EU AI ACT × NIST AI RMF × ISO 42001 · VERIFIED JULY 2026

Twelve cells. Three frameworks. One set of codes.

Boards do not ask whether your framework is elegant. They ask whether it covers what they are required to cover. Every cell of the columns grid, mapped to the article numbers that actually apply. **EU AI Act codes shown here**; the full NIST subcategory and ISO Annex A mappings are on the page and in the PDF.

	HUMAN CAPABILITY	GOVERNANCE	SUPPLY CHAIN
Runtime monitoring & response	Oversight that intervenes and overrides. **Art 14 · Art 26 · Art 4**	Record-keeping, post-market monitoring, serious-incident reporting. **Art 12 · Art 14 · Art 26 · Art 72 · Art 73**	Third-party post-market and robustness to updates. **Art 72 · Art 25 · Art 15 · Art 55 · Art 73**
Application the shipped surface	Deployer use per instructions; oversight design. **Art 4 · Art 14 · Art 26**	Prohibited practices, high-risk classification, FRIA, transparency. **Art 5 · Art 6 · Annex III · Art 9 · Art 26 · Art 27 · Art 50**	Value chain, information to deployers, marking of synthetic content. **Art 25 · Art 13 · Art 50(2)**
Model assurance the release gate	Accuracy and robustness testing you can actually read. **Art 4 · Art 14 · Art 15**	Risk management, technical documentation, conformity assessment. **Art 9 · Art 11 · Annex IV · Art 15 · Art 17 · Art 43**	GPAI provider obligations, including systemic risk. **Art 25 · Art 53 · Art 55**
Data build order starts here	Data-governance competence at this layer. **Art 4 · Art 10**	Data and data governance, QMS, risk management system. **Art 10 · Art 17 · Art 9**	Sourcing, value chain, GPAI training-data summary. **Art 10 · Art 25 · Art 53**

CONFIDENCE, STATED RATHER THAN IMPLIED

EU AI Act: high — verified against EUR-Lex. **NIST AI RMF: high** — verified against AI 100-1 and the AIRC Playbook. **ISO 42001: medium** — Annex A controls taken from agreeing secondary sources, because the standard is paywalled. A crosswalk that does not tell you which rows are weakest is asking to be trusted rather than checked.

HOW TO USE THIS IN THE ROOM

01

Pick the cell your initiative is weakest on. **Read the codes aloud.**

02

Ask who is **named** against each. Not which function — which person.

03

These are conceptual correspondences for board explanation, **not certified equivalences**.

> Coverage is not the same as compliance.
> But you cannot argue compliance without it.

Source: *A Practitioner's Guide to AI Governance* — a framework by Fredrik Lindstrom. Locked verified crosswalk, July 2026 — 13 rows (the AI-literacy prerequisite plus 12 layer × column cells), verified against primary sources for the EU AI Act (Regulation (EU) 2024/1689, EUR-Lex) and NIST AI RMF 1.0 (NIST AI 100-1 plus the AIRC Playbook), and against agreeing secondary sources for ISO/IEC 42001 Annex A. **Date discipline:** Art 4 in force 2 February 2025; Art 50 transparency obligations apply 2 December 2026 (post-Omnibus timing, provisional until Official Journal publication). Never anchor on 2 August 2026 and never describe the Act as fully operational. Mappings are conceptual correspondences, not certified equivalences.

FOLLOW FREDRIK LINDSTROM FOR MORE

Fredrik Lindstrom

AI and cybersecurity governance for boards, CISOs and senior leaders. 25+ years in enterprise security.

A practitioner to guide you.

ARTICLES & BOARD ADVISORY
fredriklindstrom.info
Long-form governance analysis and toolkits

LINKEDIN
in/fredriklindstrom
Daily commentary and article launches

YOUTUBE
@Promise-and-Risk-AI
AI education without the hype or fear

COMPANION SITE
promiseandrisk.ai
Episode notes, sources and explainers

NEWSLETTER
The Governance Memo
Monthly, board-facing. Subscribe at fredriklindstrom.info