Regulation at a Glance: EU AI Act, ISO/IEC 42001, and NIST AI RMF

A free artifact of AI GOVERNANCE CHAIN™. The map is free. The compliance packs that satisfy each requirement are the paid path.

Abbreviations and Acronyms

No prior knowledge is assumed. Every acronym used in this document is defined below.

AI: Artificial Intelligence

AIMS: Artificial Intelligence Management System

EU: European Union

EU AI Act: the European Union Artificial Intelligence Act (Regulation (EU) 2024/1689)

ISO/IEC 42001: the international standard for Artificial Intelligence Management Systems, published in December 2023 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

NIST AI RMF: the Artificial Intelligence Risk Management Framework of the National Institute of Standards and Technology (United States)

Who this is for

Compliance leaders, executives, and architects who need to understand, on a single page, the three reference points that now shape AI governance worldwide, and how they relate to one another.

Why this exists (the WHY)

Three distinct instruments dominate the AI governance conversation. They are often confused with one another, yet they do different jobs: one is law, one is a certifiable standard, and one is a voluntary framework. Knowing which is which, and what each demands, is the difference between focused effort and wasted effort.

The three instruments at a glance

1. The EU AI Act (Law)

- - What it is. The European Union's regulation on artificial intelligence, the first comprehensive AI law of its kind. It is binding.
- - How it works. It classifies AI systems into risk tiers: unacceptable risk (prohibited), high risk (strict obligations), limited risk (transparency duties), and minimal risk (largely unrestricted).

- - Why it matters. It applies to organizations that place AI systems on the EU market or whose AI outputs are used in the EU, regardless of where the organization is based. Its obligations are being phased in over time, with prohibited practices and high-risk requirements applying on a staggered schedule.
- - Who should care most. Any organization operating high-risk AI with an EU connection.

2. ISO/IEC 42001 (Certifiable Standard)

- - What it is. The first international management system standard for artificial intelligence, published in December 2023.
- - How it works. It defines requirements for an AI management system: policies, objectives, controls, roles, and continual improvement. An organization can be independently certified against it.
- - Why it matters. Certification provides external, verifiable proof that an organization governs AI systematically. It is increasingly requested in procurement and partnership.
- - Who should care most. Organizations that want to demonstrate governance maturity to customers, regulators, or partners.

3. NIST AI RMF (Voluntary Framework)

- - What it is. The AI Risk Management Framework from the United States National Institute of Standards and Technology. It is voluntary guidance, not law.
- - How it works. It is organized around four functions: Govern (set the culture and oversight), Map (understand context and risk), Measure (assess and track risk), and Manage (act on risk).
- - Why it matters. It is a widely adopted, practical structure for building a risk-based AI program, and it maps cleanly onto both the EU AI Act and ISO/IEC 42001.
- - Who should care most. Any organization building a risk program, especially those wanting a structure that bridges law and certification.

How they fit together

Think of them as law, proof, and method. The EU AI Act tells you what you must do. ISO/IEC 42001 lets you prove you do it. NIST AI RMF gives you a practical way to organize the work. They are complementary, not competing. One disciplined governance program can satisfy all three.

Where the free layer ends and the paid path begins

This card gives you the WHAT (the three instruments) and the WHY (what each one is for). It does not give you the HOW: the clause-by-clause obligations, the templates, the readiness checklists, and the crosswalk that maps one effort across all three regimes.

- - For the structured HOW: the EU AI Act Compliance Pack, the ISO/IEC 42001 AIMS Starter Kit, and the NIST AI RMF Workbook.
- - For the WITH-YOU: The Governance Circle.
- - For the DONE-FOR-YOU: the Pre-Scale Governance Audit.

Screenshot this, forward it, pin it. It is the one-page orientation every compliance conversation needs.

Your next step: Get the **EU AI Act Compliance Pack, Full Edition** in the Execution Library (www.aigovernancechain.com/storefront.html, section: The Flagship Packs). Every instrument in the Execution Library is also included in the **Governance Vault**, the all-access annual licence.

AI GOVERNANCE CHAIN™

AI Governance Framework

Member, Harvard Business Review Advisory Council.

Document standard for AI GOVERNANCE CHAIN™: human-first AI governance.