This resource is general information only. It does not constitute legal, regulatory, tax, or certification advice and should not be relied upon as a substitute for tailored professional advice. See full disclaimer on page 2.

**THEODORA MONYE | AI Governance Advisor**

# AI GOVERNANCE FRAMEWORKS COMPARISON

## EU AI Act | NIST AI RMF | ISO/IEC 42001 — Practical Implementation Roadmap

*Version: v2.0 — Date: June 2026. Information accurate as at the date stated. Laws, standards, and certification practices change; confirm current status before making legal, compliance, or certification decisions.*

## FRAMEWORK COMPARISON AT A GLANCE

| ASPECT | EU AI ACT | NIST AI RMF | ISO/IEC 42001 |
|---|---|---|---|
| **Status** | Mandatory Regulation | Voluntary Framework | Certifiable standard (published 2023). Certification issued by accredited bodies; national accreditation arrangements and timelines may vary. |
| **Nature** | Legal Compliance | Risk Methodology | Management System (AIMS) |
| **Geographic** | EU + Global (if used in EU) | Global (US Origin) | International (ISO) |
| **Focus** | Rights, Safety and Fines | Technical Risk Functions | Operational Structure |
| **Penalties** | Tiered fines (Article 99): up to 7% global turnover for prohibited AI systems; up to 3% for other infringements; up to 1.5% for incorrect information to authorities. Fixed euro amounts apply where lower. | N/A | Loss of certification following surveillance or recertification audit failure. |
| **Best Use** | EU Market Alignment | Risk Process Maturity | Enterprise B2B Trust |

**■ EU AI Act Scope: Annex I vs Annex III**

**Annex I** lists the AI techniques in scope (e.g. machine learning, logic-based approaches). This defines what counts as an AI system under the Act. **Annex III** lists the high-risk use cases subject to strictest obligations (e.g. biometric identification, critical infrastructure, employment, education, law enforcement). If your system falls within an Annex III category and uses an Annex I technique, full high-risk compliance requirements apply. Confirming which annex applies is the first scoping step.

## INTEGRATED STRATEGY (A 360-Degree Governance Shield)

• **EU AI Act:** Defines the legal boundaries you must stay within. • **NIST AI RMF:** Provides the technical engine to measure and manage risk. • **ISO 42001:** Provides the management shell to sustain and certify efforts.

## ILLUSTRATIVE SCENARIO EXAMPLES

Which framework to prioritise depends on your immediate obligation. Most organisations need elements of all three; the column below indicates where to start.

| SITUATION | PRIMARY FRAMEWORK | RATIONALE |
|---|---|---|
| Launching AI in European markets | EU AI Act | Mandatory legal obligation; compliance not optional for in-scope systems. |
| Scaling B2B enterprise sales | ISO/IEC 42001 | Certifiable governance proof; increasingly required by enterprise procurement. |
| Building internal AI risk management capability | NIST AI RMF | Structured risk functions (GOVERN, MAP, MEASURE, MANAGE) for systematic management. |
| Demonstrating board-level AI accountability | ISO/IEC 42001 + EU AI Act | ISO 42001 Clause 5 (Leadership) + EU AI Act Article 17 (Quality Management). |
| Regulated-sector AI audit (pharma, financial services, healthcare) | All three frameworks | Sector regulators increasingly reference EU AI Act, ISO 42001, and NIST RMF together. |

# 12-MONTH IMPLEMENTATION PLAN

Indicative timeline for organisations with moderate existing AI governance maturity. Actual timing depends on organisation size, complexity, resourcing, audit findings, and certification body schedules. This plan does not guarantee certification within 12 months.

### MONTHS 1-4: FOUNDATION

- Multi-framework Gap Analysis
- NIST GOVERN implementation
- System Inventory and Classification
- Secure Board sponsorship

### MONTHS 5-8: COMPLIANCE

- NIST MAP and MEASURE execution
- High-risk system documentation
- Data governance review
- Technical AI Safety testing

### MONTHS 9-11: STRUCTURE

- ISO 42001 AIMS Documentation
- Internal audit and remediation
- Operational controls rollout
- Employee awareness training

### MONTH 12: CERTIFICATION

- NIST MANAGE monitoring
- Stage 1 external audit (docs)
- Stage 2 external audit (impl)
- Certification decision (indicative; typically issued several weeks after Stage 2 completion)

## ISO/IEC 42001 — Certification Pathway

- Readiness assessment and gap remediation
- Development of AIMS (policies, procedures, records)
- Internal audit and management review
- Stage 1 and Stage 2 audits by accredited bodies
- Certification decision and ongoing surveillance

### On Framework Relationships

ISO 42001 does not replace the law; it provides the mechanism to demonstrate you follow it. The three frameworks are complementary, not interchangeable. Overlap exists across governance, risk, and documentation requirements, but each framework addresses distinct obligations and should be scoped separately.

## FUNCTIONAL MAPPING AND ALIGNMENT

| NIST CORE | ISO 42001 / EU AI ACT ALIGNMENT |
|---|---|
| **GOVERN** | Policy, Leadership (Cl. 5) and Transparency (EU AI Act Art. 13) |
| **MAP** | Context (Cl. 4) and Annex III risk classification (EU AI Act Art. 6) |
| **MEASURE** | Performance Evaluation (Cl. 9) and Technical Documentation (EU AI Act Art. 11) |
| **MANAGE** | Operational Controls (Cl. 8) and Post-Market Monitoring (EU AI Act Art. 72) |

## WHEN TO SEEK EXPERT HELP

**What I can do:** Advisory, gap analyses, risk mapping, AIMS documentation drafting, readiness preparation, executive coaching.

**What I cannot do:** Regulated legal advice, formal legal opinions, or act as an accredited certification body.

**GAP ANALYSIS • IMPLEMENTATION • AUDIT • TRAINING**

### Disclaimer and Limitation of Liability

*The contents of this document are provided for general information and advisory purposes only and do not constitute legal, regulatory, tax, or certified-audit advice. Theodora AI Advisory provides independent advisory services; this document does not create a client-lawyer relationship and is not a substitute for obtaining specific legal or certification body advice. While reasonable efforts have been made to ensure accuracy as at the date shown, laws, standards, and certification practices change and may differ by jurisdiction. Users should obtain tailored professional advice before acting on the information provided.*

*To the fullest extent permitted by applicable law, Theodora AI Advisory's liability for any claim arising out of or in connection with this document is limited to the fees paid for the advisory services provided. Theodora AI Advisory shall not be liable for any indirect, special, consequential, or punitive losses, or for any loss of profit, loss of business, or reputational loss arising from reliance on this document.*