PAN · SENIOR AI ADVISOR

EU AI Act Readiness Checklist

Do you actually know if your company is compliant with the August 2, 2026 deadline? Thirty questions, fifteen minutes.

Angelo Pallanca · pallanca.info

April 2026

Do you actually know if your company is compliant? Thirty questions, fifteen minutes.

Why this matters. Why now.

On **August 2, 2026**, the obligations of EU Regulation 2024/1689 ("EU AI Act") on **high-risk AI systems** (Annex III) come into effect. Maximum penalty for non-compliance: **€35 million or 7% of global annual turnover**, whichever is higher.

The problem isn't the regulation itself. The problem is that more than half of European companies don't have a systematic inventory of their AI systems in production. Not from negligence. Because AI has spread capillary in the past two years, inside HR applications, inside CRMs, inside marketing tools, inside credit scoring processes, and no one has ever mapped it.

Even before fines, an audit request from the regulator or the data protection authority can shut down a production system. The European regulator will use the first two years as "example years": the cases that hit the press will define jurisprudence. You don't want to be one of the example cases.

> **Who should read this document.** General Counsel, Chief Information Officer, Chief Risk Officer, Compliance Officer at EU companies with AI systems in production in regulated sectors: banking, insurance, healthcare, HR tech, edtech, scoring, access control, education.

How to use the checklist

- **Thirty questions** in **six thematic sections**.
- For each question: answer **Yes** / **No** / **I don't know**.
- **Scoring**: each "No" or "I don't know" adds 1 point to your gap score.
- At the end, sum the points across sections and read the interpretation on the final page.
- **Estimated time**: 12-18 minutes if you answer honestly. The questions require that you know what's happening in your systems, not that you're a legal expert.
- Best filled in jointly with your CIO, DPO, and a Legal representative.

Section 1 — AI system identification & inventory

Reference: Art. 3, Art. 25 (provider chain)

1. Do you have a **formal inventory** of AI systems used or developed by your company, updated within the last six months?

2. Have you mapped AI systems **inside third-party suppliers** (HR tech, CRM, marketing automation, identity providers, fraud detection)?

3. Can you distinguish **high-risk AI systems** from others according to Annex III criteria (8 areas: biometrics, critical infrastructure, education, employment, essential services, law enforcement, migration, justice & democracy)?

4. Have you identified your role for each system under the AI Act: **provider**, **deployer**, **importer**, **distributor**?

5. Do you have a **formal process** to update the inventory when an AI system is introduced, substantially modified, or decommissioned?

Section 2 — Risk classification

Reference: Art. 5 (prohibited), Art. 6 (high-risk), Annex III

6. Have you **classified every AI system** into the four Regulation categories: **prohibited**, **high-risk**, **limited risk**, **minimal risk**?

7. For each high-risk system, have you documented the **specific use case** under the relevant Annex III item?

8. Have you verified that none of your systems falls under the **prohibited practices** in Article 5 (subliminal manipulation, general social scoring, emotion recognition in workplaces, etc.)?

9. Do you have a **periodic review process** for the classification (at least yearly or upon use case change)?

10. Do you understand the difference between a **General-Purpose AI Model (GPAI)** and a **High-risk AI System** under Article 51 onwards, and which set of obligations applies?

Section 3 — Conformity & technical documentation

Reference: Art. 8-15, Annex IV

11. For each high-risk system, do you have a **documented risk management system** (Art. 9): identification, estimation, evaluation, mitigation of risks?

12. Do you have a **data governance policy** specific to training, validation, and test datasets used in high-risk systems (Art. 10)?

13. Do you have **complete technical documentation** per Annex IV for each high-risk system (architecture, purpose, hardware, training data, performance metrics, validation, etc.)?

14. Do you have **automated record-keeping (logging)** active on high-risk systems, with a retention policy that allows traceability of major events (Art. 12)?

15. Do you have a defined **conformity assessment procedure** (internal via Annex VI or via notified body via Annex VII) for high-risk systems?

Section 4 — Transparency & disclosure

Reference: Art. 13, Art. 50, Art. 52

16. For systems that **interact with natural persons** (chatbots, assistants, agents), have you clearly informed users they are interacting with AI (Art. 50)?

17. For **AI-generated or manipulated content** (text, image, audio, video, deepfake), do you have a **marking, watermarking, or disclosure** system (Art. 50.2)?

18. For each high-risk system, do you have **instructions for use** clearly written for the deployer, meeting Article 13 requirements?

19. Have you published (where required for your provider category) the necessary information on the **EU register of high-risk AI systems** (Art. 71)?

20. Do you have a **process to handle transparency requests** from data subjects or their representatives, coordinated with your GDPR compliance?

Section 5 — Human oversight, accuracy & robustness

Reference: Art. 14, Art. 15, Art. 73

21. For each high-risk system, have you defined **specific human interventions** (kill switch, override, opt-out) accessible to people with real authority?

22. Do the people designated for **human oversight** have adequate training on the system's limitations and formal authority to intervene?

23. Do you have **accuracy, robustness, and cybersecurity** tested and documented to relevant metrics for high-risk systems (Art. 15)?

24. Do you have an active **post-market monitoring system** to detect malfunctions, performance drift, anomalous cases (Art. 72)?

25. Do you have a **serious incident reporting system** (Art. 73): processes, roles, timelines (15 days standard, 2 days for critical cases), connection with national competent authorities?

Section 6 — Internal governance & organizational compliance

Reference: Art. 4, Art. 26, Art. 27 (FRIA)

26. Do you have a designated **AI compliance officer**, or a formally constituted AI Act committee with clear responsibilities?

27. Do all employees who design or use AI systems have **AI literacy training** appropriate to their role (Art. 4, in force since February 2, 2025)?

28. Have you **revised supplier contracts** to include AI Act clauses (liability, access to documentation, audit support, indemnification)?

29. Do you have a **dedicated budget** and a **compliance roadmap** with milestones up to August 2, 2026, approved by the board or equivalent management?

30. For high-risk systems in regulated sectors, have you completed (or planned) the **Fundamental Rights Impact Assessment (FRIA)** required by Article 27?

Interpret your gap score

Sum all “No” + “I don’t know” answers across the six sections. Find your score in the table.

SCORE	STATUS	INTERPRETATION
0–3	Mature	You’re ahead of most EU companies. A targeted audit will likely close the last formal gaps and produce final documentation. Estimated time to be ready by August 2: 3–4 weeks.
4–10	Partially ready	You’re in “compliance achievable by deadline with focused effort” territory. Gaps are likely concentrated in 1-2 specific sections (often Section 3 and Section 5). Audit + remediation, 8-10 weeks.
11–20	Significant gap	Real risk of missing the deadline. Remediation must start now, not in July. AI system inventory in 2 weeks, gap analysis in another 3, remediation in 8-10 weeks. Time is almost up.
21–30	Critical	Compliance for August 2, 2026 is doubtful with internal resources only. Two decisions needed: (a) immediate investment in advisor + remediation (order of magnitude €50-150k between fees, tools, internal hours), or (b) formal acceptance of regulatory risk for the most exposed systems, documented by the board. There is no third option.

What to do now, depending on your level

If you’re mature (0-3)

Focus on three things: **continuous monitoring** (a quarterly AI status report to the board), **completing documentation** (Annex IV for each system), and **active post-market vigilance**. You probably don’t need external consulting: you need internal discipline.

If you’re partially ready (4-10)

Identify the 2-3 sections where you have most “No” answers. Typically these are Section 3 (technical documentation) and Section 5 (human oversight & robustness). Plan a 3-week audit in April-May 2026 to close formal gaps, then 8 weeks of internal remediation. Without external help, it’s feasible if you have a competent PMO.

If you’re significant gap (11-20)

Engage an advisor by May 2026. The sequence: complete AI system inventory (2 weeks), per-system gap analysis (3 weeks), action plan with prioritization and budget (1 week), then remediation (8-10 weeks). Without an external advisor it’s realistically too late.

If you’re critical (21-30)

You need a board-level decision in your next board meeting. Three scenarios to evaluate with CFO and Legal: immediate investment to attempt closing by August, scope-down (disable highest-risk systems, accept loss of functionality, return to compliance), or documented acceptance of risk (requires advisor anyway to minimize exposure and prepare defense in case of regulator request).

AI Act glossary (12 key terms)

Provider — entity that develops or has developed an AI system, places it on the market or puts it into service under its own name or trademark. (Art. 3)

Deployer — entity using an AI system under its authority in the course of professional activity (excluding personal non-professional use). (Art. 3)

Annex III — list of eight domains where AI systems are classified high-risk: biometrics, critical infrastructure, education, employment, essential services, law enforcement, migration, justice & democracy.

High-risk AI — AI systems falling under Article 6 criteria or listed in Annex III. Subject to the most stringent obligations of the Regulation.

Conformity assessment — procedure to demonstrate that a high-risk AI system meets the AI Act requirements. May be internal (Annex VI) or via notified body (Annex VII), depending on category.

Notified body — accredited third party authorized to conduct external conformity assessments of high-risk AI systems.

Post-market monitoring — ongoing system to collect and analyze AI system performance data after market placement, identify malfunctions, and trigger corrective actions. (Art. 72)

Substantial modification — change to a high-risk AI system that affects compliance, performance, or intended use. Triggers a new conformity assessment. (Art. 43)

General-Purpose AI Model (GPAI) — AI model trained on large amounts of data, capable of performing a wide range of tasks, integrable into many systems. Specific obligations from August 2, 2025. (Art. 51-55)

Real-time biometric identification — identification of natural persons through biometric data in real time or near-real time. Generally prohibited in public spaces, with narrow law enforcement exceptions. (Art. 5)

Regulatory sandbox — controlled environment that allows testing of innovative AI systems under regulator supervision before market placement. Mandatory in every Member State by 2026. (Art. 57)

AI literacy — skills, knowledge, and understanding that allow deployers, providers, and persons affected by AI systems to make informed use and to understand opportunities and risks. (Art. 4)

AI Act timeline 2025-2027

DATE	EVENT
August 2, 2024	Regulation entered into force
February 2, 2025	Obligations on prohibited practices (Art. 5) and AI literacy (Art. 4)
August 2, 2025	Obligations on General-Purpose AI Models (Art. 51-55), penalties (Art. 99-101), governance authorities
August 2, 2026	**Full obligations on high-risk Annex III systems** — the deadline that matters for most companies
August 2, 2027	Obligations on high-risk systems embedded in products already regulated by other EU regimes (medical devices, automotive, etc.)

About the author

Angelo Pallanca (Pan) — Senior AI advisor to European leadership teams. Thirty years cross-industry. Has worked on AI projects in production for African Central Banks (AML compliance),

Government of the Canary Islands (tourism intelligence), Principality of Monaco (AI governance in public sector), UNICEF (AI-powered distance learning). Independent, no vendor commissions.

Publishes regularly at pallanca.info/blog (editorial signature “Pan” for My 5 cents).

Found critical gaps?

If your gap score is above 10, it’s worth having a thirty-minute conversation to figure out what’s priority in your specific case. I don’t sell compliance software, I have no commissions from AI Act tool vendors, and if your company is not in AI Act scope I’ll tell you explicitly in those thirty minutes.

Request a written proposal: pallanca.info/en/proposal **Or email me:** angelo@pallanca.info