High-Risk AI Systems: Criteria and Examples

Identifying regulated high-risk systems.

Co-authored with **Jessica Mendoza**, *AI Safety Advocate*

7 July 2025

---

2. Risk Classification of AI Systems — Levels, Impact, Categories, Compliance

2.1 Understanding the Risk-Based Approach	2.2 Prohibited AI Practices	2.3 High-Risk AI Systems: Criteria and Examples	2.4 Obligations for High-Risk AI Systems
AI systems grouped by risk	*AI uses completely banned*	*Identifying regulated high-risk systems.*	*Rules for high-risk system compliance*

Understanding the High-Risk Classification

Under the EU Artificial Intelligence Act, high-risk AI systems form the regulatory centerpiece. Though not outright prohibited, these systems are subject to strict legal requirements due to their significant impact on fundamental rights, health, and safety. The designation of "high-risk" rests on specific criteria rooted in the system's intended use, sector of operation, and potential consequences if it fails or functions improperly.

High-risk classification operates within a layered regulatory framework. At the top level, the Act distinguishes four risk tiers: unacceptable, high, limited, and minimal. Only systems that fall into the second tier — high-risk — are subject to the most extensive obligations without being outright banned. These systems are considered essential to regulate due to their capability to influence critical decisions and processes across public and private sectors.

Criteria for High-Risk Designation

The EU AI Act sets out a two-part test to determine whether an AI system qualifies as high-risk:

- Sectoral Relevance: The system must be used in a domain listed in Annex III of the Act. These domains are typically associated with safety-critical applications or rights-sensitive environments.
- Use Case and Impact: The system must pose a significant risk to the health, safety, or fundamental rights of individuals. This includes evaluating the scale, context, and likelihood of harm.

Only when both conditions are met is a system formally considered high-risk. This structured approach prevents overregulating low-impact tools while ensuring that consequential systems receive appropriate oversight.

Enumerated High-Risk Categories

The Act provides a list of categories where high-risk AI systems are most likely to occur. These categories form an exhaustive reference point for regulatory enforcement. Each category reflects a different facet of public interest and societal infrastructure.

Biometric Identification and Categorization

AI used for remote biometric identification, especially in real-time and in public spaces, falls under the high-risk bracket. This includes facial recognition technologies used for surveillance or access control. The primary concern is the potential intrusion into individual privacy and the disproportionate power imbalance such systems create between users and those subject to the system.

Critical Infrastructure

AI that manages or operates essential infrastructure — such as energy networks, water systems, and transportation grids — is deemed high-risk due to the cascading effects that failures in these systems can produce. Automation in traffic management, railway control, or electrical distribution must meet heightened safety and reliability standards to mitigate widespread disruption.

Education and Vocational Training

Systems used to determine access to education or influence academic outcomes are regulated as high-risk. This includes AI tools that grade exams, allocate university placements, or assess skills. Due to the influential nature of education and its long-term effects, the Act requires strict measures for accuracy and transparency.

Employment, Workers' Rights, and HR Management

AI systems currently used in recruitment, employee evaluation, promotion decisions, and productivity tracking qualify as high-risk. These applications influence individual livelihoods and often operate with limited human oversight. The potential for bias, discrimination, or opaque decision-making creates a high regulatory priority.

Access to and Enjoyment of Essential Private and Public Services

This includes AI systems used to evaluate creditworthiness, assess eligibility for social benefits, or facilitate asylum procedures. These decisions affect access to housing, education, healthcare, and financial support — core components of social welfare. Inaccurate or biased systems can lead to unjust exclusion or deprivation.

Law Enforcement and Border Control

AI applications in predictive policing, criminal risk assessments, evidence evaluation, or migration management are considered high-risk. The sensitivity of these functions, combined with the coercive power of the state, raises the stakes for fairness, accountability, and non-discrimination.

Administration of Justice and Democratic Processes

AI tools assisting in legal interpretation, court decision support, or document analysis within judicial systems fall into the high-risk category. The role of AI in shaping or interpreting legal outcomes requires extreme care to maintain judicial integrity and procedural fairness.

Conditional Classification: Flexibility and Updating

As it stands the European Commission retains the authority to update Annex III based on evolving technologies and usage patterns. A dynamic classification mechanism ensures the regulation remains relevant and effective as new applications emerge.

The Act also introduces conditional classification mechanisms that allow for the inclusion of AI systems not explicitly listed but meeting the risk thresholds outlined in the framework. For instance, if a newly developed AI application in the healthcare sector demonstrates a comparable risk profile to those in Annex III, it may be provisionally treated as high-risk.

Role of Intended Purpose and Deployment Context

A crucial element is that the classification hinges not only on the AI's function but also on how and where it is deployed. The intended purpose, as defined by the provider, establishes the baseline for evaluation. An AI system designed for general-purpose use may not initially be considered high-risk, but if it is integrated into a critical workflow, such as patient triage in emergency rooms, tts classification may change.

Contextual deployment also matters. For example, facial recognition software may not be high-risk if used to organize personal photo libraries. However, the same software used by law enforcement in public spaces would trigger high-risk obligations due to surveillance implications.

Examples of High-Risk AI in Practice

To better understand how these rules apply, consider the following real-world applications:

Automated Hiring Tools

AI that screens resumes or ranks candidates for interviews in large organizations must comply with high-risk requirements. The system must be documented, tested for bias, and monitored for ongoing fairness.

Loan Approval Algorithms

An AI model assessing individual credit risk to determine loan eligibility is high-risk. The decision impacts access to essential financial services and must be transparent, explainable, and contestable.

Medical Diagnostic Systems

Tools that assist in identifying diseases or recommending treatment pathways based on imaging or patient history fall under the high-risk bracket. These systems must be validated rigorously to ensure safety and efficacy.

Border Screening Applications

AI used to assess the likelihood of fraud in visa applications or to detect false documents is considered high-risk due to implications for individual liberty and movement.

Predictive Policing Platforms

Systems designed to forecast crime hotspots or suggest patrol areas based on historical data must adhere to high-risk standards, including bias assessment and human oversight.

Compliance Requirements for High-Risk Systems

Providers and deployers of high-risk AI systems must comply with a range of obligations before, during, and after deployment. These obligations are designed to ensure safety, fairness, and accountability.

Risk Management System

A comprehensive framework must be in place to identify, evaluate, and mitigate risks throughout the AI system's lifecycle. This includes design, development, testing, and post-market monitoring.

Data Governance and Quality

High-risk AI systems must be trained on high-quality datasets that are representative, relevant, and free from systemic bias. Clear documentation of data sources and preprocessing steps is required.

Technical Documentation and Logging

Detailed documentation must accompany the AI system, describing its design, intended use, limitations, and performance. Logging mechanisms must be implemented to track decisions and enable traceability.

Human Oversight

Appropriate human intervention mechanisms must be established to ensure that AI outputs can be monitored, overridden, or stopped in case of malfunction or unexpected behavior.

Transparency and Information Provision

Users must be clearly informed that they are interacting with an AI system and provided with meaningful explanations of how the system functions and how decisions are made.

Accuracy, Robustness, and Cybersecurity

The system must achieve a defined level of accuracy and be resilient against manipulation or failure. Providers are responsible for ensuring cybersecurity protections are embedded in system architecture.

Post-Market Monitoring and Reporting

Providers must monitor the system's real-world performance and report any serious incidents or malfunctions to the relevant authorities. This includes establishing feedback channels and maintaining continuous risk assessment.

Exemptions and Special Considerations

Not all deployments of AI in high-risk areas are automatically regulated. The Act allows for limited exemptions, particularly in the context of research, national security, or temporary emergency use. For instance, a law enforcement agency may deploy a high-risk system under urgent conditions but must comply with post-hoc transparency and reporting requirements.

There are also provisions for SMEs and startups to ensure that innovation is not stifled. These include reduced administrative burdens, regulatory sandboxes, and technical support for compliance without compromising safety or rights protections.

Alignment with Broader Regulatory Goals

High-risk classification is aligned with the EU's broader digital strategy, which emphasizes trustworthy, human-centric AI. It complements existing legislation such as the GDPR, Product Safety Regulation, and Medical Device Regulation. The intent is to create a coherent regulatory ecosystem where AI innovation and fundamental rights co-exist.

Moreover, the EU's international trade partners are watching closely. The clarity and structure of the high-risk classification serve as a potential blueprint for global regulatory convergence, especially in sectors like finance, healthcare, and public administration.

Conclusion

High-risk AI systems under the EU AI Act represent the focal point of regulation, balancing innovation with accountability. Through a structured classification system, clear obligations, and adaptive governance, the Act seeks to ensure that the most consequential AI applications are developed and deployed responsibly. The criteria are specific, the examples are instructive, and the compliance pathways are well-defined — offering legal certainty while safeguarding public interest.

As AI continues to evolve, the high-risk framework provides a durable foundation for oversight, rooted in principles of transparency, fairness, and human oversight. It ensures that trust remains at the core of the EU's AI vision, both now and in the future.

Glossary

Act or EU AI Act: European Union Artificial Intelligence Act

AI: Artificial Intelligence

Board: European Union Artificial Intelligence Board

EU: European Union

SME: Small and Medium-Sized Enterprise

How can we help?

AI & Partners
Amsterdam - London - Singapore

AI & Partners – 'AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.