Navigating the EU AI Act: what you need to know

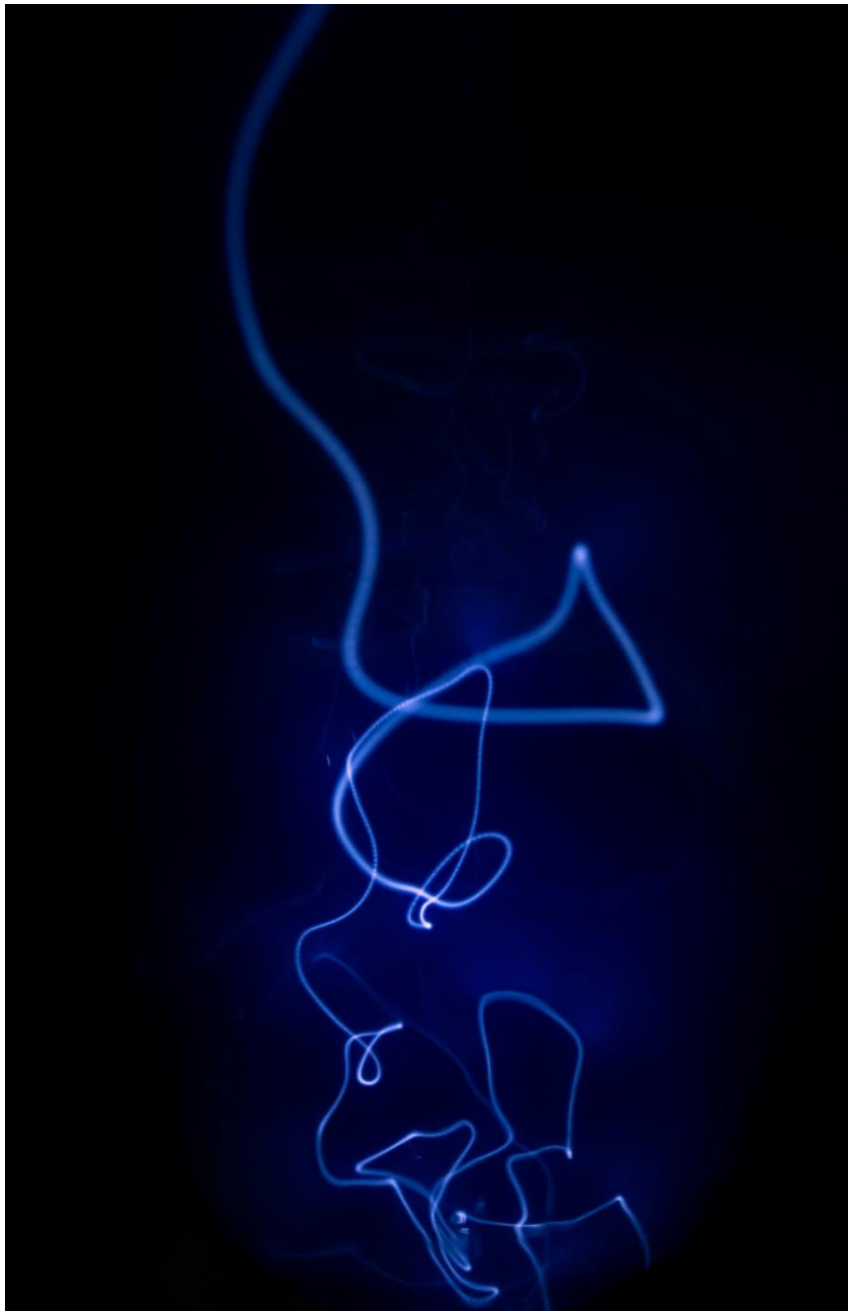
SORAINEN

Oliver Kuusk

22 February 2024

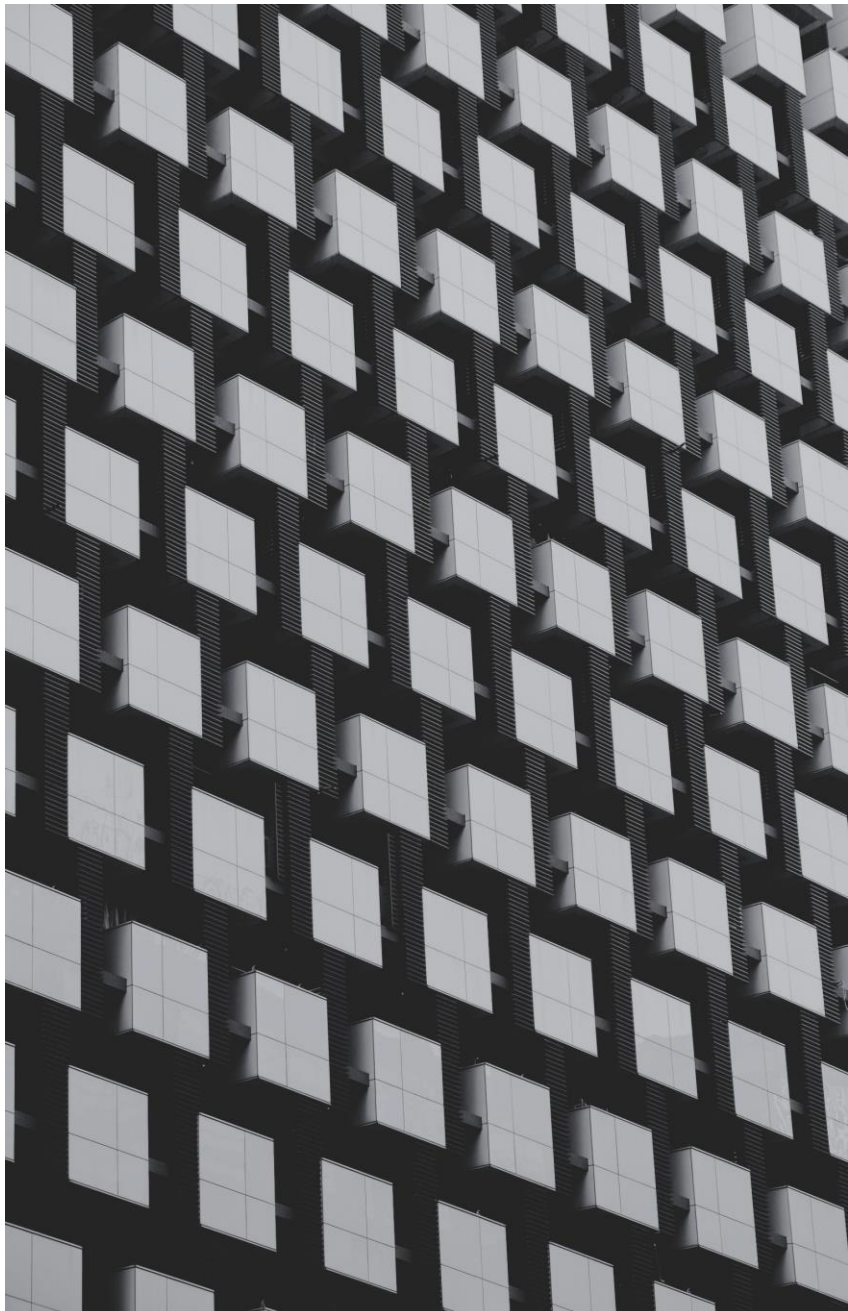
Agenda

- Scope of the AI Act
- Risk-based approach
  - Prohibited AI practices
  - High-risk AI systems
    - High-risk AI: operator obligations
- Enforcement timeline & fines
- Key steps for preparation



Scope: definition of AI

- Definition of AI
  - ‘AI system‘ is a
    1) machine-based system;
    2) designed to operate with varying levels of **autonomy**; and
    3) that may **exhibit adaptiveness** after deployment; and that,
    4) for explicit or implicit objectives, **infers, from the input it receives, how to generate outputs** such as predictions, content, recommendations, or decisions that **can influence physical or virtual environments**



Scope: territory & applicable persons

Where will it apply?

Extraterritorial effect:

- Businesses located in the EU
- Businesses supplying AI systems to the EU
- Businesses located outside the EU, if output of their AI system is used in the EU

Who will it apply to?

AI operators:

- Providers – develop AI & place on the market or put into service
- Importers & distributors – place AI or make AI available on the market
- Deployers – users of AI systems

Scope: exclusions

Personal, non-professional activities

AI systems used exclusively for military, defence or national security purposes

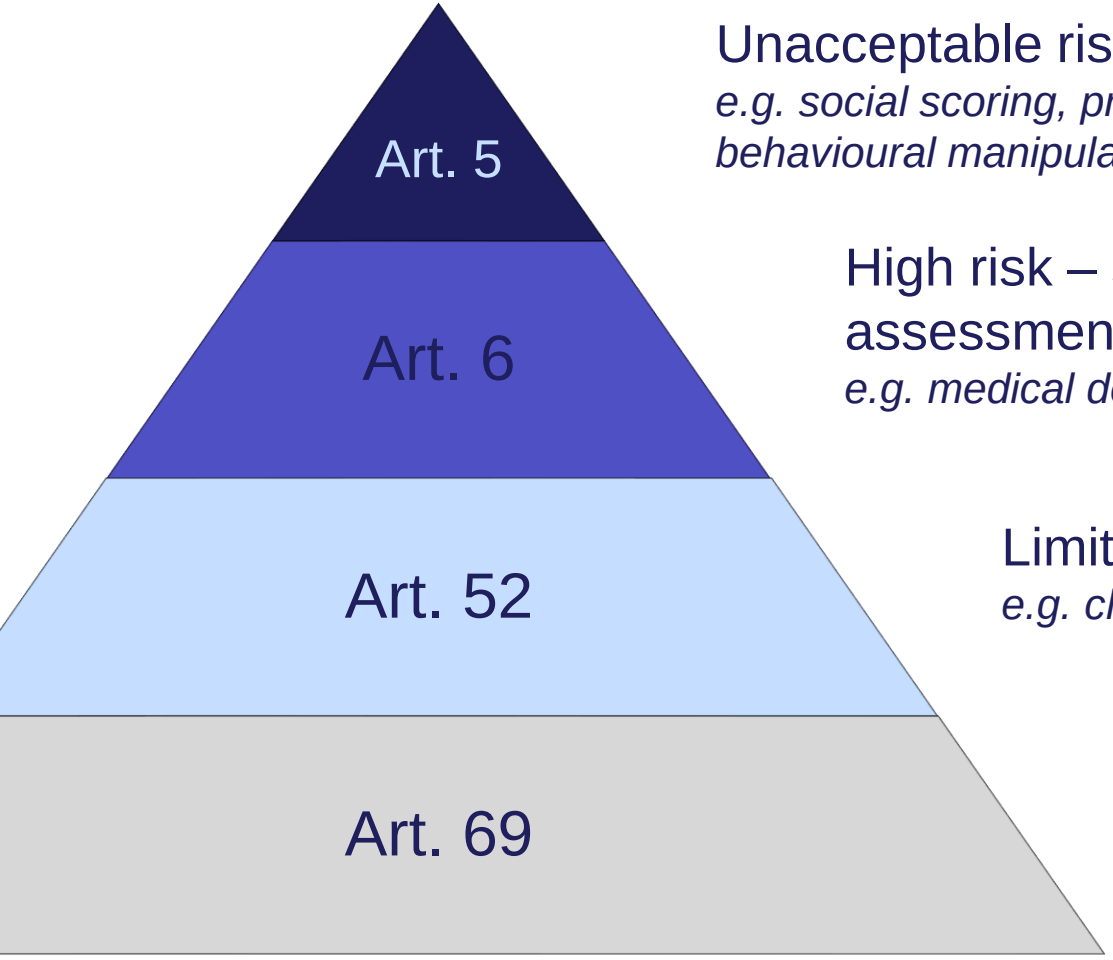
AI with the sole purpose of scientific research and development

Research, development and testing of AI systems

AI used by public authorities outside the EU and international organisations

AI systems released under free and open source licenses (excluding prohibited and high-risk AI and GPAI models under some conditions)

Risk-based approach



Unacceptable risk – prohibited
e.g. social scoring, predictive policing
behavioural manipulation

High risk – subject to mandatory requirements and ex ante conformity assessment
e.g. medical devices, vehicles, law enforcement, education, immigration

Limited risk – subject to transparency obligations
e.g. chatbots, deep fakes

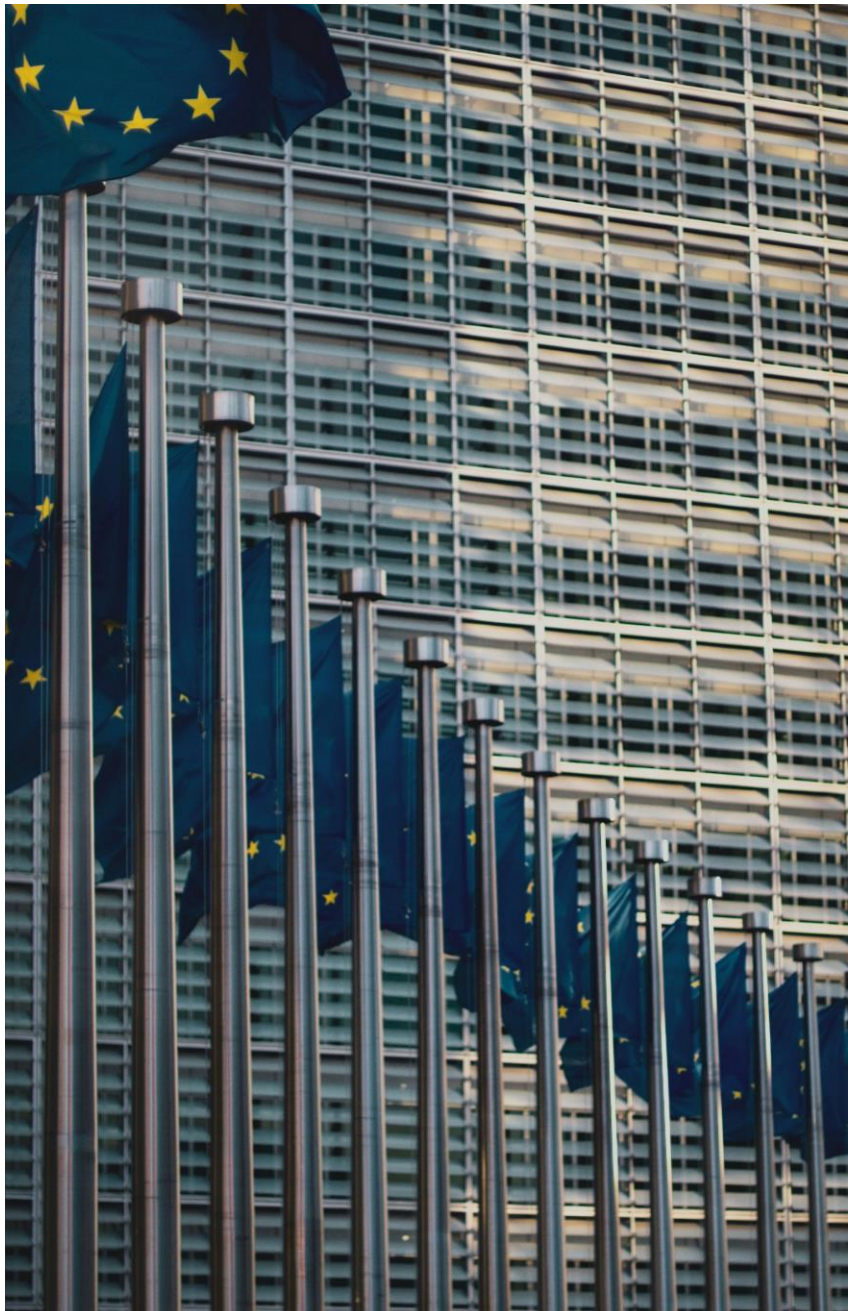
Unregulated – voluntary codes of conducts
e.g. spam filters, games

+ general-purpose AI
e.g. GPT, Gemini

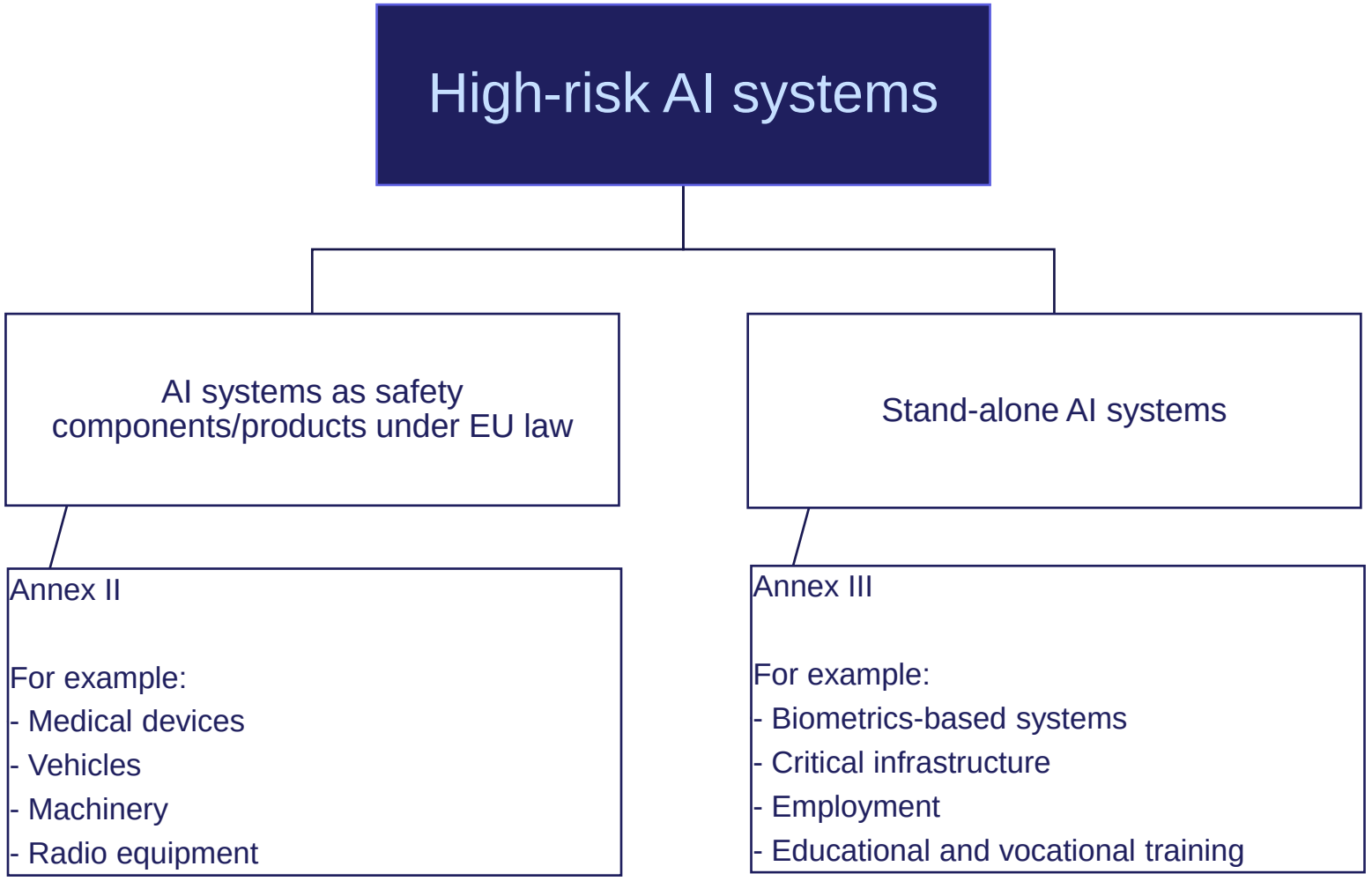
Prohibited AI

Prohibited AI practices under the AI Act:

- Subliminal or purposefully manipulative or deceptive techniques
- Exploiting vulnerabilities due to age, disability or specific social or economic situation
- Biometric categorisation to deduce/infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation
- Social scoring based on behaviour or characteristics
- Real-time biometric identification in public spaces for law enforcement
- Predictive policing
- Facial recognition databases through untargeted scraping of facial images
- Inferring emotions in the workplace or an educational institution



High-risk AI: two categories



High-risk AI – Annex II

Where the AI systems fulfills **both** conditions:

1) AI system is intended to be used as a safety component (or is itself a product) under EU legislation listed in Annex II; AND
2) product is required to undergo third-party conformity assessment

---

Annex II EU legislation covers:

- Machinery
- Toys
- Recreational craft and personal watercraft
- Lifts
- Equipment and protective systems for explosive atmospheres
- Radio equipment
- Cableway installations
- Personal protective equipment
- Appliances burning gaseous fuels
- Medical devices
- In vitro diagnostic medical devices
- Civil aviation security
- Two- or three-wheel vehicles and quadricycles
- Agricultural and forestry vehicles
- Marine equipment
- Rail systems
- Motor vehicles and trailers
- Civil aviation and aircraft

High-risk AI – Annex III

AI systems in Annex III are considered high-risk:

- Biometrics-based systems
- Critical infrastructure
- Educational and vocational training
- Employment, workers management and access to self-employment
- Access to essential private and public services/benefits
- Law enforcement
- Migration, asylum and border control management
- Administration of justice and democratic processes

Except where there is **no significant risk of harm to the health, safety or fundamental rights of natural persons**, including by not materially influencing the outcome of decision-making. This applies when the AI system is intended to:

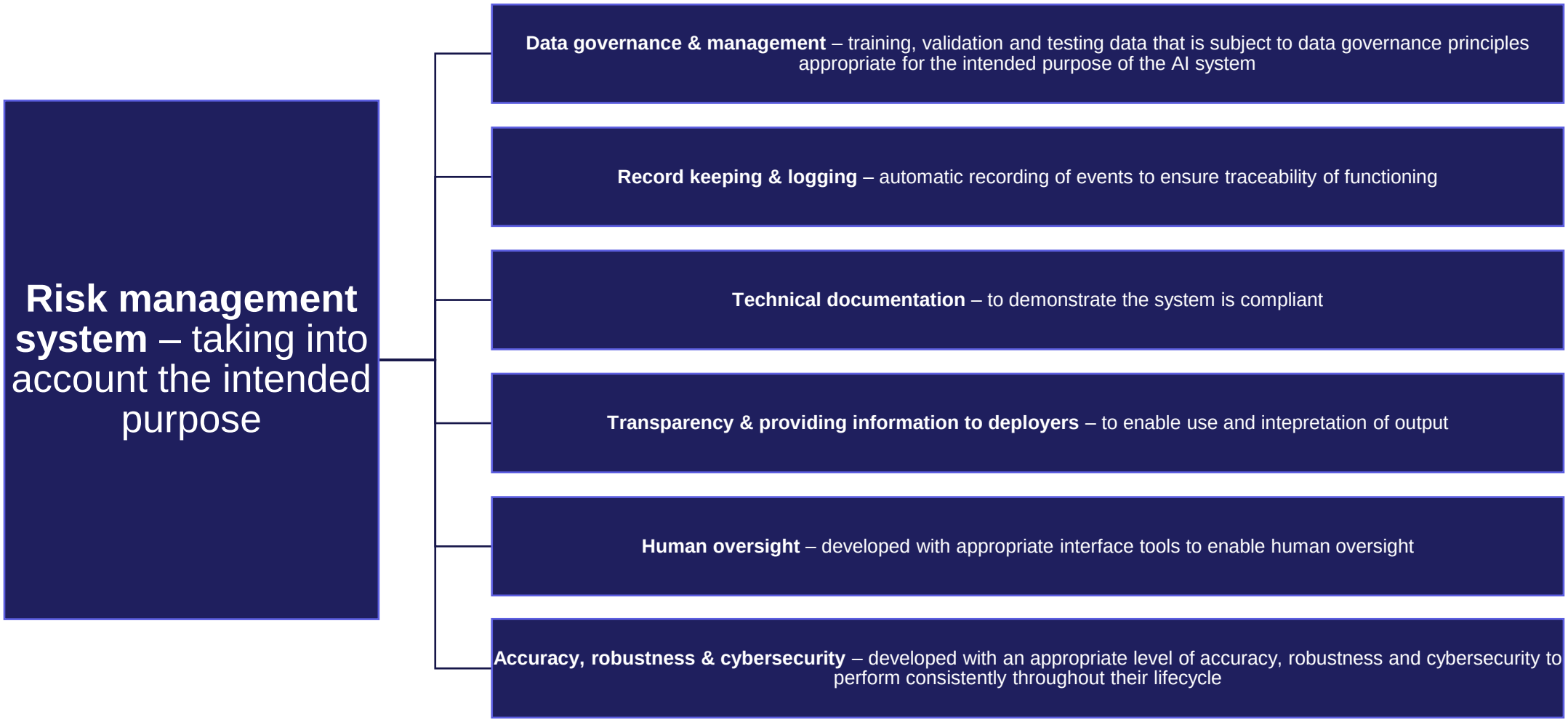
a) perform a narrow procedural task;

b) improve the result of a previously completed human activity;

c) detect decision-making patterns or deviations from prior decision-making patterns; or

d) perform a preparatory task to an assessment relevant to the purpose of the use cases listed in Annex III.

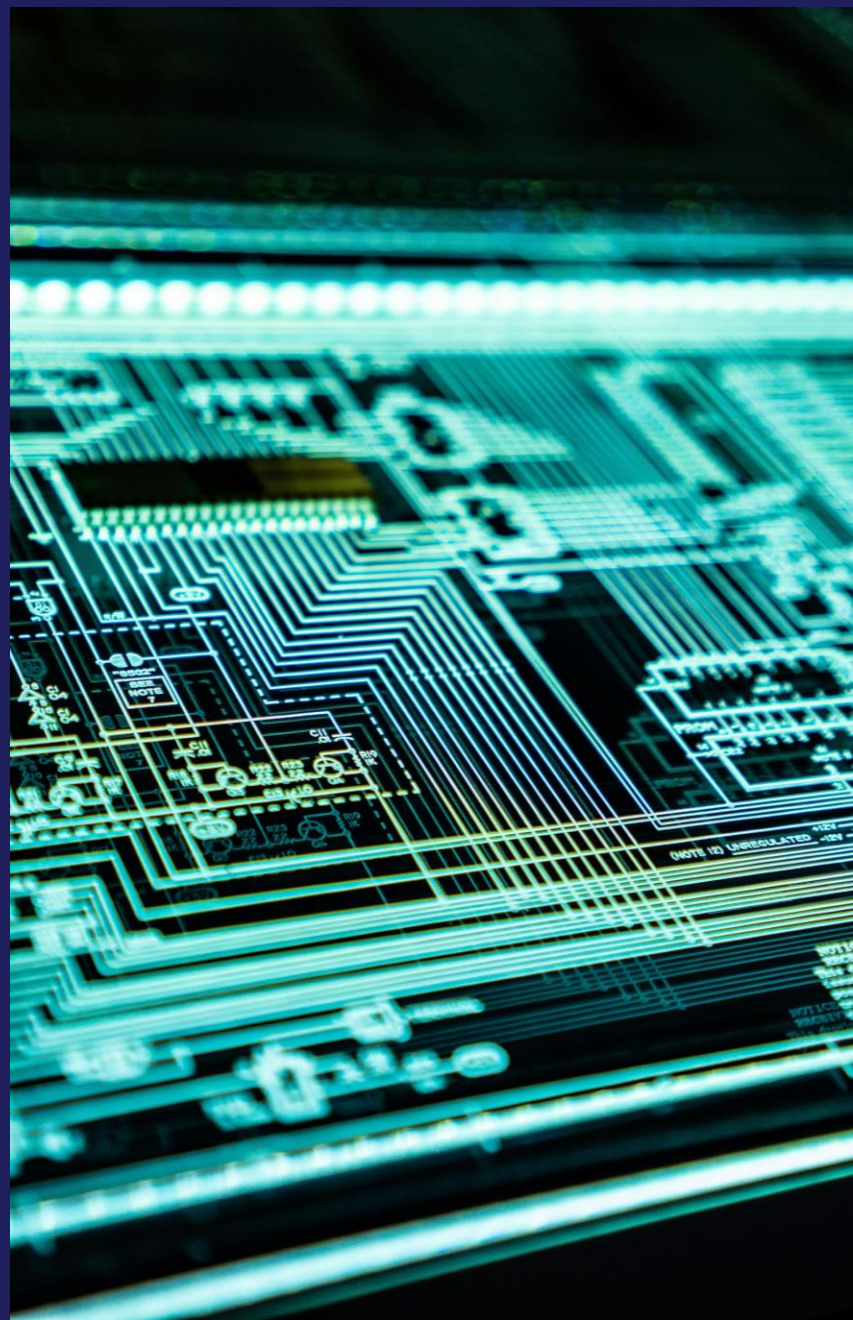
High risk AI: key requirements



High risk AI: operator obligations

- Providers:
  - Risk assessment & quality management system
  - Ex ante conformity assessment
  - Register in the EU AI database
  - Demonstrate conformity
- Standards: presumed to be in conformity with requirements for high-risk AI systems

- Deployers:
  - Measures to ensure AI system used in accordance with instructions
  - Ensure human oversight
  - Monitoring & record-keeping obligations
  - Fundamental rights impact assessment, if:
    - deployer is a body governed by public law/providing a public service
    - deploying an AI system to assess creditworthiness/risk assessment and pricing for life and health insurance



Fines under the AI Act

EUR 35 million or up to 7% of global annual turnover	EUR 15 million or up to 3% of global annual turnover	EUR 7.5 million or up to 1% of global annual turnover
• Non-compliance with prohibited AI system rules	• Violation of obligations of providers, importers, distributors, deployers and other obligations	• Supplying incorrect, incomplete or misleading information to regulators

Timeline

Entry into force

EU Parliament vote likely in early April 2024

Publication in the EU OJ + 20 days = entry into force

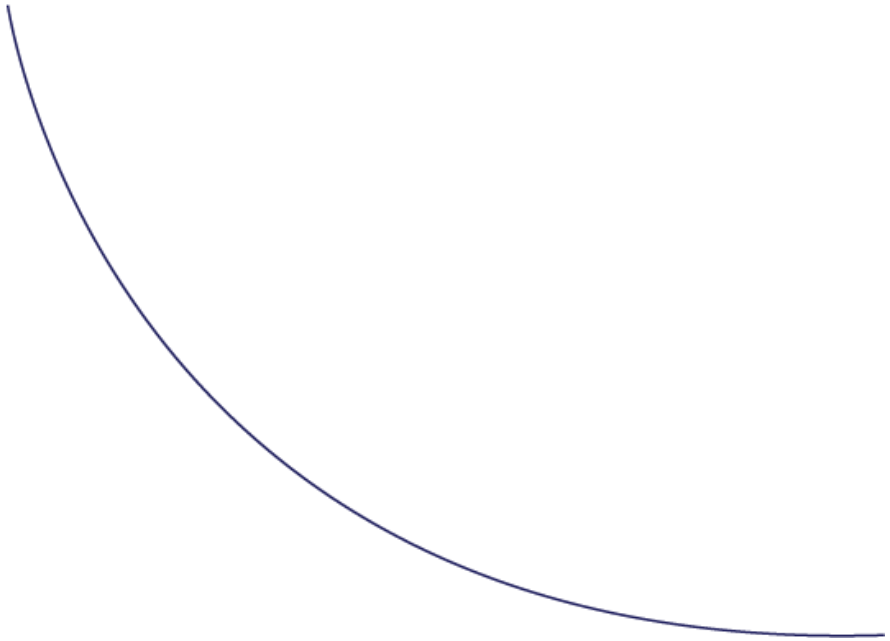
6 months
Prohibited practices

12 months
GPAI, penalties

24 months
AI Act enters into force, high-risk AI

36 months
Obligations for high-risk AI systems used as safety components/products under EU-harmonised legislation (Annex II)

Key steps for preparation



1. **Map your AI systems**
    1) Identify and map all AI systems developed or used
2. **Conduct a risk assessment**
    1) Identify the risks of each system
    2) Categorise each AI system based on the risks – is your AI regulated?
3. **Implement quality management system**
    1) Implement risk management measures based on the level of risk
    2) High risk:
        - Data governance
        - Technical documentation
        - Record keeping
        - Transparency
        - Human oversight
        - Accuracy, robustness & cybersecurity
    3) Limited risk:
        - Transparency
        - Code of conduct
    4) Look out for standards

Oliver Kuusk
oliver.kuusk@sorainen.com