⚡ AI GOVERNANCE ROADMAP

# 5 Phase Roadmap for AI Governance : *From Policy To Practice.*

**A structured roadmap for building AI governance from the ground up.**

***Grounded in NIST AI RMF, EU AI Act, and ISO 42001.***

For AIGP candidates, compliance leads, DPOs & risk managers.

1. Foundation
2. Risk
3. Implementation
4. Monitoring
5. Audit

→ SAVE & SHARE

*Swipe →*

# Three ways governance *programmes die.*

1. Produce a policy but fail to operationalise it
2. Build a risk framework but lack the data to populate it
3. Complete an assessment but have no mechanism to act on findings

**Same root cause every time:**

***Governance was designed as a document exercise — not an operational system.***

01

# Foundation

*Establish accountability & policy*

1. Appoint an AI governance lead or committee with clear accountability
2. Define your AI Acceptable Use Policy: what is permitted, prohibited, and who approves exceptions
3. Create an AI inventory — a register of ALL AI systems in use or development, including third-party tools
4. Map roles under applicable regulations (provider, deployer, distributor under EU AI Act)
5. Establish a governance review cadence: quarterly minimum

02

# Risk Assessment

*Classify & prioritise by risk*

1. Classify each AI system: Unacceptable(prohibited), High-risk, Limited risk, or minimal risk
2. Conduct an AI Impact Assessment (AIA) for high-risk systems
3. Complete DPIAs for systems processing personal data at scale
4. Document identified risks in a risk register with likelihood, severity, and ownership
5. Prioritise remediation based on residual risk, not inherent risk alone

03

# Implementation

*Operationalise controls across lifecycle*

1. Apply NIST AI RMF Govern and Manage functions to embed controls in development workflows
2. Implement human oversight mechanisms for high-risk systems
3. Define incident response procedures for AI failures or unexpected outputs
4. Establish data governance: training data provenance, quality checks, and retention
5. Document technical documentation requirements per EU AI Act Article 11

04

# Monitoring

*Track performance, drift & compliance*

1. Define key performance indicators for each high-risk AI system
2. Monitor for model drift: degradation in accuracy or fairness over time
3. Track bias indicators across demographic groups where relevant
4. Log incidents, near-misses, and user complaints in a structured format
5. Report to the governance committee on a defined schedule

05

# Audit & Improvement

*Test, verify & iterate*

1. Conduct internal audits of high-risk systems against documented controls
2. Commission third-party conformity assessments where required by regulation
3. Review and update risk assessments after significant model changes
4. Feed audit findings back into Phase 1 policy review
5. Build a culture of accountability: governance fails when treated as a compliance checkbox

# One Roadmap. Three Frameworks.

| Perspective | NIST AI RMF (Risk governance) | EU AI Act (Regulatory compliance) | ISO 42001 (Operational management) |
|---|---|---|---|
| **Governance (cross-cutting)** | Govern (continuous) | Roles, obligations (providers/deployers) | Context, Leadership |
| **Risk Identification** | Map | Risk classification | Planning (risk & impact assessment) |
| **Risk Analysis** | Map | Risk management system, testing, documentation | Risk assessment + evaluation |
| **Risk Treatment** | Manage | Technical controls, human oversight, docs | Operation (controls, Annex A) |
| **Monitoring** | Measure (ongoing) | Post-market monitoring | Performance evaluation |
| **Assurance** | Govern / Manage (review) | Conformity assessment | Internal audit |
| **Continuous Improvement** | Iterative loop | Implicit via compliance updates | Improvement (Clause 10) |

# Five Ways Governance Fails

- ✗ Starting with a policy document instead of an inventory — you cannot govern what you have not identified
- ✗ Treating risk classification as a one-time exercise — AI systems evolve, and so must their risk tier
- ✗ Assigning governance to a single team with no executive sponsorship — governance without authority can't enforce controls
- ✗ Conflating compliance with governance — compliance is the legal minimum, governance is what makes AI trustworthy
- ✗ Skipping decommissioning — retired AI systems without proper data disposal create long-tail risk

# Governance is not a policy.

# *It's an operational system.*

Repeatable processes. Accountable roles. Feedback loops.

That's what keeps AI systems aligned with your values

and your regulatory requirements — over time.

**NIST AI RMF** | **EU AI Act** | **ISO 42001**

💾 **SAVE THIS ROADMAP**

5 phases. 3 frameworks. One path from policy to practice.

♻️ Repost · 💬 Which phase does your org get stuck at?

#AIGovernance #AIGP #EUAIAct #ResponsibleAI