AI GOVERNANCE IN PRACTICE

Beyond the frameworks: what actually works?

A practical discussion

Olivia Roth
Data Protection & AI Protection Officer

THE CHALLENGE

The gap between governance on paper and governance in reality

The question is not whether we have a framework. It is whether it can be useful to us and the business.

On paper

- policies
- committees
- risk matrix
- controls
- principles
- questionnaires
- approval workflows
- Inventories
- audits

In the business

AI features appear everywhere:

- in software and processes
- introduced by employees or vendors
- As a POC or major project
- planned or spontaneously activated

What works

A practical, simple process, clear ownership and the right documentation and assessment as well as continuous dialogue with the stakeholders.

Governance is an operating model — not a document collection.

THE CHALLENGE

Where does AI governance get stuck?

01	**Discovering AI use**	Shadow AI, embedded features, decentralised adoption, unawareness
02	**Getting engagement**	Business teams see governance as cause for delay
03	**Assessing consistently**	Unclear thresholds and duplicated questionnaires, committees or documentation
04	**Clarifying ownership**	Who decides? Who accepts residual risk? Who needs to be involved?
05	**Monitoring change**	Approvals become obsolete as tools and use cases evolve

OPERATING MODEL

Six capabilities that make governance operational

Build a practicable process from first idea to responsible use.

1

TRAIN

Train your teams – create awareness

2

DISCOVER

Know which AI is in use

3

BUILT

Built your frameworks & rules

4

DECIDE

Assign accountable decision-makers / committees

5

ENABLE

Embed controls into workflows

6

MONITOR

Reassess when things change

Make the default path easy; reserve deeper scrutiny for material risks.

DISCOVER

AI inventory: start small, but make it useful

The register should enable decisions — not become an administrative burden in itself.

Use case / purpose	Owner	Data & people	Provider / model	Risk & status
Automated Meeting Notes	Sales Ops	Internal notes	Enterprise AI tool	Review pending
Candidate interview summary	HR	Applicant data	Recruitment vendor	Enhanced review
Internal search chatbot	IT	Knowledge base	RAG platform	Approved / monitored

Minimum viable intake

Purpose • owner • data • affected individuals • vendor • decision • review trigger

BUILT

Risk-based approach: one door, different routes

Do not treat an office productivity assistant and a consequential HR system the same – you will lose credibility
Built your frameworks based on the AI you work with and the risks it inherits.

Fast path

Clear permitted purpose; approved provider; low sensitivity; basic safeguards; recorded owner.

Enhanced review

Sensitive data or material effects; privacy, security, legal and fairness assessment; human oversight.

Stop / redesign

Unlawful purpose, unacceptable risk, inadequate evidence or controls that cannot be made effective.

Set clear rules who is in charge of decisions in each case

Important: organisational risk tiers are not the same as EU AI Act legal classifications – make this difference in your framework

DECIDE

Accountability: advice is not the same as ownership

Not all is the AI Officer / Data Protection Officers responsibility

Business / use-case owner	Purpose, outcomes, operational controls, risk acceptance
AI governance / risk function	Common methodology, register, challenge, reporting
Privacy / DPO	Independent GDPR advice, DPIA guidance, monitoring
Legal / compliance	AI Act and other legal obligations, contractual issues
Security / IT / procurement	Technical assurance, integration, vendor due diligence

Decision rights, escalation thresholds and residual-risk acceptance must be explicit.

ENABLE

Put governance where work already happens

The best control is one people encounter at the right moment.

PROCUREMENT

New AI supplier or feature

IT / CHANGE

Model, integration or data-flow change

PRIVACY BY DESIGN

New processing purpose or data category

BUSINESS LAUNCH

Go-live conditions and owner sign-off

INFORMATION MATERIAL / GUIDELINES

Have documentation ready for information

PREPARED MATERIALS

Transparency & presentation templates etc....

One shared intake • reused evidence • specialist review only when triggered

Monitor your AI

When building your AI Audit procedure, take into consideration the practicability and usability!

1. Human in the Loop	Where necessary, install a human in the loop to verify the outcome / decision made
2. Logging	Install logging mechanisms where necessary
3. Quality /Functionality Checks	Find mechanisms and examples to verify the quality / functionality of the AI Tool
4. Documentation	Document the findings and assure you are accountable
5. Escalation	Establish mechanisms to alert the right people about issues and errors
6. Audit	Audit frequency should be adapted to the risk and frequence of usage

LESSONS LEARNED

What tends not to work — and what to do instead

LESS EFFECTIVE	MORE WORKABLE
40-page policy nobody uses	**Short rules, examples and decision aids**
Same assessment for every tool	**Tiered review based on purpose and impact**
DPO as sole gatekeeper	**Business accountability + independent DPO advice**
Committee approves everything	**Delegation and clear escalation thresholds**
One-off approval	**Owner, triggers, monitoring and periodic review**

TAKEAWAYS

Six actions to take back to your organisation

1. **Talk to your teams – train them!**
2. Make AI use visible with a lightweight inventory.
3. Create one intake with proportionate assessment paths.
4. Clarify ownership, decision rights and escalation.
5. Connect AI controls to existing business processes.
6. Define monitoring and material-change triggers.

Good governance makes better decisions easier — and risky decisions harder to ignore.

QUESTIONS?

Olivia Roth
Olivia.roth@yrnet.com
https://www.linkedin.com/in/olivia-roth-92827b13a/