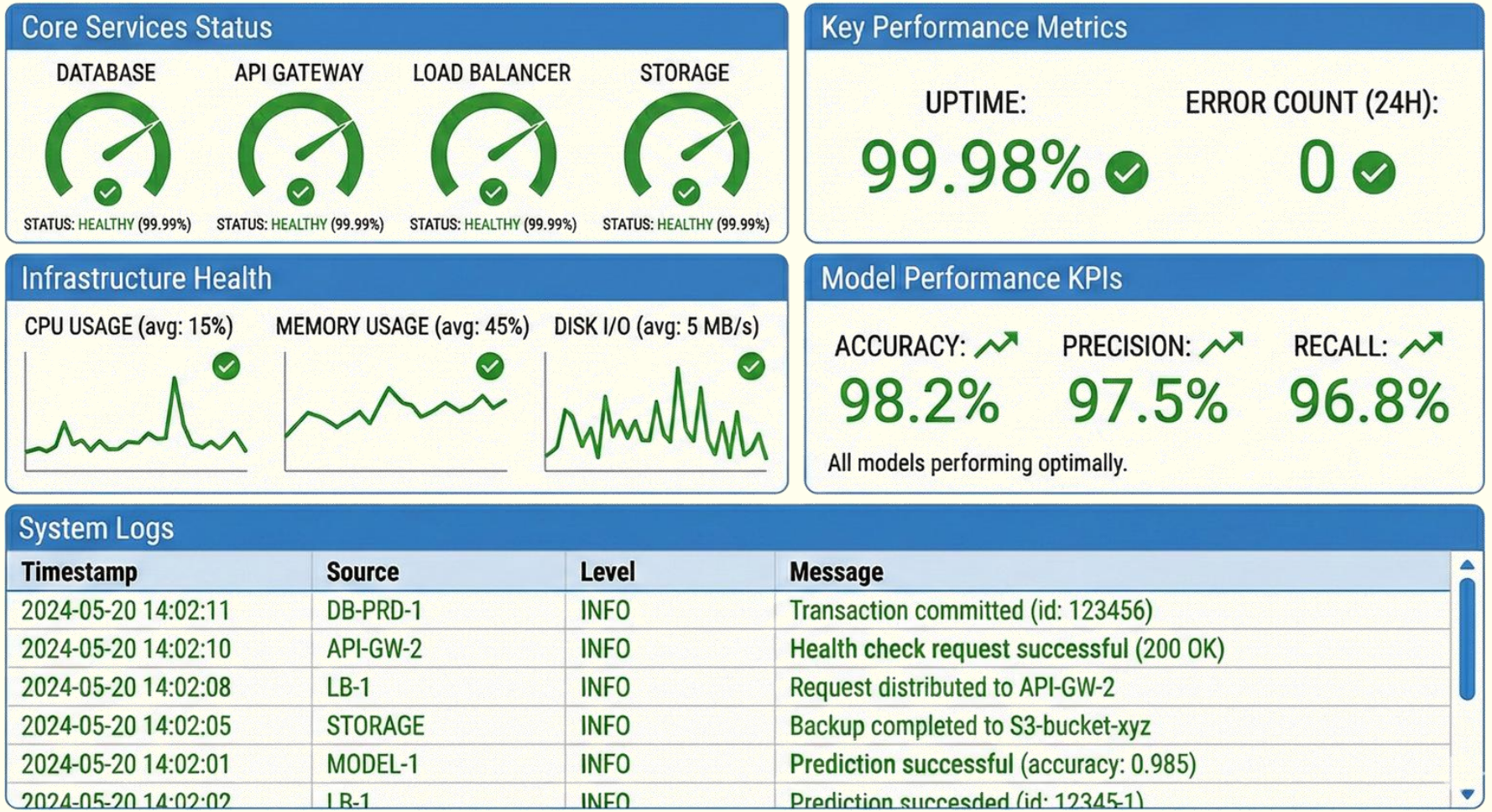
A mortgage AI: What could go wrong?

Scenario introduction

Failure Layer 1 — Supply chain poisoning



Failure Layer 2 — Monitoring blind spots



Failure Layer 3 — Fairness violation emerges

Failure Layer 4 — Accountability lacking

The Damage

Financial, reputational, regulatory

How can we prevent this from happening?

Framework: Secure business foundation

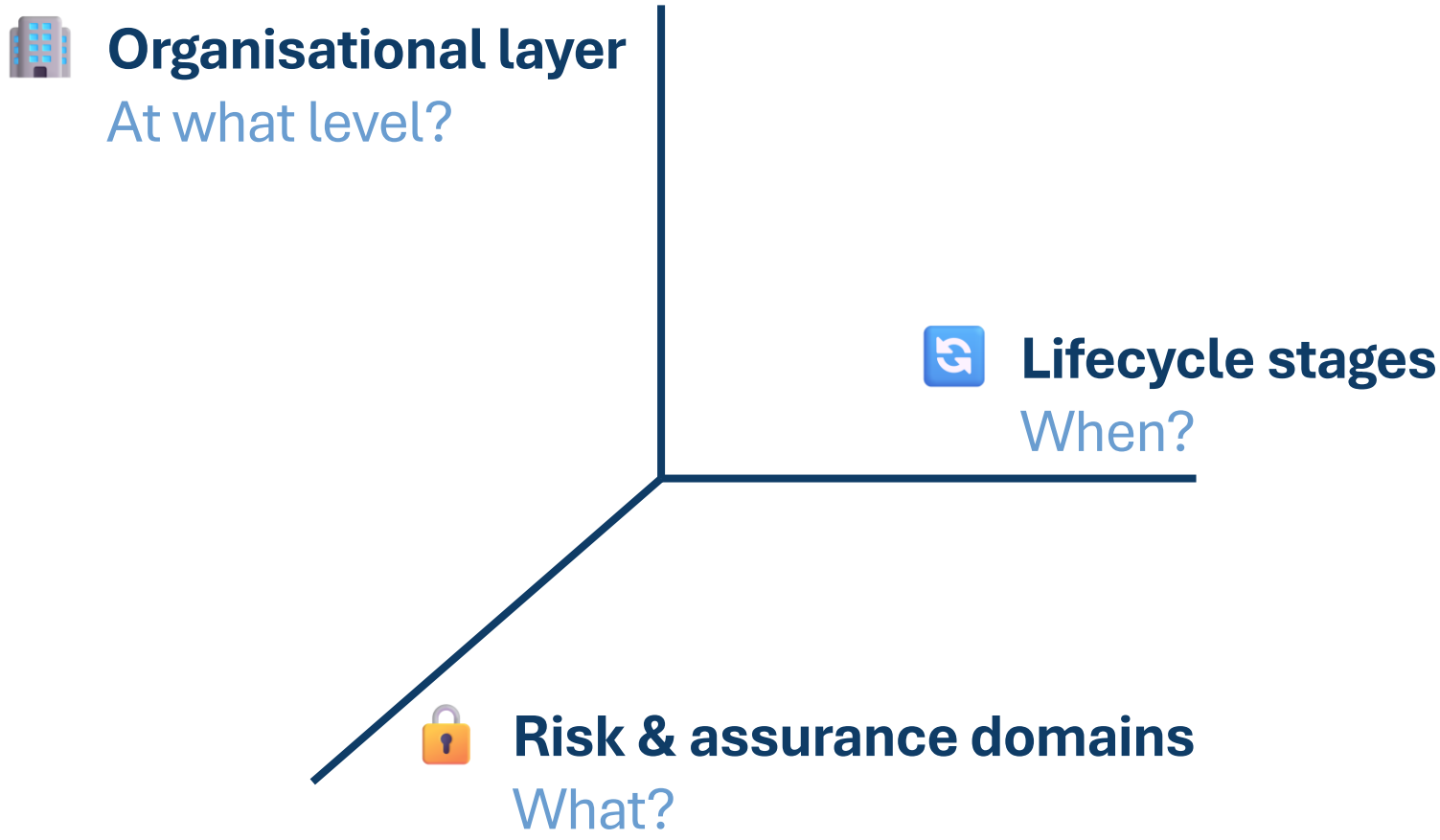
How to think about platform security

How do you know you've covered everything?

Team	Responsibility
IT Security	Infrastructure
Data Science	Model performance
Compliance	Regulatory requirements
Risk	Business impact
Legal	Discrimination law

Who asks: "Have we addressed all dimensions, at all lifecycle stages, at all organisational levels?"

Three dimensions of (AI) platform security



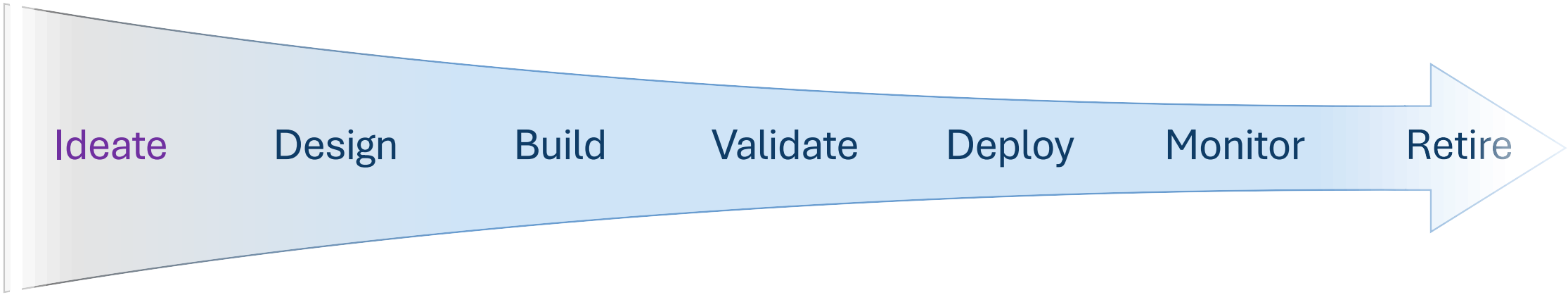
Dimension 1 — Organisational layer

Each layer has distinct responsibilities across the framework

Strategy	• Purpose, risk appetite, roadmap
Governance	• Accountability, oversight, approval
Architecture	• Design, data flows, observability
Operations	• Execution, monitoring, response

Full breakdown available on request

Dimension 2 — Lifecycle stages



Dimension 3 — Risk & assurance domains

Data	Provenance, quality, lineage, privacy, representativeness, bias
Models	Robustness, adversarial resilience, explainability, fairness, performance, drift
Infrastructure	Compute, storage, network, access control, encryption, availability, resilience
Supply chain	Third-party models, libraries, APIs, data vendors, licensing
Processes	Governance workflows, change control, documentation, compliance, audit
People	Skills, awareness, training, culture, independence, accountability
Use & impact	Human oversight, scope limits, feedback loops, decision quality, harm prevention

Working with the framework

The basis

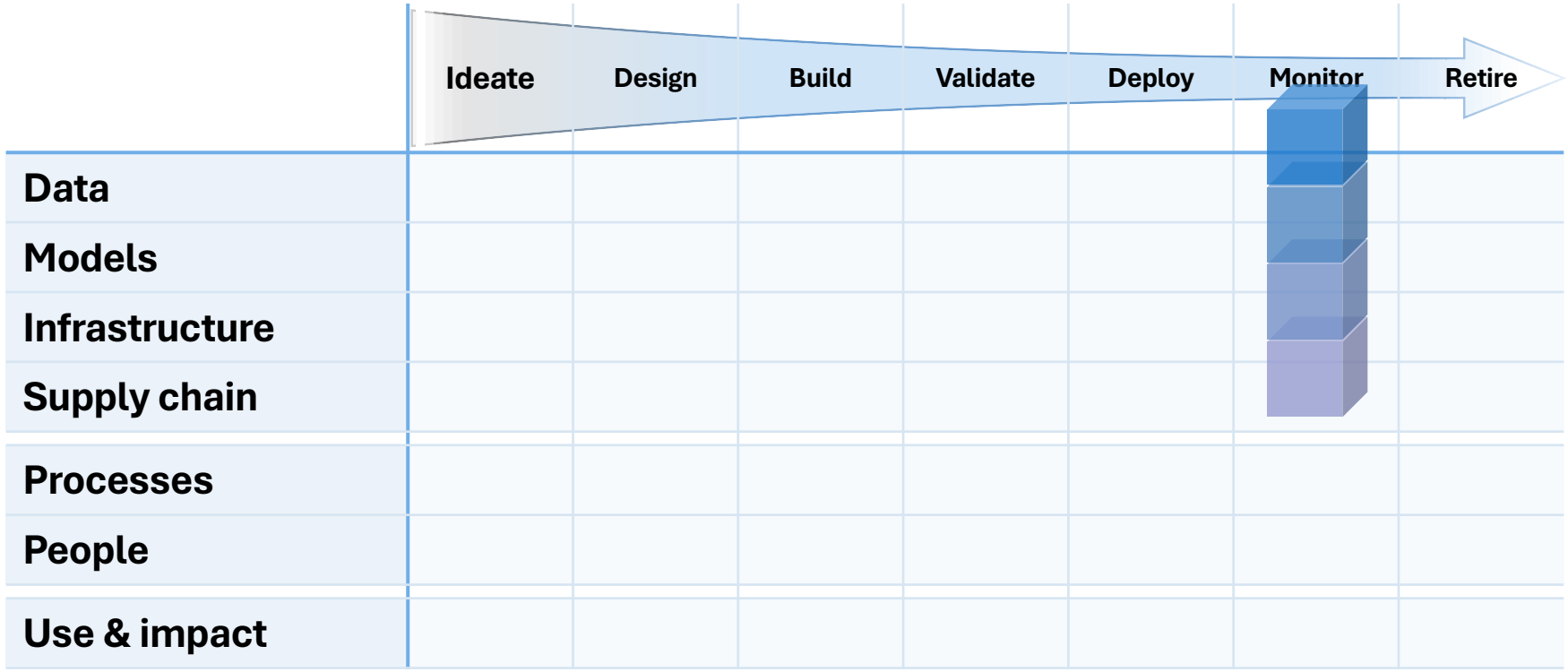
Assess every risk and assurance domain, for every stage of the lifecycle

	Ideate	Design	Build	Validate	Deploy	Monitor	Retire
Data							
Models							
Infrastructure							
Supply chain							
Processes							
People							
Use & impact							

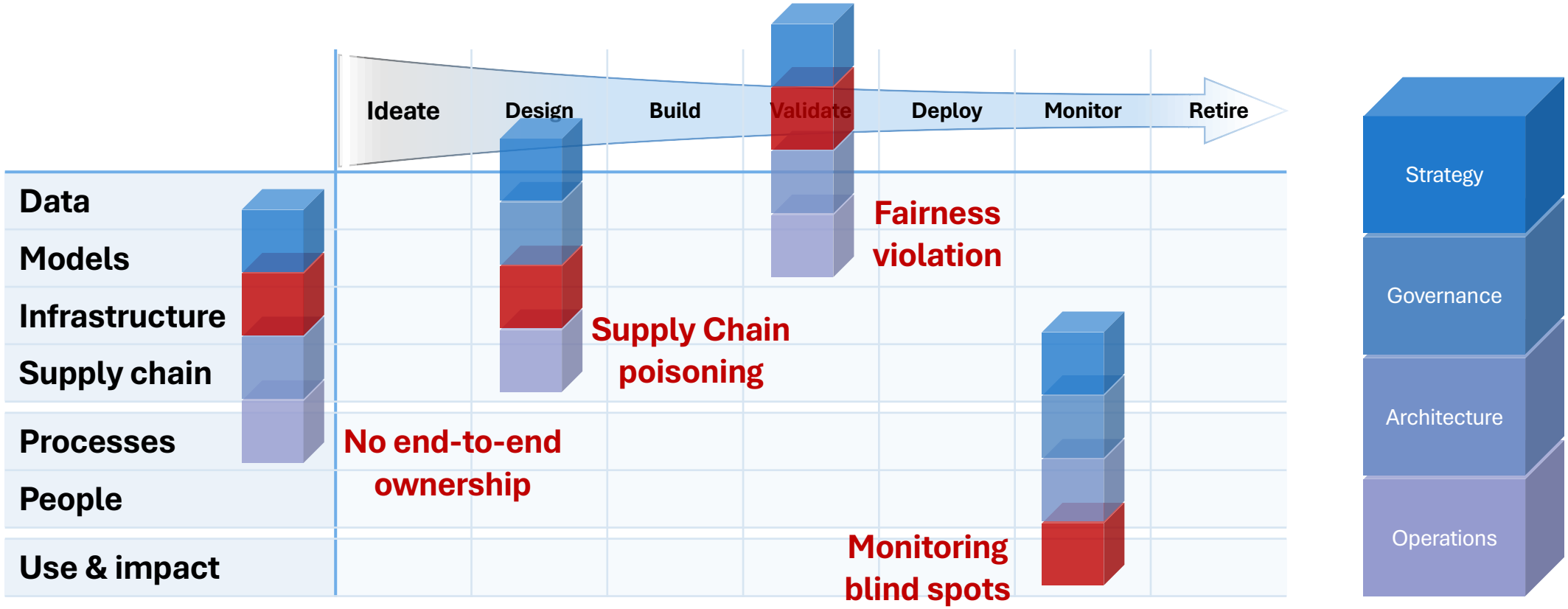
Working with the framework

Adding the organisational layer

For each cell, have we addressed this at all organisational layers?



How using the framework could have prevented the mortgage failure



Role of actuaries

Actuaries are structurally well-positioned for AI governance...

Risk Quantification & Tolerance-Setting

Analyzing probability and setting acceptable risk limits.

Independent Validation & Documented Limitations

Bias detection, accuracy checks, and clear communication of model constraints.

Process Governance & Audit Trails

Traceability of data sources, decisions, and model lifecycle management.

Stress Testing & Scenario Analysis

Evaluating model resilience under severe market shocks and diverse scenarios.

Assumption Challenge & Stakeholder Protection

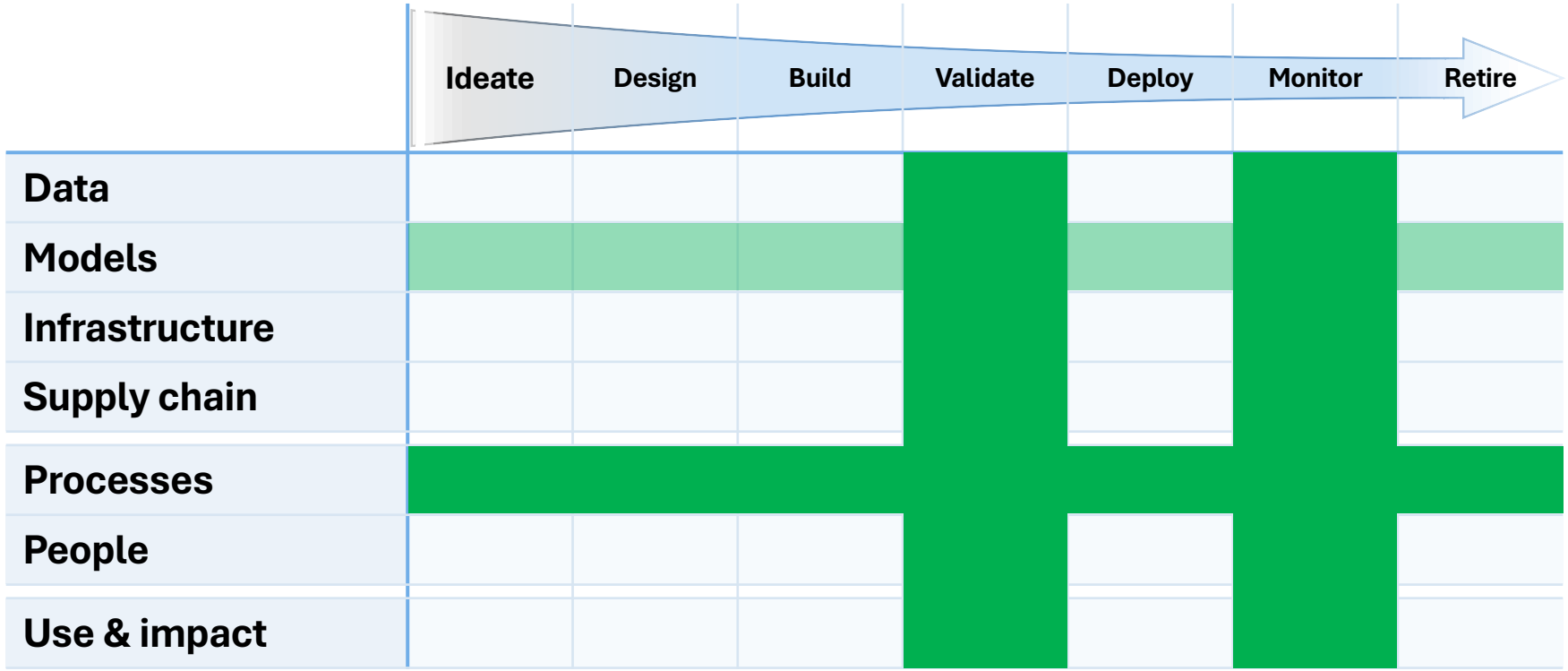
Critical review of data, model assumptions, and ensuring fair policyholder outcomes.

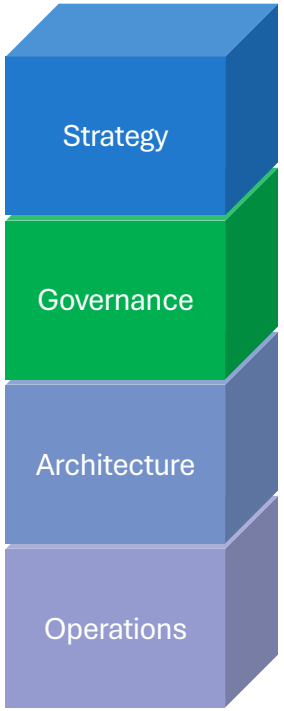
Board-Level Reporting & Escalation

Clear communication of AI risks to senior leadership and formal escalation of critical issues.

Actuaries are structurally well-positioned for AI governance…

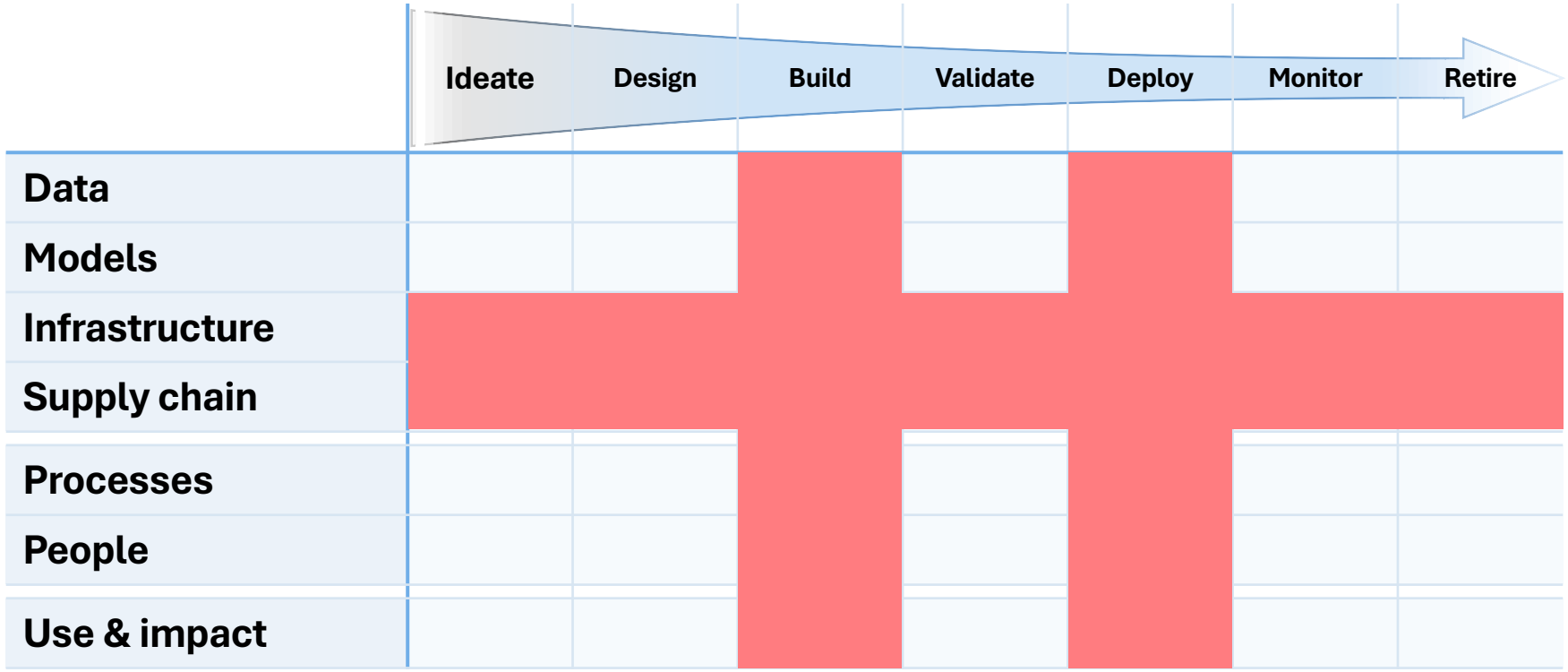
Actuarial strengths mapped to the framework

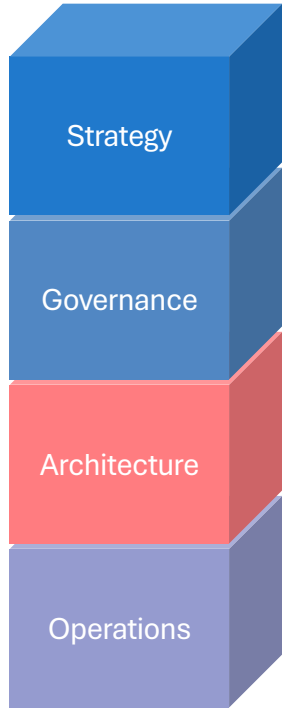




… but being well positioned ≠ entitlement

Actuarial weaknesses mapped to the framework





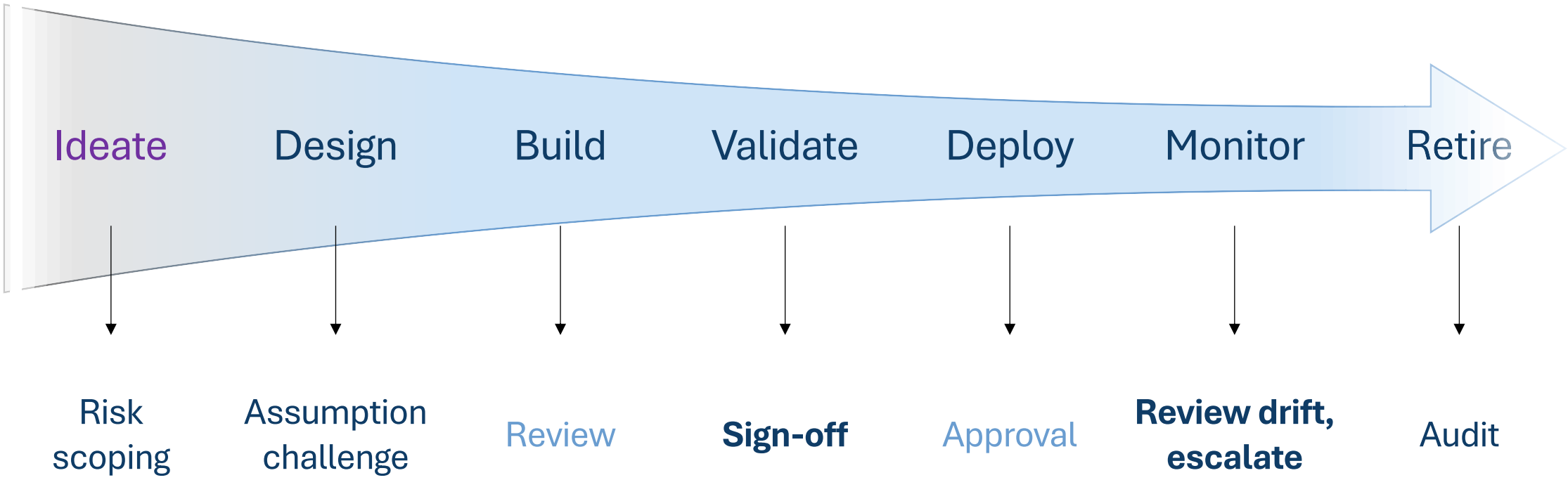
AI Governance partnerships solve the competency gap

The Actuary
(governance, risk)

The AI Engineer
(implementation, tooling)

Actuarial governance throughout the AI lifecycle

Example pattern



You need a formal governance structure, not ad hoc review

Four operating models

Embedded actuarial reviewers

(in model teams)

Cross-functional AI Risk Committee

(with actuarial seat)

Actuary-led AI Assurance

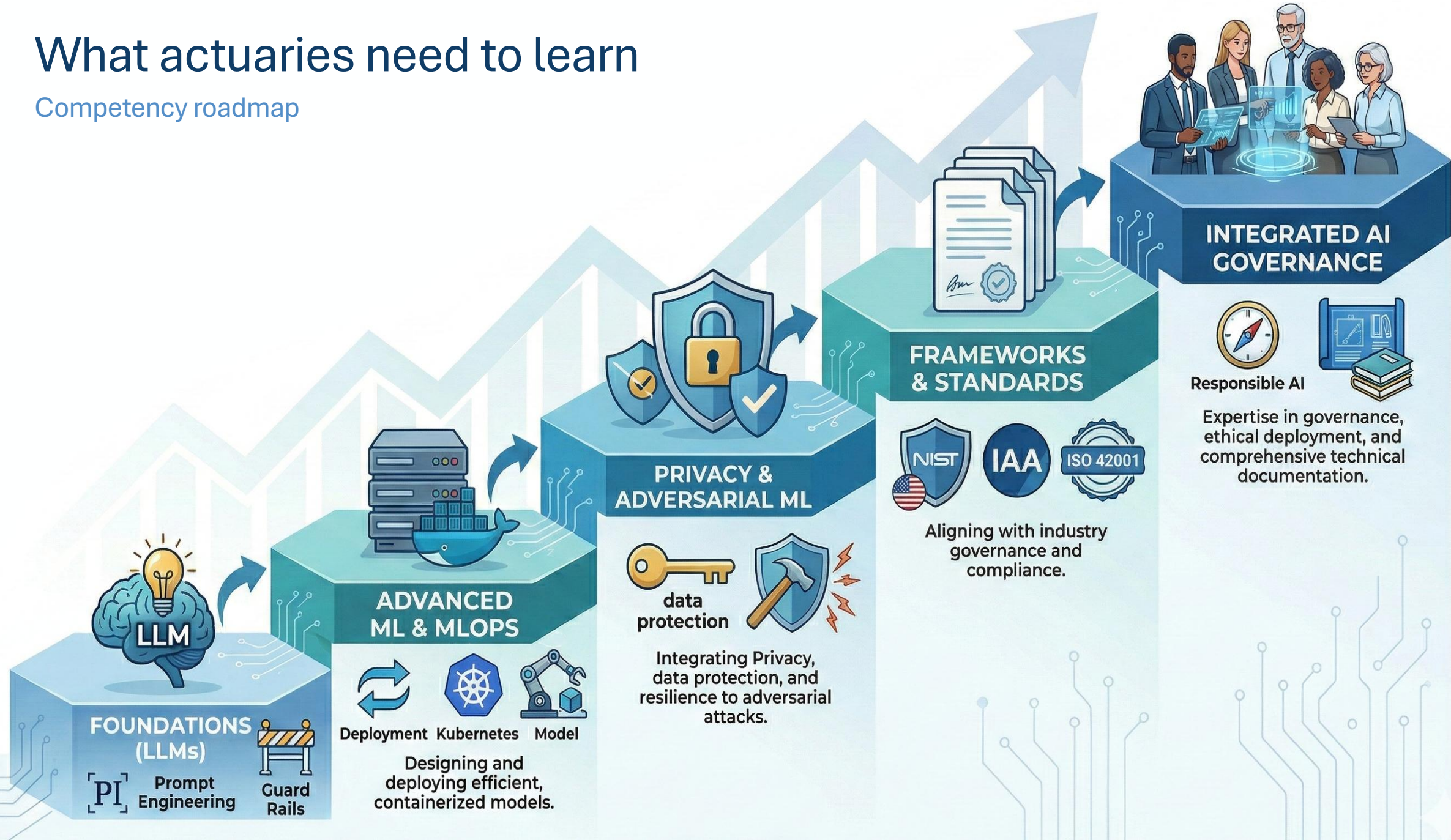
(2nd line)

External actuarial assurance

(third party)

What actuaries need to learn

Competency roadmap



What actuaries bring — and what they need

Actuaries bring:

- Governance discipline
- Independence
- Risk quantification and stress testing
- Board communication
- Professional accountability

Actuaries need:

- MLOps / GenAI understanding
- Technical fluency
- Adversarial / privacy awareness
- Supply chain security knowledge

The solution:

- Partnerships (with AI / ML and Security engineers)
- Clear role definitions
- Formal operating models
- Targeted training

Competition

AI governance is contested territory

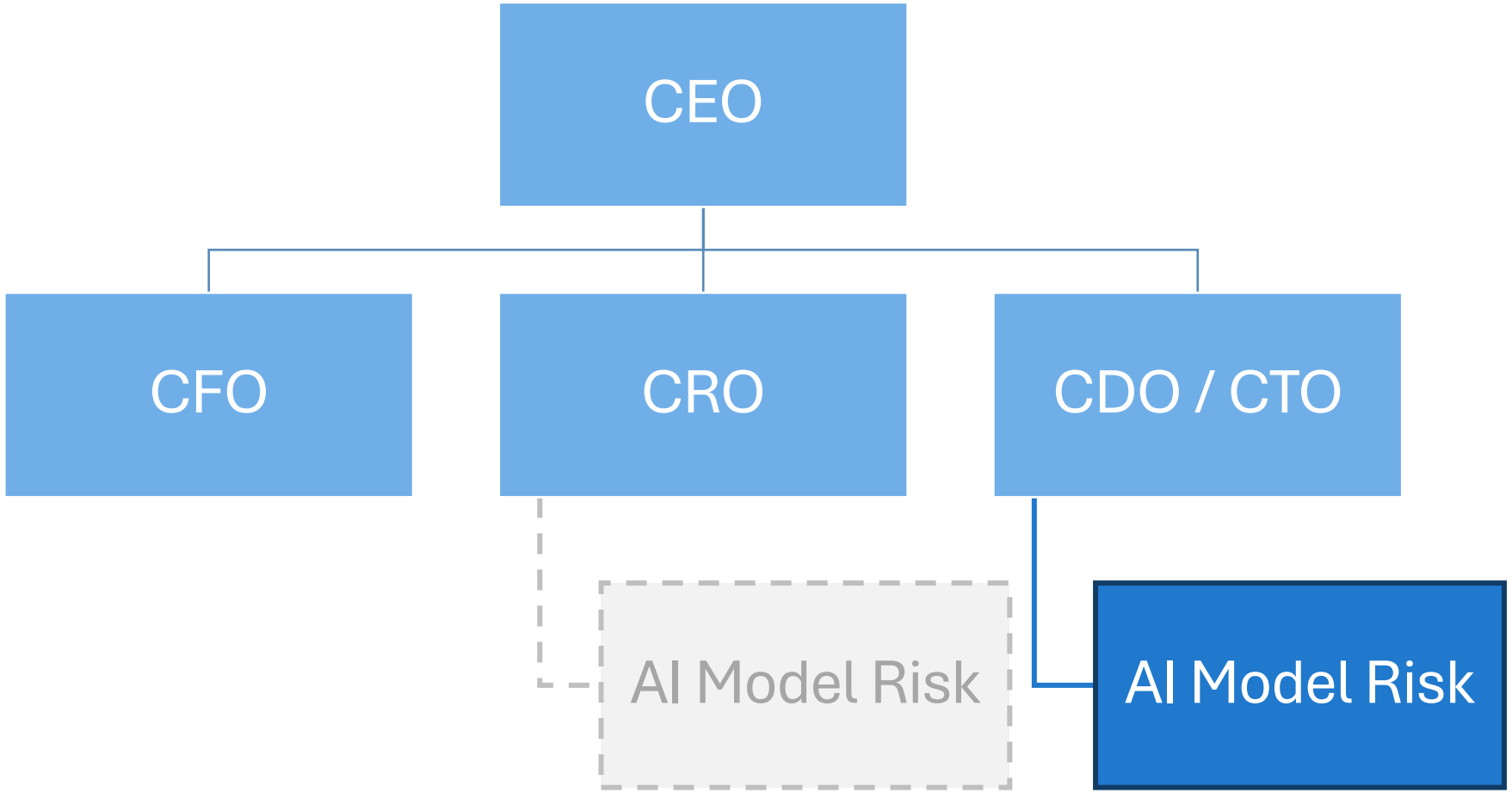
Who will own AI governance in five years?

Data scientists are reckless hackers.

Actuaries are slow and don't understand code.

Both are half-right. Who will own AI governance?

What happens if actuaries don’t act?



Do you want **independent professional oversight** or **engineering self-regulation**?

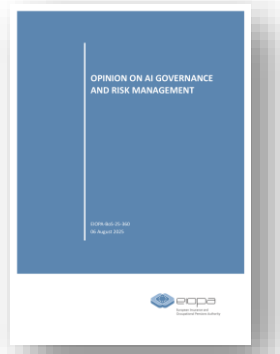
The window of opportunity is finite

AI Governance will be decided in the next 12-24 months

Regulation is not coming — it’s already here

DORA

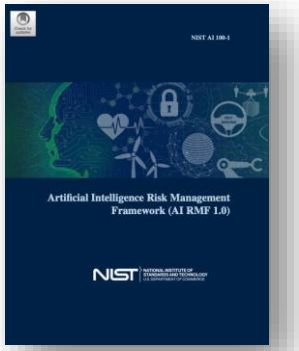
EU AI Act



EIOPA Opinion

2022-12 2023-01 2023-12 2024-07 2025-08 2026 ?

NIST AI RMF



ISO 42001

IAA AI Governance

What to do next

Action plan

Step 1 — Assess your organisation

Using the framework

Where are you? Where are the gaps?

	Ideate	Design	Build	Validate	Deploy	Monitor	Retire
Data							
Models							
Infrastructure							
Supply chain							
Processes							
People							
Use & impact							

Step 2 — Decide

Make a conscious choice

What role should actuaries play?

Lead AI governance

2nd line function

Partner as equals

joint sign-off with technical specialists

Focus elsewhere

traditional actuarial domains

Step 3 — Act

Concrete next steps

1. Start a conversation
2. Ask the five questions
3. Get training
4. Build partnerships
5. Propose a pilot

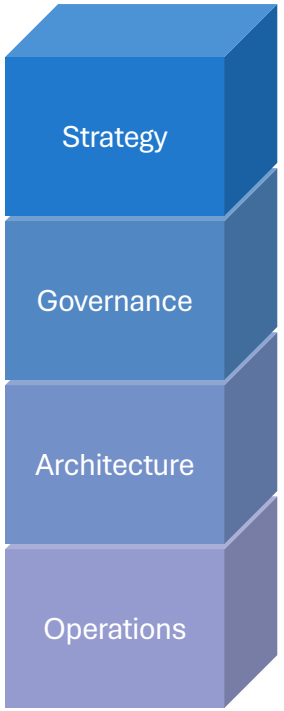
Five questions for your organisation

1. Who owns AI model risk governance?
2. What governance frameworks are we using?
3. How do we validate third-party AI dependencies?
4. Do we test fairness and drift at the subgroup level?
5. What would it take for actuaries to have a formal AI governance role?

Securing your business foundation = risk management

AI models will fail — will you be there to catch them?

	Ideate	Design	Build	Validate	Deploy	Monitor	Retire
Data							
Models							
Infrastructure							
Supply chain							
Processes							
People							
Use & impact							



Want to talk about
what this means for your organisation?

Erik Jan de Vries, AI & MLOps Consultant

https://linkedin.com/in/erikjandevries