As AI gains human traits, will it gain human trust?

An overview of the EU AI Act and its impact on the markets

The better the question. The better the answer. The better the world works.

Shape the future with confidence

The AI Act

After reaching a political agreement in the end of 2023, the EU Parliament finally passed the AI Act on 13 March 2024. This important milestone in the field of AI will place the EU at the frontier of AI regulation for the coming years. The AI Act entered into force on 1 August 2024, and will be fully applicable by 1 August 2026.

Rules on prohibited AI and AI literacy will take effect by 1 February 2025, while the ones on general purpose AI (GPAI) will be enforced 1 August 2025. The AI Act aims to harmonize rules for the development, market placement, use and adoption of AI, while addressing the risks posed by the technology. The AI Act also promotes the uptake of human centric and trustworthy AI, while ensuring the protection of privacy, health, safety and fundamental rights.

Thus, the AI Act proposes a risk categorization and is intended to be a key step in the EU's approach to dealing with the perceived societal, security and ethical challenges posed by some applications of AI systems.

Who will be affected?

- Operators* of AI systems located in the EU
- Operators of AI systems located outside the EU if they operate AI systems in the EU or the output produced by the AI systems is used in the EU
- Providers placing on the market or putting into service AI systems outside the EU where the provider or distributor of such systems is located within the EU

"

Success in creating AI would be the biggest event in human history. It might also be the last, unless we learn how to avoid the risks.

Stephen Hawking

*Operator is an umbrella term for provider, deployer, authorized representative, importer and distributor.

Enforcement

The AI Act lays down a strict liability regime so compliance with the AI Act is essential as enforcement can lead to significant fines. In this context, the AI Act operates on the notion of three levels. Depending on the violation, the Act sets the following upper limits for fines:

Non-compliance case	Proposed fine
Use of high-risk AI systems without solid data governance or violation of transparency requirements	Fines up to €15 million or 3% of turnover, whichever is higher
Non-compliance with the prohibition of the AI practices	Fines up to €35 million or 7% of turnover, whichever is higher
Other violations of the AI Act, e.g., misleading information to the public	Fines up to €7.5 million or 1% of turnover, whichever is higher

Roles under the AI Act

Provider — A natural or legal person, public authority, agency or other body that develops an AI system or a GPAI model or that has an AI system or a GPAI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge.

Deployer — Any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

Importer — Any natural or legal person located or established in the EU that places on the market an AI system that bears the name or trademark of a natural or legal person established outside the Union.

Distributor — Any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market.

The risk classification: A three-tier model

The AI Act applies a risk-based approach to consider and remediate the potential negative impact of AI systems on fundamental rights and user safety. The approach entails different requirements per the three tiers:

Unacceptable risk

Systems with an unacceptable risk rating are prohibited by the European Commission:

- AI systems that deploy subliminal techniques beyond a person's consciousness in order to materially influence one's behavior or opinions.
- AI systems that exploit vulnerabilities of a specific group of persons, such as age, disabilities or specific economic or social situation.
- AI systems used for the evaluation or classification of natural persons based on their social behavior or personality characteristics.
- The use of "real-time" remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement (still to be confirmed).

High-risk

Systems with a high-risk rating must comply with multiple requirements and undergo a conformity assessment:

- AI systems according to Annex I:
  - Automotive
  - Machinery ((EU) 2023/1230)
  - Medical devices ((EU) 2017/745)
- AI systems (according to Annex III) used for:
  - Biometric identification and categorization of natural persons.
  - Management and operation of critical infrastructure.
  - Education and vocational training.
  - Employment, workers management and access to self-employment.
  - Law enforcement.

Limited risk

Certain AI systems which do not meet the specified criteria for the other two tiers and still present limited risk are recommended to apply the same practices as high-risk AI systems and are subject to transparency obligations (which shall be clearly communicated at the latest at the time of first interaction or exposure):

- Users must be informed that they are interacting with an AI system unless this is obvious from the circumstances.
- Users must be informed when biometric categorization and emotion recognition systems are used unless they are permitted by law to detect, prevent and investigate criminal offences.
- Content that has been artificially generated or manipulated to generate deep fakes must be disclosed.

Requirements for high-risk AI systems

Deployment of an appropriate risk management system

An appropriate risk management system shall be established, implemented, documented and maintained. In addition, an established continuous iterative process must run throughout the entire lifecycle of the AI systems.

Accuracy, robustness and cyber security

High-risk AI systems shall be developed to consistently perform at an appropriate (i.e., relevant, representative, free of errors and complete) level of accuracy, robustness and cyber security, in line with each AI system's specific purpose. These must be clearly documented in the system's instructions of use.

Comprehensive instructions for use

To ensure AI systems are clear for natural persons, they shall be accompanied by instructions for use that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users (i.e., the system's intended purpose, performance and any circumstances that may lead to risks to the health and safety or to fundamental rights).

Logging and human oversight

AI systems must be designed and developed to enable the automatic recording of events, ensuring traceability of the systems throughout their entire lifecycle. Also, AI systems shall be designed and developed in such a way to enable natural persons to effectively oversee their use.

Data governance

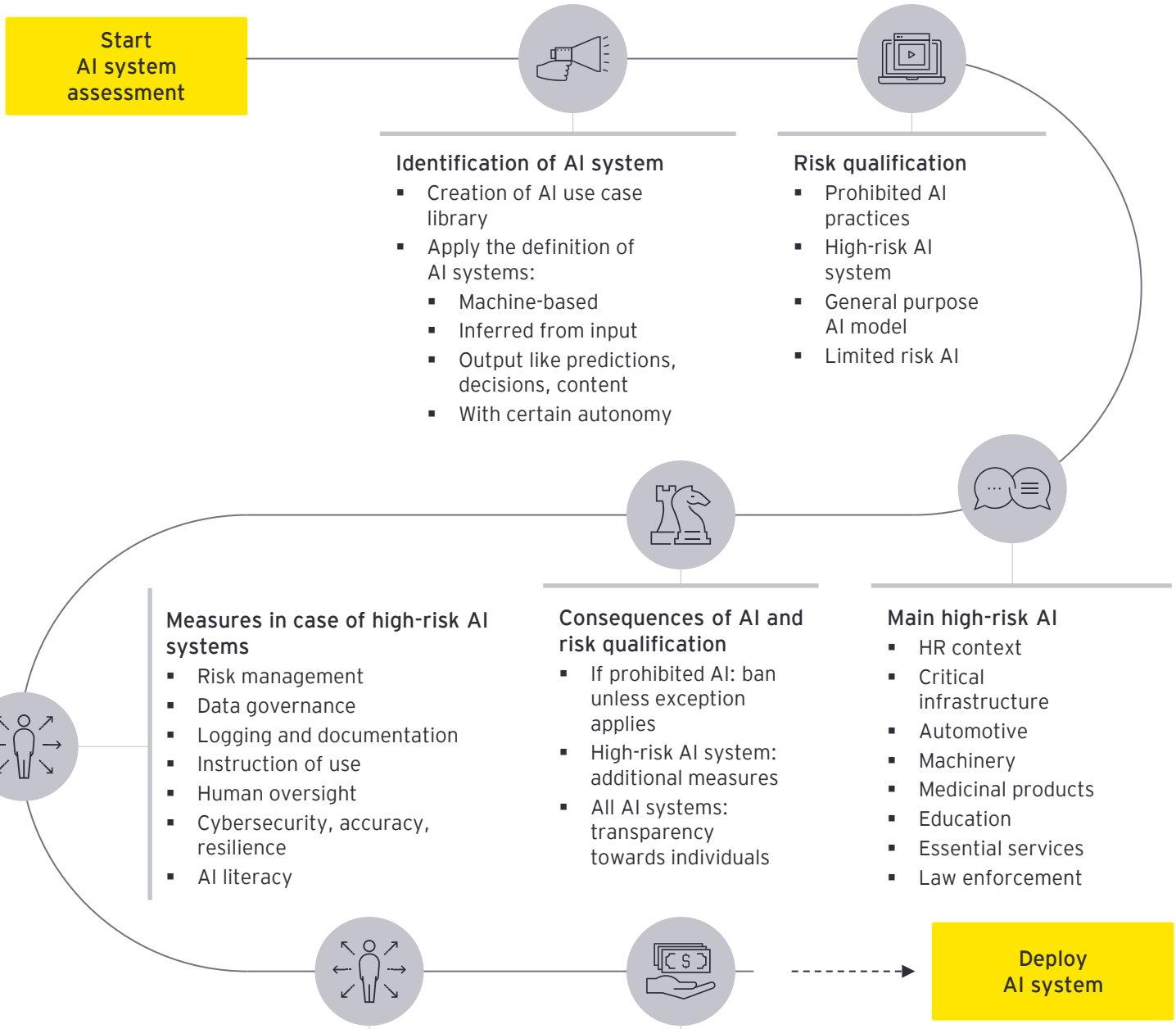
Training, validation and testing datasets must be subject to appropriate data governance and management practices, including relevant design choices, data collection, data preprocessing, formulation of assumptions, prior assessment of availability and statement of biases and shortcomings.

Transparency

The AI Act mandates certain transparency obligations for providers and deployers of specific AI systems and GPAI models. This includes disclosure obligations for providers if an AI system is intended to interact with a natural person. Extended transparency obligations apply for providers of systems generating synthetic content as well as deployers of emotion recognition or biometric systems.

Roadmap for assessments of AI systems

The AI Act requires accountability and quality management. For the underlying implementation and operationalization, organizations must define processes, procedures and responsibilities. Therefore, we recommend the following **steps to legally assess and deploy AI systems** within the regulatory framework of the AI Act. Further implementation **must establish processes to help ensure the below requirements** including the underlying measures.



What can you start doing now?

It is often more costly and complex to ensure compliance once AI systems are operating and in use than during the initial design phase. Here are some practical steps you can start implementing now:

- **Establish formal governance**
  Establish an AI ethics committee with experienced professionals to decide on challenging AI ethics disputes.
- **Assess your risks including other areas of law**
  Also consider data privacy, IP, trade secret, sector regulations and product liability laws.
- **Assign responsibility and accountabilities**
  Determine and enforce roles and responsibilities for the entire AI lifecycle and associated requirements.
- **Design ethical systems**
  Promote a sustainable and ethical use of AI incorporating it in your organizational strategy.
- **Raise awareness**
  Disseminate information and train your people with regards to the benefits and risks brought by AI.
- **Stay up to date and maintain a good documenting discipline**
  Stay tuned to new regulatory developments to anticipate their impact on your organization and ensure timely compliance. Further, invest in an appropriate tool environment to document the AI lifecycle.
- **Maintain database of AI applications**
  Maintain a comprehensive database of AI applications used by your organization including the ones provided by external suppliers -- e.g., to be vigilant for shadow AI.
- **Start preparing now**
  Start designing and implementing strategic improvements to your AI lifecycle in order to decrease complexity and implementation costs.

How EY teams can support you in preparing for the AI Act

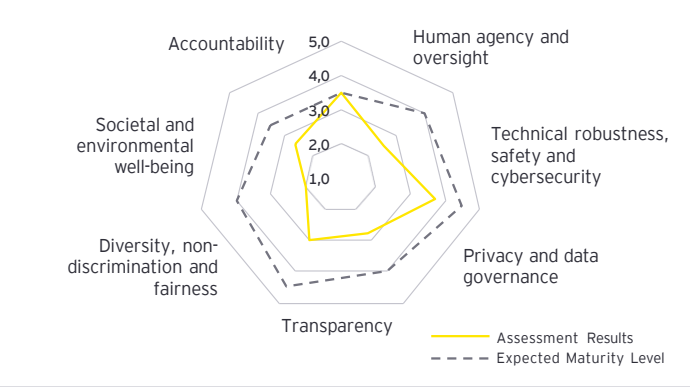
Entry into force started 1 February 2025 and companies can now face **fines of up to 40 million euros or 7% of turnover,** whichever is higher, if they fail to comply with the AI Act.

In our experience, systematically applying changes is often a challenging and lengthy process. We believe **it is crucial to start acting as soon as possible** to comply with the timelines and enable sustainable change.

Therefore, EY teams developed the **AI Act Readiness Assessment** to:

- Help organizations navigate through the regulatory requirements.
- Assess the use of AI systems and the extent to which the regulations apply.
- Support organizations in understanding where they stand regarding the regulatory requirements and determine to what extent organizations are ready to comply with the regulations.
- Assess your third-party conformity assessments in high-risk AI use cases.
- Assess organizational maturity and determine areas of prioritized focus.
- Perform a deep dive on specific AI systems in view of the legal requirements set by the AI Act.

Organization's maturity per AI ethics domain



If you are interested in finding out more about your organization's preparedness for the AI Act, reach out to your EY contact now.

EY Law Contacts

Dr. Peter Katko
Partner
Global Digital Law Leader
EY Tax GmbH
Steuerberatungsgesellschaft
peter.katko@de.ey.com

Eric Meyer
Senior Manager
Digital Law
EY Tax GmbH
Steuerberatungsgesellschaft
eric.meyer@de.ey.com

Konrad Meier
Senior Manager
Tax, Law, Corporate Law
Privacy Law Leader Switzerland
Ernst & Young AG
konrad.meier@ch.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 009694-24Gbl

ED None

ey.com