Obligations for High-Risk AI Systems

Rules for high-risk system compliance

Co-authored with Enzo di Taranto Capozzi, *Global Sustainability Stategist*

14 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*

Introduction to Compliance Obligations

The EU AI Act imposes a set of detailed compliance obligations on providers, deployers, and other actors involved in the lifecycle of high-risk AI systems. These obligations are designed to ensure that AI systems operating in sensitive contexts function safely, respect fundamental rights, and remain under meaningful human oversight. Unlike general-purpose AI tools or minimal-risk applications, high-risk systems are legally accountable through a framework of technical, procedural, and operational requirements.

These rules are not optional or advisory. Compliance is mandatory before such systems can be placed on the EU market or used within its territory. The obligations apply throughout the system's lifecycle—from development and testing to deployment and post-market monitoring—forming a continuous compliance environment.

Overview of Responsible Actors

Several parties are subject to specific legal duties under the Act. The key actors include:

- Providers: Organizations that develop or place the AI system on the market.
- Deployers: Entities that use the AI system within their operations.
- Importers and Distributors: Entities that introduce or supply systems developed outside the EU.
- Authorized Representatives: EU-based legal representatives of non-EU providers.

Each actor has distinct roles and responsibilities, although the provider carries the primary burden of ensuring the system meets regulatory standards before deployment.

Mandatory Risk Management System

All high-risk AI systems must be supported by a formal risk management system. This system must identify foreseeable risks, evaluate their severity and likelihood, and implement mitigation measures accordingly. Risk assessments must cover the entire lifecycle of the system, including design choices, data use, interaction with users, and possible misuse.

The risk management framework must be iterative, meaning it should evolve with new information obtained during deployment and real-world use. It must also be documented and available for inspection by competent authorities.

Data Quality and Governance

High-risk systems must be trained, validated, and tested using datasets that are relevant, representative, and statistically appropriate. This requirement ensures that the system's performance is reliable across various subgroups and use conditions.

Data governance obligations include:

- Clear documentation of data sources
- Assessment of potential biases
- Preprocessing methods to improve balance or completeness
- Measures to ensure integrity and security of data throughout its use

These standards are particularly important for applications involving people, such as employment screening, loan approvals, or educational assessment.

Technical Documentation and Record-Keeping

Comprehensive documentation must accompany every high-risk AI system. This includes a description of the system's architecture, functionality, intended purpose, training methodology, risk controls, and limitations.

Key aspects include:

- The system's design specifications
- Instructions for use

- Evaluation results and performance metrics
- Testing procedures and outcomes

The documentation must be sufficiently detailed to enable authorities to assess compliance. Providers must also implement **automatic logging** capabilities that record system decisions, inputs, and outputs to ensure auditability and traceability during operation.

Transparency and User Information

Transparency is central to high-risk AI governance. Providers must ensure that users understand:

- That they are interacting with an AI system
- The system's intended purpose and capabilities
- How to operate it safely
- The limitations and potential outcomes of system use

Instructions for use must be clear, complete, and easily accessible. Where appropriate, users should also receive information on how to interpret the system's results and how to intervene in its operation if needed.

This obligation helps mitigate risks associated with overreliance on automated outputs and supports accountability in decision-making processes.

Human Oversight Measures

High-risk AI systems must be designed to allow **effective human oversight**. The goal is to ensure that human operators can:

- Understand the system's functioning
- Detect anomalies or errors
- Override or halt the system when necessary
- Prevent or minimize harm in real time

Oversight mechanisms vary based on the system's complexity and use case. In some contexts, a human may review individual decisions. In others, oversight may occur through periodic audits or alerts triggered by unusual system behavior.

Human oversight is not a formality; it must be meaningful and built into the system's design. This ensures that final control remains with humans, particularly when systems affect rights, safety, or dignity.

Accuracy, Robustness, and Cybersecurity

Technical performance standards are a cornerstone of high-risk AI compliance. Systems must achieve an appropriate level of accuracy, which is context-specific and defined during the system's design phase.

In addition to accuracy, systems must demonstrate:

- **Robustness**: The ability to handle errors, disruptions, and unexpected inputs without failure.

- **Resilience**: Ongoing stability during operation under different conditions.
- **Cybersecurity**: Protection against unauthorized access, data breaches, or manipulation that could impair performance or safety.

Providers must conduct thorough testing and validation to prove these qualities before placing the system on the market. They must also ensure that the system continues to meet these benchmarks during its use.

Conformity Assessment Procedures

Before deployment, high-risk systems must undergo a **conformity assessment** to verify that they meet all legal requirements. The assessment process depends on the nature of the AI system and the applicable harmonized standards.

There are two main models:

1. **Internal Control**
   The provider conducts a self-assessment using applicable standards. This path is only available for certain systems, typically those not related to safety-critical domains.
2. **Third-Party Evaluation**
   In most cases, especially where risks are higher, an independent **notified body** must evaluate the system. This includes reviewing technical documentation, testing processes, and design specifications.

Successful assessments result in a **CE marking**, which signifies regulatory compliance and authorizes market entry in the EU. However, the CE mark is not permanent—it may be revoked if post-market obligations are violated or new risks are identified.

Post-Market Monitoring and Reporting

Compliance does not end after deployment. Providers must establish a **post-market monitoring system** to detect performance issues, emerging risks, or unintended consequences. This includes:

- Gathering user feedback
- Analyzing system performance logs
- Reviewing real-world outcomes
- Initiating updates or patches as needed

Serious incidents—such as malfunctions leading to harm or systemic bias—must be reported to competent national authorities within a defined timeframe. Providers must also cooperate with investigations and make system data available upon request.

Deployers are expected to monitor system behavior within their organization and report anomalies or failures through the appropriate channels.

Obligations for Deployers and Other Parties

While providers carry most of the technical compliance duties, **deployers** have their own set of responsibilities:

- Use the system in accordance with its intended purpose
- Maintain records of system use
- Enable and apply human oversight measures
- Ensure relevant staff are trained to use the system safely

Importers and distributors must verify that systems they place on the EU market have undergone the necessary assessments and bear the CE marking. They must also cooperate with market surveillance authorities and withdraw non-compliant systems if issues arise.

Authorized representatives, appointed by non-EU providers, act as a legal contact point within the EU and may be held accountable for compliance failures.

Support Mechanisms and Exceptions

To support compliance, the Act introduces several mechanisms, especially for small and medium enterprises:

- Regulatory Sandboxes: Controlled environments for testing AI systems under regulatory supervision
- Guidance and Templates: Standardized documentation to help actors meet obligations
- Technical Assistance: Access to expert resources through national authorities or EU bodies

In limited cases, certain systems may be temporarily exempt from obligations, such as during public emergencies or for research purposes. However, these exemptions are narrow, time-bound, and often require separate authorization or notification.

Enforcement and Penalties

Failure to meet high-risk system obligations carries significant legal consequences. Enforcement actions can include:

- Fines based on annual global turnover
- Suspension or withdrawal of CE certification
- Market withdrawal or recalls
- Public disclosure of non-compliance

Supervisory authorities in each Member State are responsible for monitoring compliance and coordinating enforcement. Cross-border issues are managed through the European Artificial Intelligence Board, ensuring consistency across the EU.

Conclusion

The EU AI Act establishes a comprehensive and enforceable set of obligations for high-risk AI systems. These obligations serve a dual purpose: they safeguard users and affected individuals while creating clear standards for responsible innovation.

From risk management and data governance to human oversight and technical robustness, each requirement is calibrated to the system's potential impact. The compliance process is rigorous but structured, offering predictability for developers and accountability for users.

As AI systems become more integrated into critical services and decision-making processes, the rules governing high-risk applications will define the ethical and legal boundaries of technological advancement. By setting high expectations for safety, transparency, and trust, the EU positions itself at the forefront of global AI regulation.

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.