




AI GOVERNANCE FRAMEWORKS COMPARISON

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

Version: v1.0 — Date: March 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 is issued by accredited certification 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 & Fines	Technical Risk Functions	Operational Structure
Penalties	Tiered fines under the EU AI Act. Depending on type/severity, penalties can include fines of up to 7% of global annual turnover or specified euro amounts.	N/A	Loss of Certification
Best Use	EU Market Alignment	Risk Process Maturity	Enterprise B2B Trust

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.

SCENARIO DECISION TOOL

REQUIREMENT	RECOMMENDED FRAMEWORK
Launch AI in European Markets	EU AI Act (Mandatory Duty)
Scale B2B Enterprise Sales	ISO/IEC 42001 (Certifiable Proof)

12-MONTH IMPLEMENTATION PLAN

Indicative timeline: The 12-month implementation plan is an illustrative, 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 & Classification
- Secure Board sponsorship

MONTHS 5-8: COMPLIANCE

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

MONTHS 9-11: STRUCTURE

- ISO 42001 AIMS Documentation
- Internal audit & 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)

FUNCTIONAL MAPPING & ALIGNMENT

ISO/IEC 42001 — Certification pathway

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

NIST CORE	ISO 42001 / EU AI ACT WALK
GOVERN	Policy, Leadership (Cl. 5) & Transparency
MAP	Context (Cl. 4) & EU Classification
MEASURE	Performance Eval (Cl. 9) & Technical Docs
MANAGE	Operational Controls (Cl. 8) & Monitoring

Common Myths: ISO 42001 does not replace the law; it provides the mechanism to prove you follow it. Frameworks overlap by ~70%.

WHEN TO SEEK EXPERT HELP

What I can do: Advisory, gap analyses, risk mapping, AIMS documentation drafting, readiness prep, 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.