

# AI Governance Glossary

*Plain definitions of the terms buyers meet in AI governance: EU AI Act roles and risk tiers, ISO/IEC 42001, NIST AI RMF, model risk, guardrails, red teaming, bias audits and LLM risks.*

Updated October 29, 2026

---

Terms are grouped by topic. Where a law or standard defines a term, we follow its wording.

## EU AI Act terms

**AI system.** "A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment", and that infers from its input how to generate outputs such as predictions, content, recommendations or decisions ([EU AI Act, Article 3, via Article 26 page](#)).

**Provider.** A person or body that develops an AI system or general-purpose AI model, or has it developed, and places it on the market or puts it into service under its own name or trademark.

**Deployer.** A person or body that uses an AI system under its authority, except for personal non-professional use.

**Prohibited practice.** An AI use banned by Article 5, such as social scoring or emotion recognition in the workplace. These bans have applied since 2 February 2025 ([implementation timeline](#)).

**High-risk AI system.** An AI system in an Annex III area, such as recruitment or credit scoring, or a safety component of a product under Annex I. Annex III duties apply from 2 December 2027. Annex I duties apply from 2 August 2028 ([Article 113](#)).

**General-purpose AI (GPAI) model.** A model that can serve many tasks, such as a large language model. GPAI rules have applied since 2 August 2025.

**AI literacy.** The skills and knowledge to deploy AI in an informed way and to understand its risks. Providers and deployers must take measures to support it ([Article 4](#)).

**Deepfake.** AI-generated or manipulated image, audio or video that resembles real people, objects or events and would falsely appear authentic. It must be disclosed ([Article 50](#)).

**Digital Omnibus on AI.** Regulation (EU) 2026/1744 of 8 July 2026. It amends the AI Act, moves the high-risk dates and adds new prohibitions. It entered into force on 27 July 2026 ([artificialintelligenceact.eu](#)).

**Small mid-cap (SMC).** A new category from the Omnibus. It covers companies that are not SMEs, employ fewer than 750 people, and have turnover of no more than EUR 150 million or a balance sheet of no more than EUR 129 million ([Orrick](#)). For SMCs, the lower fine cap applies for most breaches ([Article 99](#)).

## Standards and frameworks

**AI management system (AIMS).** A set of policies, objectives and processes for the responsible development, provision or use of AI systems. ISO/IEC 42001 specifies the requirements ([ISO](#)).

**ISO/IEC 42001.** The international standard for AI management systems, published in December 2023. It uses the Plan-Do-Check-Act method.

**NIST AI RMF.** The NIST AI Risk Management Framework, released on 26 January 2023, for voluntary use ([NIST](#)).

**Govern, map, measure, manage.** The four functions of the NIST AI RMF Core. Govern is cross-cutting and informs the other three ([NIST AIRC](#)).

**Trustworthy AI characteristics.** In the NIST AI RMF: valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed ([NIST AIRC](#)).

## US rules

**Model risk management (MRM).** Bank practice to control the risk of using models. SR 26-2 replaced SR 11-7 on 17 April 2026. It excludes generative AI and agentic AI from scope ([OCC Bulletin 2026-13](#)).

**Model (in MRM).** In SR 26-2, a complex quantitative method that applies statistical, economic or financial theories to turn input data into quantitative estimates. Simple spreadsheet math and rule-based software are excluded.

**Automated employment decision tool (AEDT).** A tool covered by New York City Local Law 144. An employer may use one only after a bias audit within one year of use, with the audit published and notices given ([NYC DCWP](#)).

**Bias audit.** A review of whether a tool's results differ unfairly between groups of people. New York City requires one for each AEDT.

**Automated decision-making technology (ADMT).** The core term of Colorado SB26-189. It is technology that processes personal data and computes output used to make or assist a decision about a person ([Colorado General Assembly](#)).

**Consequential decision.** In SB26-189, a decision about a person's access to education, employment, housing, lending, insurance, health care and similar services.

## LLM and security terms

**Guardrail.** A control that screens AI inputs or outputs at run time and blocks, edits or flags them.

**Red teaming.** Testing an AI system by attacking it, to find failures before others do.

**Prompt injection.** Input that changes an LLM's behavior against the developer's intent. It is LLM01 in the [OWASP Top 10 for LLM Applications 2025](#).

**Excessive agency.** An LLM agent that has more tools or permissions than its task needs. OWASP LLM06.

**System prompt leakage.** Exposure of the hidden instructions given to an LLM. OWASP LLM07.

**Misinformation.** False or misleading LLM output that people rely on. OWASP LLM09.

**Evaluation (eval).** A repeatable test that scores model output against a standard.

**Observability.** Tracing and logging what an AI system does in production, including prompts, responses and tool calls.

**Drift.** A change over time in input data or model behavior that can lower quality.

**AI inventory.** A register of every AI system an organization builds or uses, with owner, purpose and risk tier.

See [how to choose an AI governance platform](#) for how these parts fit together.

## Sources

- [Article 4](#), [Article 26](#), [Article 50](#), [Article 99](#), [Article 113](#), [artificialintelligenceact.eu](#), accessed 2026-10-29
- [Implementation Timeline](#), [artificialintelligenceact.eu](#), accessed 2026-10-29
- [Digital Omnibus on AI](#), [artificialintelligenceact.eu](#), accessed 2026-10-29
- [EU AI Act Update: Digital Omnibus Finalizes 8 Compliance Changes](#), Orrick, 29 July 2026, accessed 2026-10-29
- [ISO/IEC 42001:2023](#), International Organization for Standardization, accessed 2026-10-29
- [AI Risk Management Framework](#), NIST, accessed 2026-10-29
- [AI RMF Core](#) and [trustworthiness characteristics](#), NIST Trustworthy and Responsible AI Resource Center, accessed 2026-10-29
- [OCC Bulletin 2026-13](#), Office of the Comptroller of the Currency, accessed 2026-10-29
- [Automated Employment Decision Tools \(AEDT\)](#), NYC Department of Consumer and Worker Protection, accessed 2026-10-29
- [SB26-189 Automated Decision-Making Technology](#), Colorado General Assembly, accessed 2026-10-29
- [OWASP Top 10 for LLM Applications 2025](#), OWASP GenAI Security Project, accessed 2026-10-29

## Frequently asked questions

### What is the difference between a provider and a deployer?

Under the EU AI Act, a provider develops an AI system or has it developed and places it on the market under its own name. A deployer uses an AI system under its authority in a professional capacity. Most buyers are deployers.

### What is the difference between AI governance and AI security?

AI governance decides who may build and use AI, for what, and with which controls and records. AI security protects AI systems from attack and misuse. Governance programs include security checks, but they are wider.