AI IN THE ENTERPRISE

Governance Frameworks

NIST AI RMF · EU AI Act · ISO/IEC 42001 · OECD

PAPER 03 / 04

A Furtherance reference compendium on the intellectual traditions behind organisational design, leadership, execution, and culture.

IN THIS PAPER

Safety concerns become obligations through governance. This paper surveys the four reference points every enterprise AI programme is now measured against — a voluntary risk framework, a binding law, a certifiable standard, and a set of shared principles. The question it answers: what must responsible AI governance actually contain, and how do the major regimes fit together?

The four differ in force and origin but converge on a common spine: risk-based, lifecycle, documented, human-overseen and accountable. A firm that builds to that spine positions itself for whichever specific regime applies — though, as the caveat stresses, the regulatory detail is moving quickly.

NIST AI Risk Management Framework AI RMF 1.0, 2023

United States · voluntary risk framework

CORE THESIS

A **voluntary, flexible** framework for managing AI risk across the lifecycle, organised around four core functions and a definition of what makes AI **trustworthy**. Built to be adaptable across sectors and organisation sizes rather than prescriptive.

FRAMEWORK

Core function	What it covers
Govern	A culture and structure for managing AI risk throughout
Map	Context and the risks a system actually poses
Measure	Analyse, assess and track those risks
Manage	Prioritise and act on them, with monitoring

Trustworthy AI is defined as valid and reliable, safe, secure and resilient, accountable and transparent, explainable, privacy-enhanced, and fair with harmful bias managed. A Generative AI profile extends the framework to foundation models.

SIGNIFICANCE AND CRITIQUE

The most widely referenced voluntary AI-governance framework, influential well beyond the United States. The critique: being voluntary, it relies on organisational will, and it guides process rather than setting a compliance bar.

EU AI Act Regulation 2024/1689

European Union · binding, risk-based law

CORE THESIS

The world's first comprehensive horizontal AI law. It regulates by **risk tier** rather than by technology, escalating obligations as potential harm rises, and reaches any provider or deployer whose systems affect the EU market — a de facto global benchmark.

FRAMEWORK

Risk tier	Treatment
Unacceptable	Prohibited (e.g. social scoring, manipulative or exploitative systems)
High-risk	Strict duties: risk management, data governance, documentation, human oversight, robustness
Limited	Transparency duties (e.g. disclosing AI interaction and AI-generated content)
Minimal	Largely unregulated – the vast majority of systems

The Act entered into force in August 2024 and applies in phases: prohibitions from early 2025, general-purpose AI model obligations from August 2025, and most remaining rules from August 2026. A 2025–26 simplification package (the "Digital Omnibus", agreed in mid-2026) deferred the most demanding high-risk obligations – for use-cases such as recruitment and worker management – to late 2027, and added new prohibitions on non-consensual and abusive synthetic content. Dates and detail continue to move; see the caveat.

SIGNIFICANCE AND CRITIQUE

The global regulatory reference point, exporting its risk-based template through the "Brussels effect". The critique: it is complex and burdensome for smaller firms, and its implementation timeline has already been amended under industry pressure.

ISO/IEC 42001 AI Management System, 2023

International · certifiable management standard

CORE THESIS

The first **certifiable** AI management-system standard. It applies the familiar management-system model – as in quality (ISO 9001) or information security (ISO 27001) – to responsible AI: set policy and objectives, assess risks and impacts, apply controls, and improve continually.

FRAMEWORK

Element of an AI management system	Purpose
Policy and objectives	Leadership commitment and clear aims for responsible AI
AI risk and impact assessment	Assess risks to the organisation and to affected people
Controls (Annex A)	A reference set of safeguards to apply and justify
Plan–Do–Check–Act	Continual monitoring and improvement; auditable

SIGNIFICANCE AND CRITIQUE

Turns AI governance into something **auditable and certifiable**, and integrates cleanly with existing management systems – a practical bridge to demonstrating compliance. The critique: a management-system certificate attests to process, not to the safety of any particular model.

OECD AI Principles 2019, updated 2024

Intergovernmental · values-based principles

CORE THESIS

The first intergovernmental AI standard: a set of **values-based principles** for trustworthy AI, adopted by dozens of governments and echoed in the G20 principles. It also supplied the widely reused **definition of an AI system** that later regimes adopted.

FRAMEWORK

Principle	Commitment
Inclusive growth and wellbeing	AI should benefit people and the planet
Human rights and fairness	Respect for rights, democratic values and equity
Transparency and explainability	Meaningful information and contestability
Robustness, security, safety	Systems function safely across their lifecycle
Accountability	Actors are answerable for proper functioning

SIGNIFICANCE AND CRITIQUE

The shared international baseline, and the common vocabulary beneath most national strategies. The critique: the principles are high-level and non-binding, providing direction rather than enforceable requirements.

A NOTE ON EVIDENCE

This paper is orientation, not compliance advice, and it is a snapshot of a fast-moving landscape. The EU AI Act's timeline in particular has already been amended – high-risk obligations have shifted into late 2027 under the 2026 simplification package – and guidance, standards and national measures continue to evolve. Verify the current position with primary sources and qualified counsel before making compliance decisions.

Synthesis

Framework	Type	Structure	Binding?
NIST AI RMF	Voluntary framework	Govern / Map / Measure / Manage	No – guidance
EU AI Act	Regulation	Four risk tiers + GPAI rules	Yes – law
ISO/IEC 42001	Management standard	AI management system; PDCA	Certifiable, not mandated
OECD Principles	Principles	Five values-based principles	No – intergovern mental

FOR THE OPERATOR

Governance spans a voluntary risk framework (NIST), a binding risk-based law (EU AI Act), a certifiable management standard (ISO/IEC 42001), and shared principles (OECD) – all converging on one spine: risk-based, lifecycle, human-oversight, documentation and accountability. For the operator, the practical move is to build to that spine, which positions the firm for whichever regime bites, while tracking the fast-changing specifics rather than treating any date as fixed. The final paper turns governance and capability into the organisational work of adoption.