FRACTO

# Enterprise AI Governance Framework

Roadmap

A Practical Playbook for 2026

ISO 42001 NIST AI RMF EU AI Act Policy Templates Checklist

## What's Inside

- ISO 42001-aligned AI Management System (AIMS) framework
- NIST AI RMF integration and dual-tier governance model
- EU AI Act obligations guide — providers, deployers, GPAI
- RACI matrix for AI governance accountability across teams
- 30-point enterprise AI governance checklist
- 12-month phased implementation roadmap

2026 Edition | Enterprise AI Series

fracto.ie • rahul@fracto.ie

# Table of Contents

SECTION 00

# Introduction

Enterprises are no longer asking ***whether*** to use AI — they are asking **how to govern it responsibly at scale.** Regulators, customers and boards are converging on the same expectation: AI must be governed with the same rigour applied to financial, legal and information-security risk.

The EU AI Act, ISO/IEC 42001:2023 and the NIST AI Risk Management Framework now give enterprises a coherent, interlocking set of tools to build that governance — but only if they are implemented together in a practical operating model. This playbook shows you how.

| | |
|---|---|
| **Who this is for** | Boards, CIOs, CTOs, CISOs, CDOs, General Counsel, and Risk & Compliance leaders responsible for deploying or governing AI across enterprise or regulated environments. |
| **How to use it** | Work through each section in order for a full implementation journey, or jump directly to the RACI matrix, policy templates or checklist for immediate operational use. |

SECTION 01

## Why AI Governance Is Different from Traditional IT Governance

Traditional IT governance focuses on uptime, access control and change management. AI governance adds fundamentally new dimensions that existing frameworks do not address:

| | |
|---|---|
| **Model Behaviour & Drift** | AI systems change over time as data distributions shift. Governance must include continuous monitoring for performance degradation and unexpected behavioural change. |
| **Bias, Fairness & Disparate Impact** | AI outputs can systematically disadvantage individuals or groups. Governance requires documented fairness assessments and remediation processes before and after deployment. |
| **Explainability & Transparency** | Decision-makers and regulators increasingly require AI decisions to be understandable. Governance must define when explanations are required and what form they must take. |
| **Data Lineage & Use Constraints** | Training data constraints do not automatically apply to inference. Governance must track how data flows from sourcing through training to production and reuse. |
| **Autonomy & Human Oversight** | High-stakes AI decisions require defined human oversight checkpoints. Governance must specify when humans must review, override or formally approve AI outputs. |

**Key implication:** Enterprises need a dedicated AI governance function — not an extension of cyber or data governance. The five dimensions above require specialised policies, roles, tools and processes that sit alongside, but are distinct from, existing governance frameworks.

SECTION 02

# Frameworks That Matter — ISO 42001 & NIST AI RMF

Two frameworks form the backbone of enterprise AI governance in 2026. Used together, they provide both the management system structure and the risk-based analytical lens.

## ISO/IEC 42001:2023 — AI Management System (AIMS)

ISO/IEC 42001 is the first international standard for AI management systems, published December 2023. It is certifiable — organisations can obtain third-party certification, similar to ISO 27001 for information security.

**1**

### Scope & Context

- Define how AIsupports organisational strategy
- Identify interested parties and their requirements
- Determine governance scope (internal and vendor AI)

**2**

### Policies & Objectives

- Enterprise AI acceptable use policy
- Prohibited uses and data sourcing rules
- Measurable AI governance objectives

**3**

### Risk Assessment

- AI-specific risk identification and analysis
- Bias, fairness, safety, security and compliance risks
- Tiered risk classification per AI system

**4**

### Lifecycle Controls

- Ideation to development to validation to deployment
- Monitoring, incident response, decommissioning controls
- Change management and model version control

**5**

### Continual Improvement

- Internal auditsand management review processes
- Corrective actions and root-cause analysis
- Optional: third-party ISO 42001 certification readiness

## NIST AI Risk Management Framework (AI RMF)

TheNIST AIRMF isavoluntaryframework fromtheUSNational Institute of Standards and Technology, applied per AI system to identify, analyse and treat risks in context.

| Function | Purpose | Key Activities |
|---|---|---|
| **GOVERN** | Culture, policies and processes to manage AI risk | AI policy, roles, oversight structures, accountability frameworks |
| **MAP** | Context and system definition including stakeholders and impacts | Use-case scoping, stakeholder mapping, AI risk categorisation |
| **MEASURE** | Tools and methods to analyse and monitor AI risks | Bias testing, explainability, red-teaming, drift monitoring |
| **MANAGE** | Risk treatment, controls and continuous improvement | Mitigation plans, residual risk acceptance, incident response |

**Recommended approach:** Use ISO 42001 as the structural backbone of your AI Management System — policies, roles, audits and continual improvement. Apply the NIST AI RMF functions as the risk-based lens for each individual AI system or use case. This dual-tier model avoids checklist compliance and makes governance both structured and adaptive.

SECTION 03

# EU AI Act — Obligations for Enterprises

The EU AI Act is the world's first comprehensive AI law. It applies to providers, deployers, importers and distributors of AI systems in the EU, with penalties up to **35 million euros or 7% of global turnover** for the most serious violations. Even non-EU organisations serving EU customers or processing EU data may fall within scope.

## Risk Classification

| Risk Tier | Examples | Core Obligations | Max Penalty |
|---|---|---|---|
| **Unacceptable Risk** | Social scoring, biometric surveillance in public spaces, subliminal manipulation | BANNED — must not be placed on the market | 35M€ or 7% |
| **High Risk** | Credit scoring, hiring AI, safety-critical systems, essential services AI | Risk management, data governance, human oversight, documentation, EU registration | 15M€ or 3% |
| **Limited Risk** | Chatbots, deepfakes, emotion recognition in certain contexts | Transparency obligations — users must know they are interacting with AI | 7.5M€ or 1.5% |
| **Minimal Risk** | Most other AI systems — spam filters, AI-assisted writing, recommendation engines | No specific obligations beyond existing EU law; voluntary codes encouraged | No specific fines |

## Key Obligations for High-Risk AI Systems

| Obligation Area | Providers must... | Deployers must... |
|---|---|---|
| **Risk Management** | Establish and maintain a documented risk management system across the full AI lifecycle. | Implement their own risk management and ongoing monitoring processes. |
| **Data Governance** | Ensure training, validation and testing datasets are relevant, representative and as error-free as possible. | Verify that data used in their deployment context meets applicable governance standards. |
| **Human Oversight** | Build in technical measures enabling humans to understand, monitor and intervene in AI outputs. | Assign responsibility for oversight; ensure staff are trained and empowered to intervene. |
| **Documentation & Logs** | Maintain technical documentation and logs demonstrating compliance across all Act requirements. | Retain records sufficient to demonstrate appropriate deployment and monitoring practices. |
| **Registration & Assessment** | Register high-risk AI systems in the EU database before placing on the market. | Conduct a Fundamental Rights Impact Assessment (FRIA) where required by the Act. |

***Timeline: Obligations for high-risk AI systems take effect from August 2026. General-purpose AI (GPAI) model obligations, including mandatory adversarial testing and systemic risk assessments for frontier models, phase in through 2027.***

SECTION 04

# AI Governance Operating Model, Policies & RACI

Frameworks only deliver value when translated into a clear operating model. Use this section to define who does what, and to embed governance into your organisation's existing processes and decision structures.

## Governance Operating Model — Five Core Components

**1**

### Strategy & Scope

- Define how AIsupports business strategy and risk appetite
- Scope governance to include vendor-supplied and embedded AI
- Publish AI principles and acceptable use boundaries

**2**

### Roles & Committees

- AI SteeringCommittee with cross-functional executives
- AI Governance Office: policies, inventory, assessments, training
- Named RACI for every significant AI system

**3**

### Policies & Standards

- Acceptableuse,data sourcing, model risk, oversight, incidents
- Model development, validation and decommissioning standards
- Human-in-the-loop design and explainability guidelines

**4**

### Process & Lifecycle

- Ideation,risk screening, design, development, validation, deployment, monitoring, retirement
- Checkpoints: risk assessment, ethics review, legal and compliance sign-off
- Integration into SDLC, data governance and change management

**5**

### Tooling & Integration

- AIsystem inventory and catalog — models, datasets, use cases
- Policy enforcement through identity and access controls
- Monitoring for drift, bias, performance and security events

## RACI Matrix — AI Governance Accountability

UsethisRACItoassignclearaccountabilityacrossyourtechnology, risk, legal and business teams for every key AI governance activity.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| R | = Responsible | A | = Accountable | C | = Consulted | I | = Informed |

| Activity / Control Area | Tech & Eng | Risk & Legal | Data & AI | Business |
|---|---|---|---|---|
| AI system inventory and catalogue maintenance | R | C | A | I |
| AI risk classification per system | C | A | R | C |
| Enterprise AI policy authorship and approval | C | A | C | I |
| Model development and validation controls | R | I | A | C |
| Bias and fairness assessment | C | C | R | A |
| Human oversight procedure design | R | A | C | C |
| EU AI Act impact analysis and compliance mapping | C | A | R | I |
| FRIA (Fundamental Rights Impact Assessment) | C | A | C | R |
| AI vendor and third-party risk review | R | A | C | I |
| Monitoring for drift, bias and performance | R | I | A | C |
| AI incident detection, response and escalation | R | A | C | C |
| ISO 42001 internal audit and continual improvement | C | A | R | I |
| Staff training on AI governance processes | I | C | R | A |
| Board and executive AI governance reporting | C | A | R | I |
| Generative AI acceptable use enforcement | R | C | A | C |

SECTION 05

# Policy Templates for Core Operational Controls

The following templates provide a starting framework for the three core policies required before any enterprise AI system goes into production. Adapt each template to your organisation's specific risk profile, vendors and regulatory environment.

## Policy Template 1 — Acceptable AI Use Policy

| | |
|---|---|
| 1 | Scope: All AI model training, testing, fine-tuning and inference activities that use or could produce data about individuals, covering internally built and vendor-supplied systems. |
| 2 | Classification: Every AI system must be classified at intake using the enterprise AI risk taxonomy (minimal / limited / high / unacceptable), with documented rationale and annual review. |
| 3 | Prohibited uses: AI must not be used for social scoring, covert biometric surveillance, or any purpose that constitutes an unacceptable-risk practice under the EU AI Act or applicable law. |
| 4 | Generative AI controls: Employees must not input confidential, personal or proprietary data into unapproved public AI tools. Only enterprise-licensed, contractually bound tools are permitted. |
| 5 | Vendor AI: Third-party AI embedded in SaaS or via API is subject to the same policy obligations. Procurement must complete an AI vendor risk assessment before contract signature. |
| 6 | Review cycle: Policy reviewed annually, or upon any material change in AI use, regulatory landscape or significant incident involving an AI system. |

## Policy Template 2 — Access Control & Human Oversight

| | |
|---|---|
| 1 | Principle: Least privilege by default. No user, service account or AI system may access more data than is strictly necessary for its defined purpose. |
| 2 | Authentication: All human access to AI training environments, data stores and inference APIs requires MFA and SSO integration with the organisation's identity provider. |
| 3 | Role-based controls: Access roles must be defined per AI system, reviewed quarterly, and any changes to privileged roles require dual approval. |
| 4 | Service accounts: AI pipelines must use short-lived credentials. Permanent, embedded secrets in code or containers are prohibited. |
| 5 | Human oversight access: Authorised reviewers must be able to examine and override AI outputs at any time. Oversight access must be logged and reviewed monthly. |
| 6 | Offboarding: System and data access must be revoked within four hours of departure. Quarterly access recertification is mandatory for all AI-system-touching roles. |

## Policy Template 3 — Audit Logging & Monitoring

| | |
|---|---|
| 1 | Coverage: Logging must capture all AI system inputs and outputs or summaries, all data access events, all administrative actions, and all model deployment and change events. |
| 2 | Log format: Logs must include timestamp in UTC, user or service identity, action type, data resource accessed, source system and session ID. Structured JSON is recommended. |
| 3 | Retention: All logs must be retained for a minimum of five years in an immutable, tamper-evident store. High-risk AI system logs require six-year retention minimum. |
| 4 | Monitoring: Real-time alerting must flag abnormal query volumes, after-hours access, model performance degradation beyond defined thresholds, and failed authentication above baseline. |
| 5 | Incident response: Any confirmed anomaly triggers the AI incident response protocol within four hours. Serious incidents involving EU high-risk AI systems must be reported to the EU AI Office. |
| 6 | Review: Logging configuration and alert ruleset must be tested at least annually and after any significant AI system change or incident. |

SECTION 06

# 12-Month Enterprise AI Governance Roadmap

A practical way to build an enterprise AI governance programme is to follow a phased 12-month roadmap aligned to ISO 42001 and NIST AI RMF. Each phase has clear objectives, key steps and deliverables.

## Phase 1 — Months 0–3 — Discovery & Foundations

| | |
|---|---|
| 1 | **Create an AI System Inventory:** Catalogue all AI systems: in-house models, GPT-based tools, vendor AI in SaaS, RPA with AI components. Capture ownership, purpose, data used, model types, deployment environment and business criticality. |
| 2 | **Gap Assessment Against ISO 42001 & NIST AI RMF:** Use ISO 42001 clauses and NIST AI RMF functions as a gap checklist. Identify weaknesses in governance, documentation, risk assessments and monitoring. |
| 3 | **Establish Governance Structures:** Form an AI Steering Committee and AI Governance Office. Define responsibilities, decision-making authority and escalation paths. |
| 4 | **Set High-Level Policies & Principles:** Publish initial AI principles covering transparency, fairness and accountability. Issue interim guidance on generative AI use, including restrictions on unapproved tools. |

## Phase 2 — Months 3–6 — Policies, Risk Framework & Pilot Controls

| | |
|---|---|
| 1 | **Develop Enterprise AI Policies & Standards:** Draft and approve policies across acceptable use, data sourcing, model risk, human oversight and incidents. Align language with ISO 42001 requirements for an AI management system. |
| 2 | **Define AI Risk Taxonomy & Assessment Process:** Classify AI systems as minimal, limited, high or unacceptable risk. Create a standard risk questionnaire and scoring model covering privacy, fairness, safety, security, compliance and reputation. |
| 3 | **Select 2–3 Pilot Systems for Governance Implementation:** Apply the full lifecycle to a representative set: one internal tool, one customer-facing AI and one high-risk use case. Document lessons learned for programme-wide rollout. |
| 4 | **Integrate with Existing Governance:** Embed AI reviews into change advisory boards, architecture review boards and data governance forums to avoid parallel processes. |

## Phase 3 — Months 6–9 — Scale Governance & Prepare for EU AI Act

| | |
|---|---|
| 1 | **Roll Out Risk Assessments Portfolio-Wide:** Run quick-scan assessments on all catalogued AI systems; categorise by risk level. Prioritise high-risk systems for deeper review and remediation. |
| 2 | **Implement Monitoring & Incident Processes:** Define KPIs and KRIs for all AI systems. Configure monitoring, alerting and rehearse incident response for AI-related issues including bias events and performance failures. |
| 3 | **Map EU AI Act Obligations:** Identify all systems in EU scope. Classify by Act risk category and determine whether you are a provider or deployer. Begin building documentation and human oversight controls for high-risk systems. |
| 4 | **Training & Culture:** Run targeted training for product, data and engineering teams. Deliver awareness sessions for executives and business leaders. |

| Phase 4 | Months 9–12 | Formalise AIMS & Pursue Certification (Optional) |
|---|---|---|
| 1 | **Document the AI Management System (AIMS):** Consolidate policies, procedures, roles and evidence of operation including meeting minutes, risk logs and audit records. Link AI governance into enterprise risk management. | |
| 2 | **Internal Audits & Continuous Improvement:** Conduct internal audits against ISO 42001 and NIST AI RMF. Implement corrective actions, update policies and close residual gaps. | |
| 3 | **External Certification (Optional but Powerful):** Decide whether to pursue ISO 42001 certification to demonstrate maturity to regulators and customers. If yes, engage a certification body and prepare audit evidence. | |
| 4 | **Refine Governance for General-Purpose AI (GPAI):** As EU AI Act obligations for GPAI models phase in, ensure model providers and internal teams conduct evaluations, red-teaming and systemic risk assessments. | |

SECTION 07

# 30-Point Enterprise AI Governance Checklist

Complete this checklist before launching any material AI initiative. If you cannot confirm the majority of these items, your AI governance programme requires further development before scale deployment.

| STRATEGY & SCOPE | |
|---|---|
| ■ | AI principles published and approved by executive leadership |
| ■ | AI strategy explicitly linked to business objectives and risk appetite |
| ■ | Scope of AI governance defined — covers internal builds, vendor AI and embedded AI |
| ■ | AI system inventory maintained and reviewed at least quarterly |

| ORGANISATION & ROLES | |
|---|---|
| ■ | AI Steering Committee or governance board formally established |
| ■ | AI Governance Office or cross-functional team designated with clear mandate |
| ■ | Named owner assigned to every significant AI system |
| ■ | RACI documented for all governance activities — assessments, approvals, monitoring |

| POLICIES & STANDARDS | |
|---|---|
| ■ | Enterprise AI policy covering acceptable and prohibited uses approved |
| ■ | Data sourcing and consent policy for training and inference in place |
| ■ | Model risk and validation standard defined, tiered by risk level |
| ■ | Human oversight and explainability guidelines published |
| ■ | Incident management procedure for AI-related harms and breaches tested |

| RISK MANAGEMENT & COMPLIANCE | |
|---|---|
| ■ | AI risk taxonomy aligned with EU AI Act concepts (minimal/limited/high/unacceptable) |
| ■ | Standard risk assessment template in use for all new AI initiatives |
| ■ | High-risk AI systems identified, documented and prioritised for remediation |
| ■ | EU AI Act impact analysis completed and obligations mapped |
| ■ | Fundamental Rights Impact Assessment (FRIA) process defined for in-scope systems |

| SECURITY & TECHNICAL CONTROLS |
| --- |
| ■ Access and identity controls enforced for all AI systems and data stores |
| ■ Data protection (encryption at rest and in transit) applied consistently |
| ■ Separation of development, test and production AI environments enforced |
| ■ Red-teaming and adversarial testing performed on high-risk or customer-facing systems |
| ■ Monitoring in place for drift, bias, performance degradation and abuse |
| ■ Logs and evidence retained per policy for audit and investigation purposes |

| CULTURE & TRAINING |
| --- |
| ■ Governance training delivered to product, data and engineering teams |
| ■ Awareness sessions completed for executive and business stakeholders |
| ■ Clear escalation channels for raising AI risk concerns or incidents |
| ■ Governance metrics reported to board — compliance rates, incidents, audit findings |

SECTION 08

# Next Steps with Fracto

This framework gives you the governance architecture, frameworks, RACI, policy templates, roadmap and checklist to begin a structured enterprise AI governance programme. The next step is a structured assessment of where your organisation stands today.

## Enterprise AI Governance & EU AI Act Readiness Workshop

A structured 3–5 day engagement with your technology, risk, legal and business leadership. Deliverables include:

- Current-state assessment of your AI inventory, policies and governance maturity
- Gap analysis against ISO 42001, NIST AI RMF and EU AI Act obligations
- Identification of high-priority remediation actions and quick wins
- Design of a 12-month roadmap and operating model tailored to your risk profile
- Alignment of stakeholders from legal, risk, technology and the business

## Download the Enterprise AI Governance Framework Template

- ISO 42001-aligned AI Management System structure and policy language
- NIST AI RMF-based risk assessment questionnaire (Excel)
- EU AI Act readiness checklist and scope analysis tool
- Editable RACI matrix (Excel) and governance committee charter template
- Sample AI acceptable use, oversight and incident management policies (Word)

## Contact Fracto

**Email:** rahul@fracto.ie
**Web:** fracto.ie

Fracto is an AI & digital transformation advisory firm specialising in enterprise AI governance, compliance and regulated industry deployments.