EU AI Act Risk Classification Checklist

Work through each tier in order. Classify each AI system into the highest tier that matches, and record the reasoning - the classification drives every downstream obligation.

Step 1 - Prohibited practices (Article 5)

If any apply, the system cannot be deployed in the EU. Stop and seek advice.

- Does it deploy subliminal or manipulative techniques that cause significant harm?
- Does it exploit vulnerabilities (age, disability, social situation) to cause harm?
- Is it social scoring by social/classification of persons based on behavior or characteristics?
- Does it predict criminal offense risk based solely on profiling or personality traits?
- Does it do facial-image scraping from the internet or CCTV for untargeted recognition databases?
- Does it infer emotions in workplaces or educational institutions (except medical/safety)?
- Is it biometric categorization inferring sensitive attributes (race, religion, orientation)?
- Is it real-time remote biometric identification in publicly accessible spaces (law enforcement only, with exceptions)?

Step 2 - High-risk (Article 6 + Annex I & III)

The system is high-risk if it is a safety component of a regulated product (Annex I) or used in an Annex III area:

- Biometrics: identification, categorization, emotion recognition (outside prohibited uses).
- Critical infrastructure: safety components (transport, water, gas, electricity, digital).
- Education: admissions, evaluation of learning, proctoring.
- Employment: recruitment, screening, promotion/termination decisions, task allocation, monitoring.
- Essential services: credit scoring, insurance pricing, benefits eligibility, emergency triage.
- Law enforcement, migration/asylum/border control, justice and democratic processes.
- Exception: does a purely human-review second step with real authority and discretion apply (Art. 6(3))? Record the assessment either way.

Step 3 - Limited risk / transparency obligations (Articles 50)

- Chatbots or conversational AI interacting with people: disclose that it is AI.
- Synthetic content (deepfakes, AI-generated text/images/audio published to the public): mark as artificially generated.
- Emotion recognition or biometric categorization (where lawful): inform exposed persons.
- Generative AI producing published content: machine-readable marking of outputs.

Step 4 - GPAI and general-purpose models

- Do you provide or integrate a general-purpose AI model (yours or a vendor's)?
- Systemic-risk thresholds (>10^25 FLOP): provider has extra obligations.
- Downstream deployers: pass through provider information and comply with usage terms.

Step 5 - Minimal risk (everything else)

No AI Act obligations beyond voluntary codes of practice. Keep the record anyway: risk class, date, assessor, and reasoning. Reclassification is expected as use cases evolve.

(c) Regovern.io - Free to use and adapt. More resources at https://regovern.io/resources/

Record your classification

Field	Entry
System name / ID	
Classified by / date	
Risk class	Prohibited / High / Limited / Minimal
Key reasoning	
Next reassessment	

This checklist is an educational summary, not legal advice. The classification timeline is phased (prohibitions from February 2025; GPAI from August 2025; most high-risk obligations from August 2026). Confirm current dates for your use case.

(c) Regovern.io - Free to use and adapt. More resources at https://regovern.io/resources/