Radar *AI Risk*™

The EU AI Act
A Comprehensive Overview for Risk Management

Automate AI risk assessment with Radar AI Risk™.

The EU AI Act is the European Union's flagship artificial intelligence regulation. This regulation impacts organizations developing or using AI, both inside and outside the EU. The EU AI Act adopts a risk-based approach, establishing requirements and expectations for specific uses of AI to protect privacy rights and promote the EU as a leader in AI development and governance.

The EU AI Act affects organizations that develop, distribute, and deploy AI systems within the EU market. This includes:
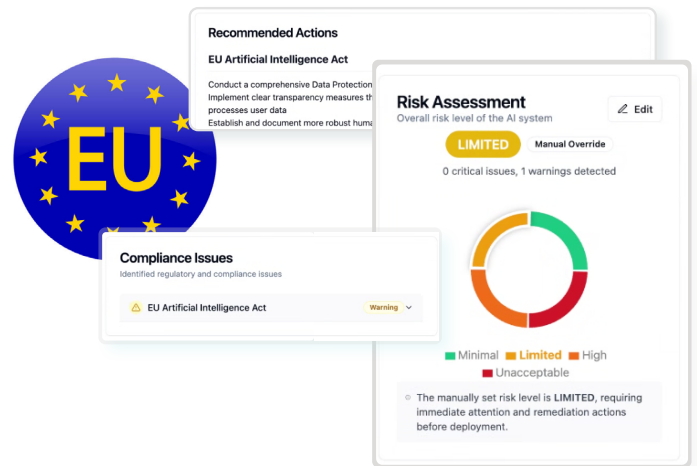
- **Providers:** Those who develop or have an AI system or model developed and place it on the EU market.

- **Deployers:** Users of AI systems.

- **Importers:** Those who place an AI system on the EU market.

- **Distributors:** Anyone who makes an AI system available on the EU market (that is not a provider or an importer).

Any organization placing its product or model on the EU market falls within the scope of this regulation, regardless of its location. This is referred to as "extraterritorial influence."

Risk Assessment and Reporting Obligations

The EU AI Act categorizes AI systems into four risk levels:

- **Unacceptable Risk:** AI systems that pose a clear threat to safety, livelihoods, and rights of people. These systems are prohibited effective February 1, 2025.

- **High Risk:** AI systems used in critical infrastructure, education, employment, law enforcement, and other sensitive areas are considered high risk and subject to stringent rules. Providers of high-risk AI systems (HRAIS) have extensive obligations, including:

  - Implementing risk management systems.
  - Adhering to data governance measures.
  - Maintaining technical documentation.
  - Ensuring record-keeping and transparency.
  - Providing for human oversight.
  - Ensuring accuracy, robustness, and cybersecurity.
  - Establishing quality management systems.
  - Monitoring post-market performance.

- **Limited Risk:** AI systems with specific transparency obligations, such as chatbots and virtual assistants.

- **Minimal or No Risk:** AI systems with minimal obligations, such as AI-enabled spam filters and video games.

General Purpose AI (GPAI)

Providers of GPAI models face transparency obligations, including maintaining technical documentation and providing information to those integrating the models into

their AI systems. GPAI models that pose systemic risks have additional requirements, such as:

- Stringent model evaluations
- Mitigating possible systemic risks
- Greater reporting obligations
- Ensuring adequate cybersecurity
- Reporting on energy efficiency

AI Systems Risk Classification with Radar AI Risk

As a trusted leader in risk management specializing in the automation of risk classification for AI systems, Radar AI Risk plays a crucial role in helping organizations navigate the complexities of the EU AI Act. The Act's risk-based approach requires organizations to thoroughly assess and manage the risks associated with their AI systems.

RadarFirst's expertise in risk assessment and reporting aligns perfectly with the needs of organizations seeking to comply with this regulation. By leveraging Radar AI Risk, companies can efficiently identify, evaluate, and mitigate risks associated with AI systems, ensuring adherence to the EU AI Act's requirements as well as other AI governance and reporting frameworks.

Scenario: Incident Response Collaboration for Third-Party AI Threat

Consider a scenario where a financial institution uses an AI-powered fraud detection system provided by a third-party vendor. The AI system identifies a high number of false positives, leading to customer dissatisfaction and potential financial losses. The incident response team must collaborate to assess and resolve the threat.

First, the data privacy team assessed whether the AI's false positives were causing unnecessary data processing or any breaches of customer privacy. They wanted

to ensure that everything was handled according to the highest standards. The compliance team also got involved, evaluating the AI system's adherence to the EU AI Act, particularly focusing on accuracy, transparency, and human oversight. Meanwhile, the cybersecurity team investigated whether the AI system had been compromised or if it was exhibiting anomalous behavior due to a cyberattack. They needed to rule out any security issues to ensure the system was safe.

To get a comprehensive view of the risks, the teams used Radar AI Risk to automate the risk assessment process. This tool helped them consider and document all relevant factors, including financial, reputational, and regulatory impacts.

The organization then engaged with the third-party vendor to address the AI system's issues and implement the necessary fixes. Collaboration with the vendor was crucial to getting things back on track, and Radar AI Risk supported this process by offering a documented assessment of the situation.

Conclusion

The EU AI Act introduces a complex regulatory landscape for organizations utilizing AI systems. Radar AI Risk offers valuable solutions for automating risk classification, ensuring compliance, and mitigating potential penalties. By partnering with RadarFirst, organizations can confidently navigate the EU AI Act and leverage AI technologies responsibly and ethically.

See how scalable AI governance works—schedule your Radar AI Risk demo today.

I'm ready to see more >

RadarFirst

Learn more at radarfirst.com