BLC Webinar
The AI Act

24th of June 2024

Agenda

01

The AI Act and its legal implications.

Heleen Lauwers

Associate | KPMG Law

02

AI Act | Compliance considerations

Mahault Piéchaud Boura

Manager Digital Risk Management | KPMG Advisory

03

Practical questions for Boards

Bart Van Rompaye, PhD

Head of AI

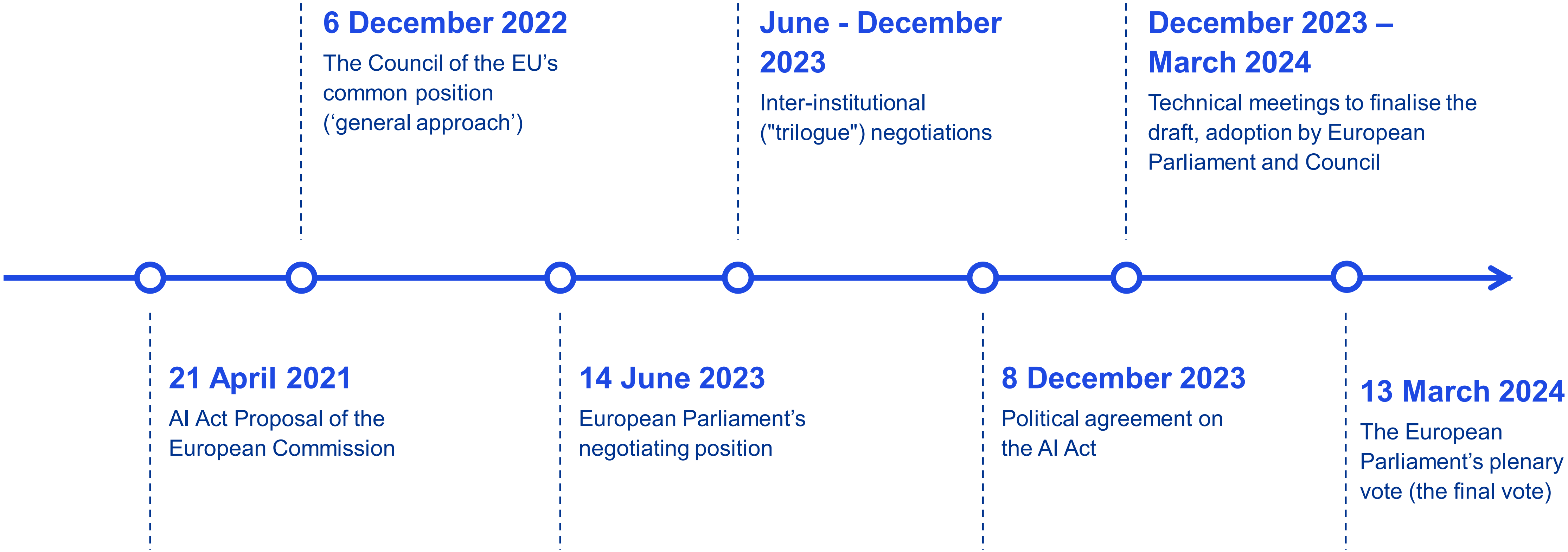
Principal | KPMG Advisory

01

The AI Act and its legal implications

Heleen Lauwers

AI Act Timeline



21 April 2021

AI Act Proposal of the European Commission

6 December 2022

The Council of the EU's common position ('general approach')

14 June 2023

European Parliament's negotiating position

June - December 2023

Inter-institutional ("trilogue") negotiations

8 December 2023

Political agreement on the AI Act

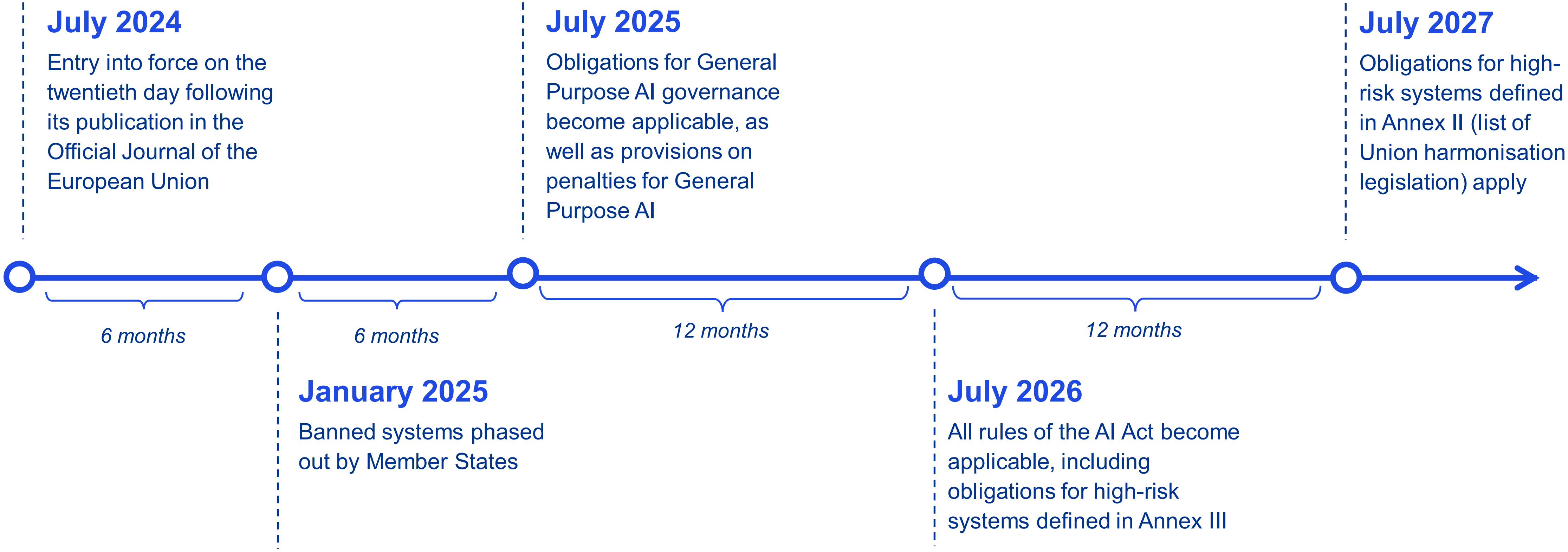
December 2023 – March 2024

Technical meetings to finalise the draft, adoption by European Parliament and Council

13 March 2024

The European Parliament's plenary vote (the final vote)

AI Act Timeline: What are the next steps?



July 2024

Entry into force on the twentieth day following its publication in the Official Journal of the European Union

6 months

January 2025

Banned systems phased out by Member States

6 months

July 2025

Obligations for General Purpose AI governance become applicable, as well as provisions on penalties for General Purpose AI

12 months

July 2026

All rules of the AI Act become applicable, including obligations for high-risk systems defined in Annex III

12 months

July 2027

Obligations for high-risk systems defined in Annex II (list of Union harmonisation legislation) apply

What is the AI Act?

The AI Act is the first horizontal legislation in the EU to regulate AI systems and takes the leading role in setting the global gold standards on the field.

Main objectives

(i) Safeguarding fundamental rights and (ii) product safety
Cultivating innovation and competitive growth

Risk - based approach

The AI Act introduces 4 risk categories and sets legal rules according to the level of risk.

Providers vs. deployers

Different actors in the AI value chain will assume distinct roles and responsibilities.

Extensive extraterritorial scope

The AI Act will govern not just AI systems developed by an EU provider, or put on the EU market, but also AI systems developed and used outside of the EU, but where the output of the system is intended for use in the EU.

Penalties Regime up to

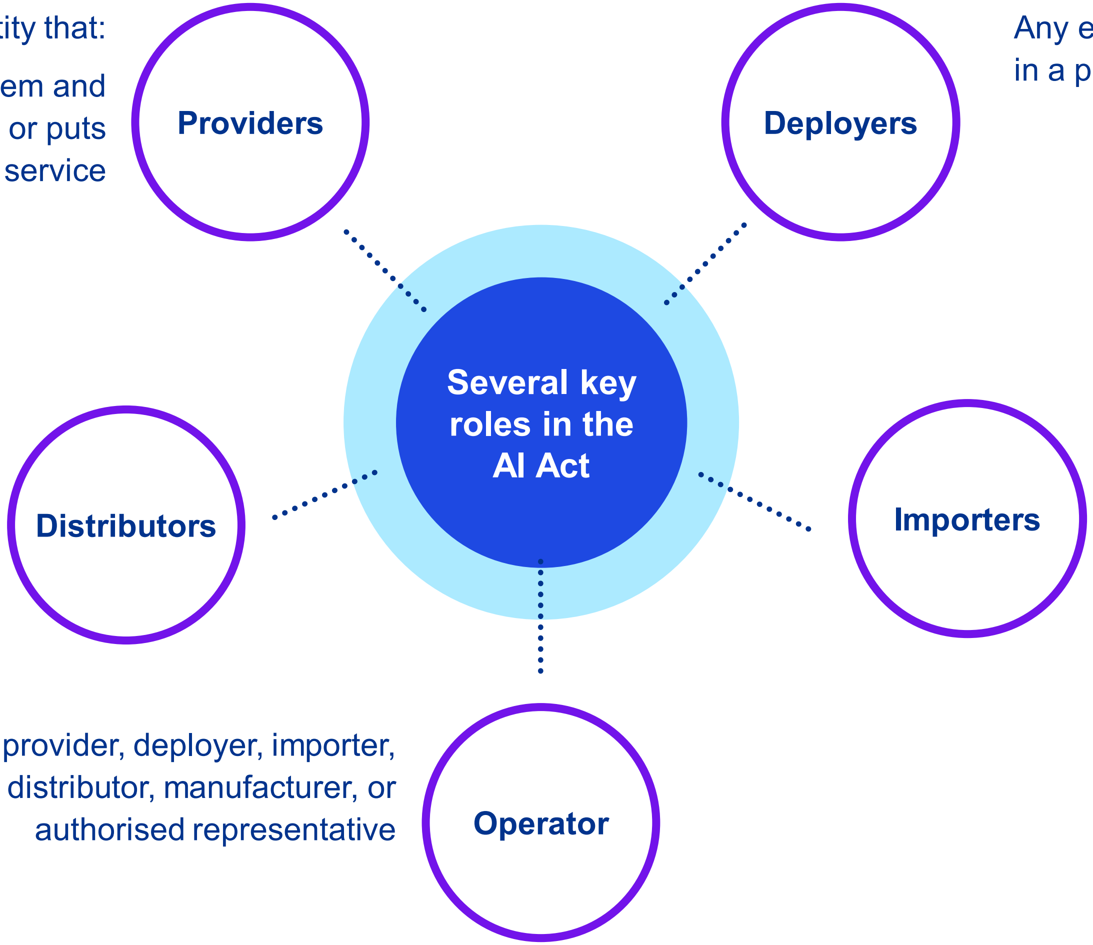
Fines for non-compliance:

€35m

7%

Company total worldwide annual turnover for the preceding financial year.

Scope of the AI Act



Several key roles in the AI Act

Providers

Any entity that:

- develops an AI system and
- Places it on the market or puts it into service

Deployers

Any entity that uses an AI system in a professional activity.

Distributors

Any entity, other than the provider or the importer, that makes an AI system available in the EU.

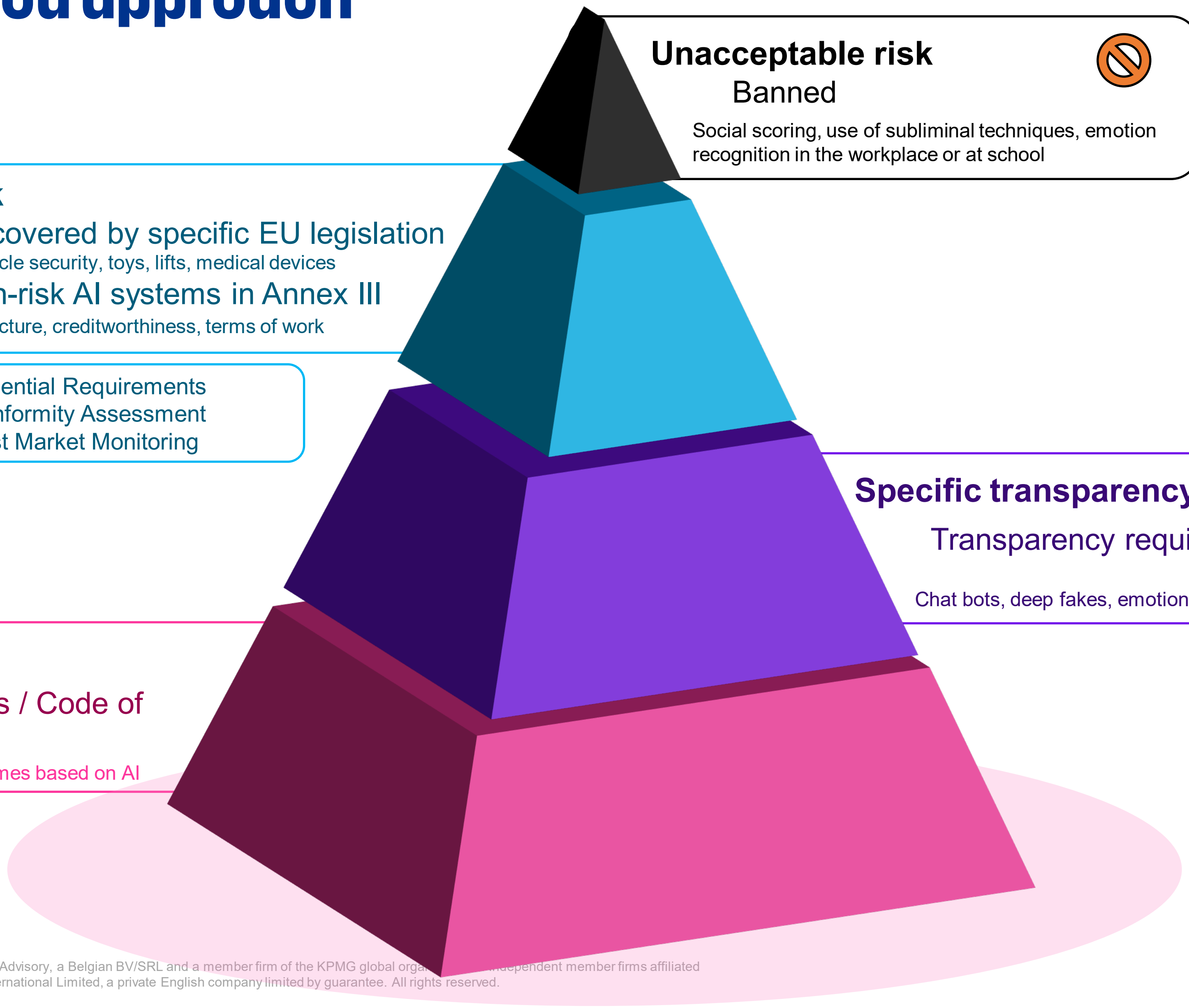
Importers

Any entity that places on the market an AI system bearing the name or trademark of an entity outside the EU.

Operator

The provider, deployer, importer, distributor, manufacturer, or authorised representative

Risk-based approach



Unacceptable risk

Banned

Social scoring, use of subliminal techniques, emotion recognition in the workplace or at school

High-risk

Products covered by specific EU legislation

Machinery, vehicle security, toys, lifts, medical devices

List of high-risk AI systems in Annex III

Critical infrastructure, creditworthiness, terms of work

- Essential Requirements
- Conformity Assessment
- Post Market Monitoring

Specific transparency risk

Transparency requirements

Chat bots, deep fakes, emotion recognition systems

Minimal risk

Voluntary basis / Code of Conduct

Spam filters, video games based on AI

Key legal challenges

Interplay with GDPR

Development and use of AI systems triggers the question of data privacy.

- Complementary frameworks
- Each with its own set of rules and obligations
- Already having in place the necessary data protection controls and policies will prove to be an advantage

Liabilities

Various liability regimes are to be taken into account.

- Allocation of liabilities in contracts between provider and deployer
- No specific attention to director liability in the AI Act
- Impact of new legislative initiatives
  - Product Liability Directive
  - AI Liability Directive

Other legal challenges

The AI Act does not answer everything.

- Consumer protection law
- Intellectual property law
- Competition law
- Product safety
- Sector specific regulations
- …

Key Take Aways

Urgency of preparation

The time to understand and prepare for the AI Act is now.

Roles and responsibilities

Understanding the different roles and responsibilities outlined in the AI Act is crucial for ensuring compliance.

Navigating legal intersections

Understanding the intersection of the AI Act with existing legislation will enable organizations to streamline their efforts and meet their requirements more effectively and efficiently.

Consider director liability

Directors should be mindful of potential liabilities and should review indemnification terms in their organization’s articles of association and their liability insurance policies.

02

AI Act and compliance considerations

Mahault Piéchaud Boura

Why compliance matters

Claims

7% or €35M

Prohibited AI violations: up to 7% of global annual turnover or 35 million euros

3% or €15M

Most other violations (providers and deployers): up to 3% of global annual turnover or 15 million euros.

1% or €7.5M

Supplying incorrect information to authorities: up to 1% of global annual turnover or 7.5 million euros.

Trust

- ○ Regulations and compliance thereto are expected to protect individuals for negative impact of AI.
- ○ The AI Act aims to ensure that AI systems are safe, respect fundamental rights, foster AI investment, improve governance, and encourage a harmonized single EU market for AI.

Board Liability & Accountability

Role of the board linked to AI

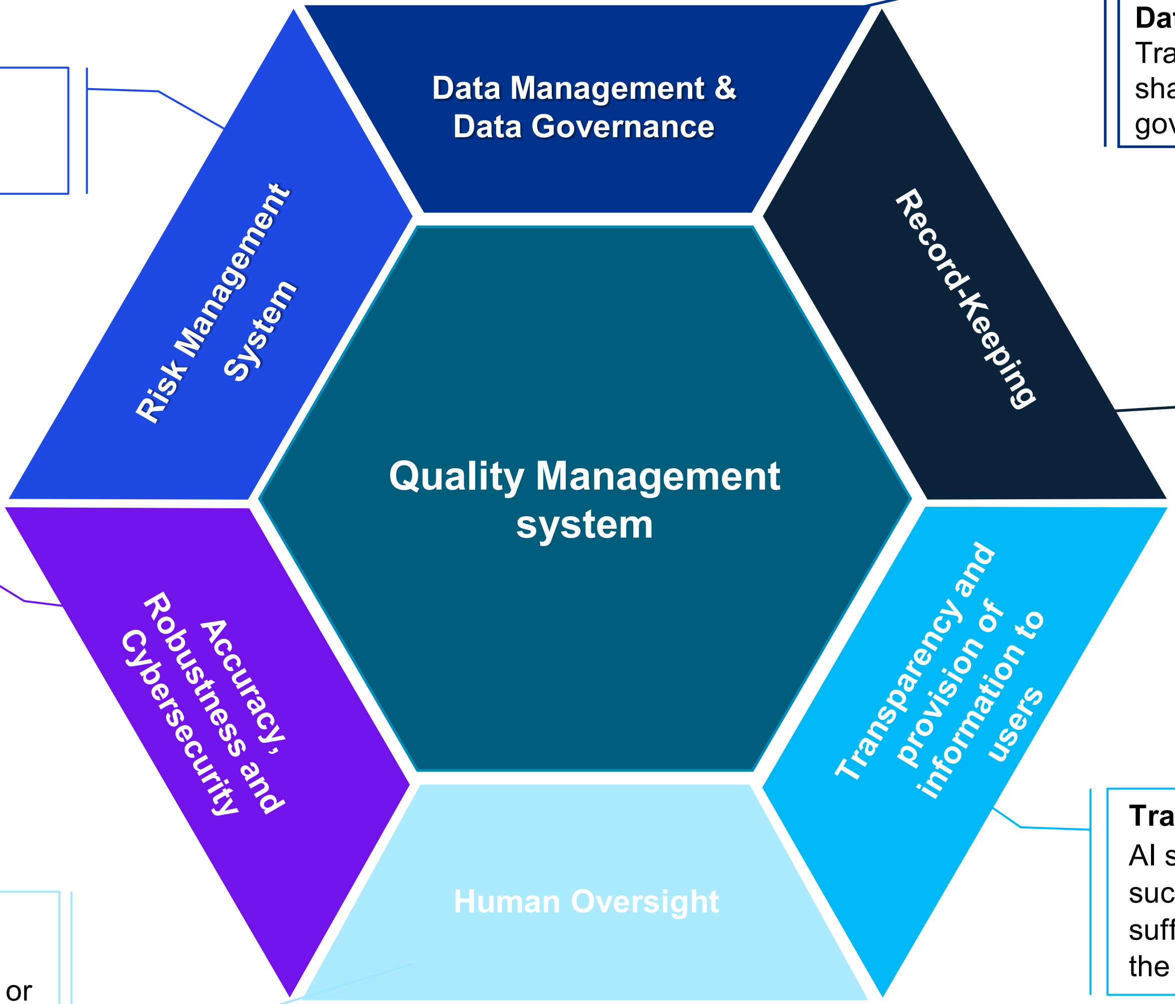
- Understanding AI as a matter of corporate strategy and risk;
- Considering the impact of AI activities on employees, customers, other key stakeholders, and the environment; and.
- Overseeing the company’s compliance with laws and regulations that are relevant to AI and the development of related policies, information systems, and internal controls.

Liability

- No direct liability under the AI Act.
- Consequences in cases of fine, and classic accountability of board members.

KPMG

What does compliance entail?


Data Management & Data Governance
Risk Management System
Record-Keeping
Quality Management system
Accuracy, Robustness and Cybersecurity
Transparency and provision of information to users
Human Oversight

Risk management
A risk management system must be established, implemented, documented and maintained.

Accuracy, robustness and cybersecurity
AI systems are designed and developed to achieve an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle

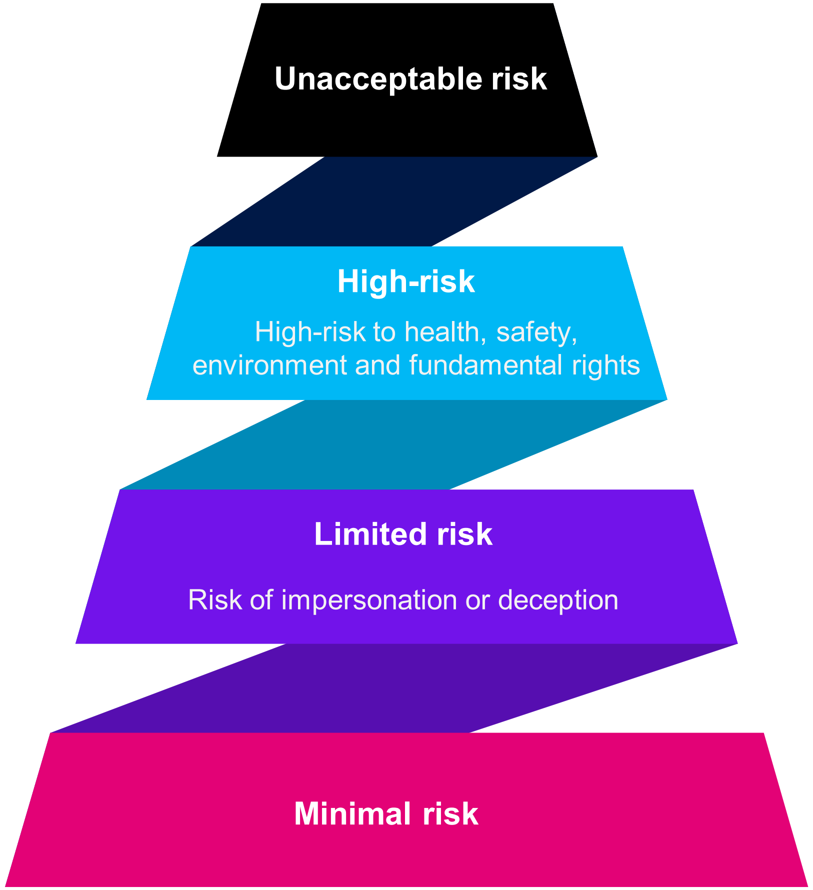
Human Oversight
AI systems are designed and developed to be effectively overseen by natural persons to prevent or minimize risk to fundamental rights.

Data Management & Data Governance
Training, validation and testing data sets shall be subject to appropriate data governance and management practices

Record-Keeping
AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating to support the traceability of the decisions

Transparency
AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately

Granular obligations



Unacceptable risk

High-risk

High-risk to health, safety, environment and fundamental rights

Limited risk

Risk of impersonation or deception

Minimal risk

Provider

Cannot market

- Quality and risk management systems
- Compliance high risks requirements
- Conformity assessment
- Risk monitoring (post market monitoring)
- Transparency and provision of information to deployers
- Incident and mal function reporting
- Retaining generated logs

Transparency by design

Code of conduct (voluntary)

Deployer

Cannot deploy

- Intended use
- Ensure human oversight
- Transparency to users / data subjects
- Keep logs
- Incident and mal function reporting

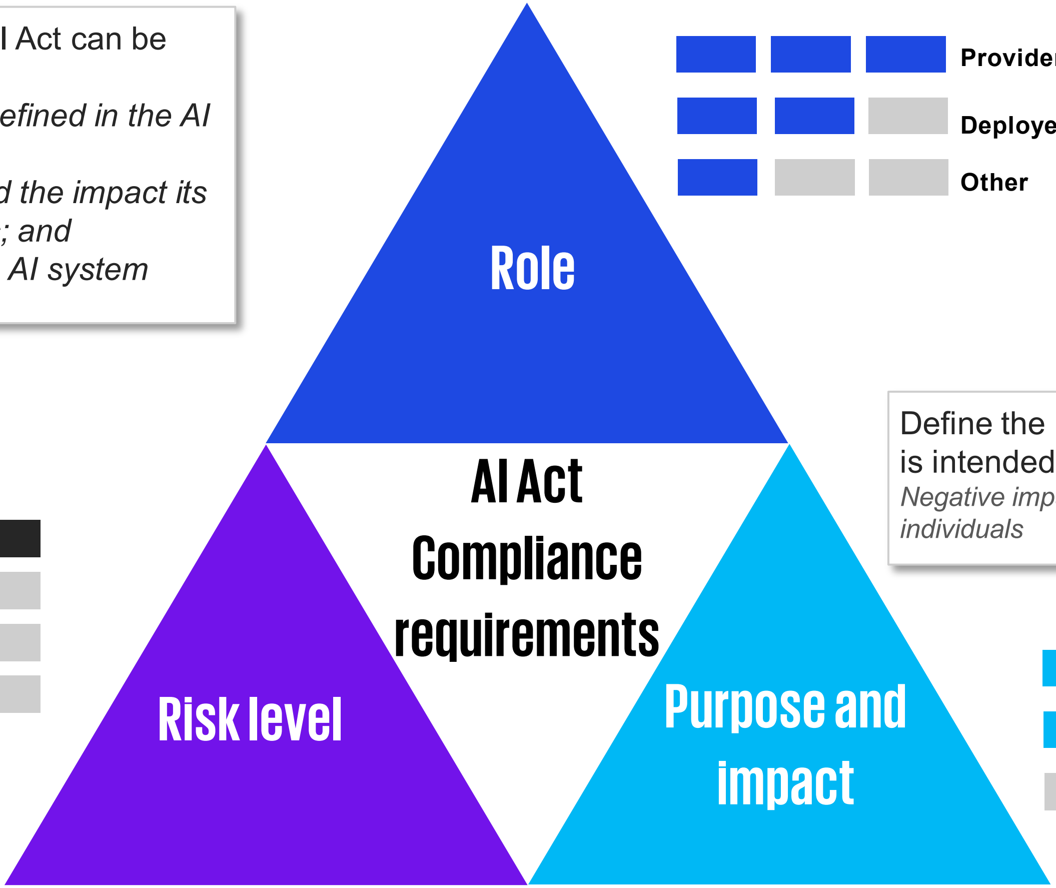
Transparency by default

Code of conduct (voluntary)

Defining compliance requirements

The degree of obligation under the AI Act can be derived from three main factors:

1. *The role of the organization, as defined in the AI Act*
2. *The purpose of the AI system and the impact its use with gave on natural persons; and*
3. *The risk level associated with the AI system*



🟦	🟦	🟦	Provider
🟦	🟦	⬜	Deployer
🟦	⬜	⬜	Other

Define the impact of the use for which the AI system is intended, it purposes, on individuals
Negative impact on security, safety and fundamental rights of individuals

🟦	🟦	🟦	Purpose negatively impacting individuals
🟦	🟦	⬜	Purpose impacting individuals
⬜	⬜	⬜	No to minimal impact in individuals

Unacceptable	⬛	⬛	⬛	⬛
High	🟦	🟦	🟦	⬜
Limited	🟪	🟪	⬜	⬜
Minimal	🟥	⬜	⬜	⬜

Purpose & impact

What is the intended purpose?

“The use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation”

Defining the impact

- Who is affected by the use of the system?
- In what context?
- Does it impact their fundamental rights?
- Does it impact their safety and security?
- Is the impact negative?

🟦 🟦 🟦 **Purpose negatively impacting individuals**

🟦 🟦 ⬜ **Purpose impacting individuals**

⬜ ⬜ ⬜ **No to minimal impact on individuals**

Assessments

Mapping of AI Systems

What AI is in use?

- Organizations must have and maintain a good view of the AI systems in use internally and externally.
- AI system registry can be used as a base line to follow on compliance.

Risk Tiering and Risk assessments

What is the Risk Level?

The AI Act categorizes AI systems by risk to public safety and rights, defining specific compliance requirements for each category.

- **Risk Management**: Identify, understand, and mitigate potential risks before they occur to prevent operational, legal, and reputational damage.
- **Regulatory Compliance**: Ensure AI system deployments adhere to all necessary laws and regulations, avoiding potential legal issues and sanctions.
- **Conformity Assessments:** AI providers must demonstrate compliance with standards before deployment and maintain these standards throughout the system's lifecycle.

Compliance Assessment

What is your organization Compliance Level?

Evaluating the maturity of your overall AI governance program to identify areas where improvements can be made, and ensure alignment with best practices, regulations, and ethical guidelines.

No matter the stage an organization is in, **AI Governance Program Maturity Assessments** will help re-align the organization with best practices, regulations, and ethics while maximizing the value derived from AI technology.

Journey to AI Act compliance

Define your organization’s strategic approach to AI

To foster compliance and adhere to legal and industry-specific requirements, minimizing risks associated with data privacy, security, and bias

Define and deploy your policies and control framework

Defining policies and standards will for AI will strengthen the organization's existing directives, guidelines, and procedures to account for the unique risks and challenges presented by AI.

Assess and Remediate

AI Deployment Risk Assessments are crucial for identifying potential risks and implementing appropriate mitigation strategies to ensure compliance with laws and regulations and your organization's policies and standards.

Monitor and Improve

Compliance is a never-ending effort, based on iterative evaluation and improvement to keep up with your organization’s activities.

Key Take Aways

Purpose and Impact

Intended purpose of a system and its impact on individuals drive the applicability of the AI act.

Compliance fosters Trust

Compliance can be used to foster trust

Granularity of obligations

The compliance requirement are dependent on the risk qualification under the AI Act. Sturdy compliance framework is necessary to flexibly take compliance requirements.

Continuous exercise

Compliance and risk assessments are iterative processes and need to be monitored overtime.

03

Practical questions for Boards

Bart Van Rompaye

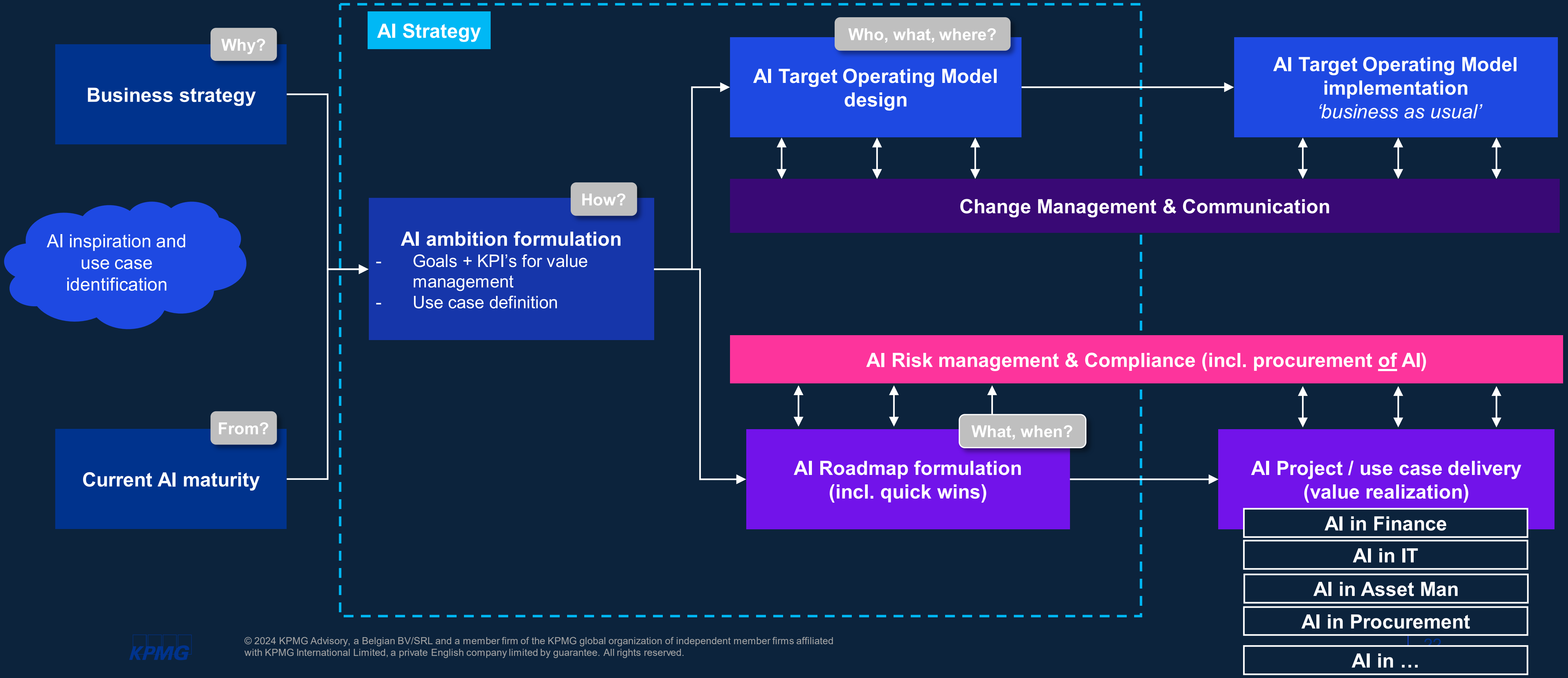
Minimize risk to individuals

AI ACT

Maximizing the value

Minimize risk to your company

The top needs to start providing structure



Why?

Business strategy

AI inspiration and use case identification

From?

Current AI maturity

AI Strategy

How?

AI ambition formulation

- Goals + KPI's for value management
- Use case definition

Who, what, where?

AI Target Operating Model design

AI Target Operating Model implementation
'business as usual'

Change Management & Communication

AI Risk management & Compliance (incl. procurement of AI)

What, when?

AI Roadmap formulation (incl. quick wins)

AI Project / use case delivery (value realization)

AI in Finance

AI in IT

AI in Asset Man

AI in Procurement

AI in …

Trusted AI is critical

AI ACT

We understand trustworthy and ethical AI is a complex business, regulatory, and technical challenge, and we are committed to helping clients put it into practice. We help develop, and deploy an end-to-end Trusted AI program across the AI/ML lifecycle

Fairness
Ensure models reduce or eliminate bias against individuals, communities or groups

Transparency
Include responsible disclosure to provide stakeholders a clear understanding as to what is happening within the AI solution and across the AI lifecycle

Explainability
Ensure AI solutions are understandable as to how and why recommendations are made or conclusions drawn

Accountability
Human oversight and responsibility embedded across the AI lifecycle to manage risk and ensure compliance with regulations and applicable laws

Security
Safeguard against unauthorized access, bad actors, misinformation, corruption, or attacks

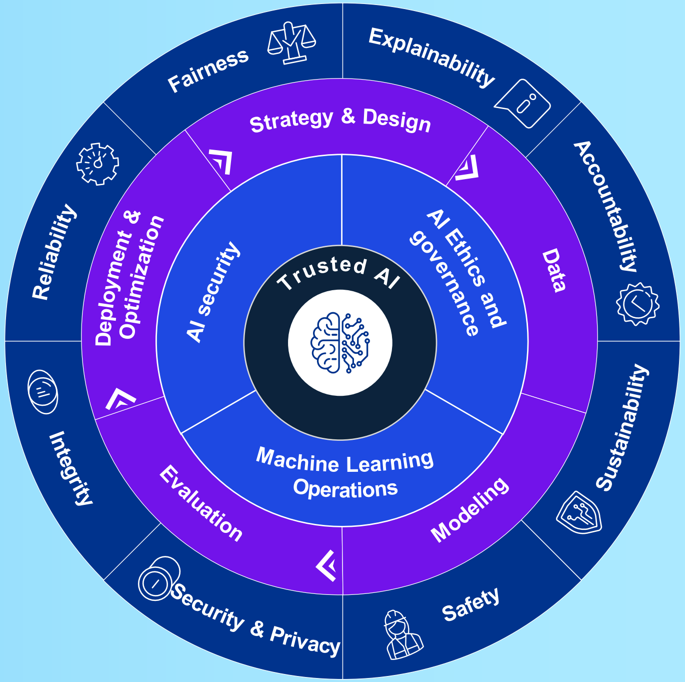
Privacy
Ensure compliance with data privacy regulations and consumer data usage

Sustainability
Optimize AI solutions to limit negative environmental impact where possible

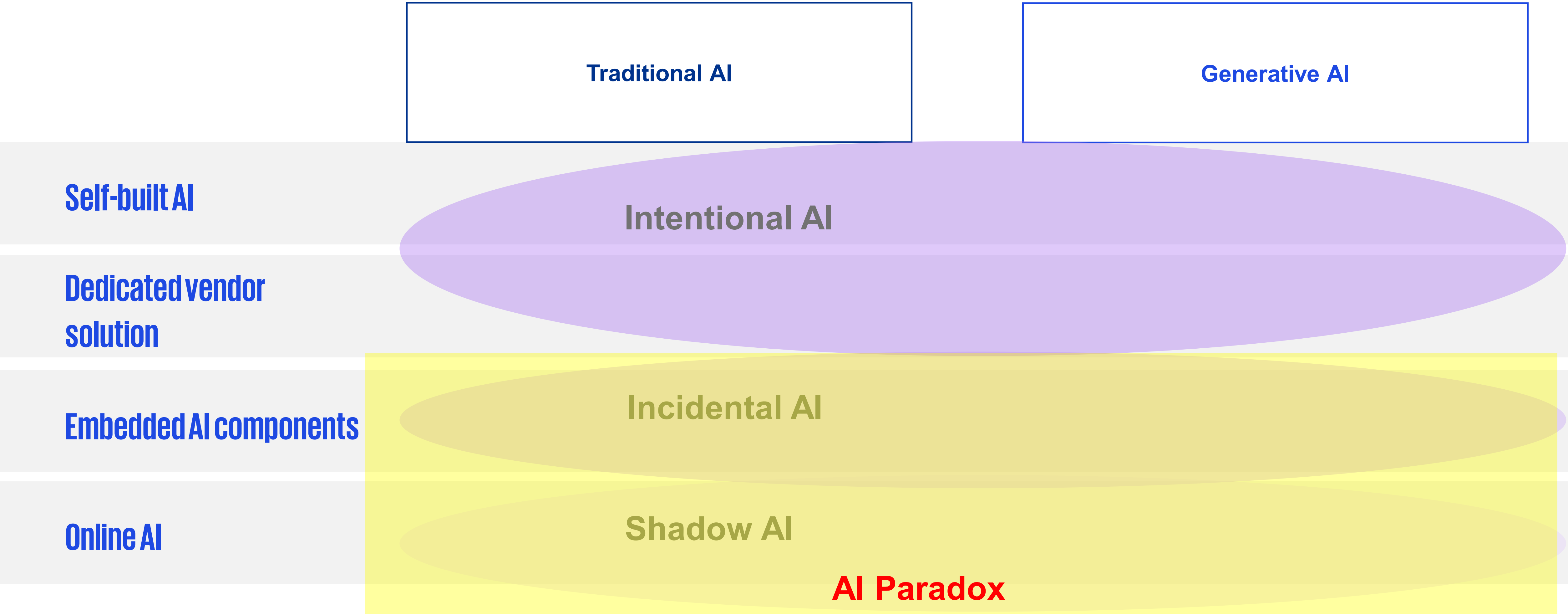
Data integrity
Ensure data quality, governance, and enrichment steps embed trust

Reliability
Ensure AI systems perform at the desired level of precision and consistency

Safety
Safeguard AI solutions against harm to humans and/or property



AI – the full playing field



Traditional AI

Generative AI

Self-built AI

Dedicated vendor solution

Embedded AI components

Online AI

Intentional AI

Incidental AI

Shadow AI

AI Paradox

Creating visibility: from an initial view…

Define

- What is AI
- What is a model
- What is a solution
- What is the lifecycle
- Structure of the landscape
- …

High level Risk Assessment

High level questionnaire

- Get first view on usage
- Get first view on existing controls
- Allows first risk level assessment
- Allows priority setting

AI Governance

Focus: the current governance framework around AI

Auditor knowledge: AI and governance knowledge, and IT auditor

AI Integration

Focus: management and operations of AI-enabled activities

Auditor knowledge: Auditor with AI knowledge, much involvement of IT auditor

AI Development

Focus: solution risk of specific project/model/application and its regulatory compliance

Auditor knowledge: AI and governance knowledge, and IT auditor, and AI experts

Creating visibility: from an initial view… to BAU

Technical Screening

- Of tools
- Of online interactions
- Of company resources (documentation, collaboration sites,…)
- Of own code

Processes

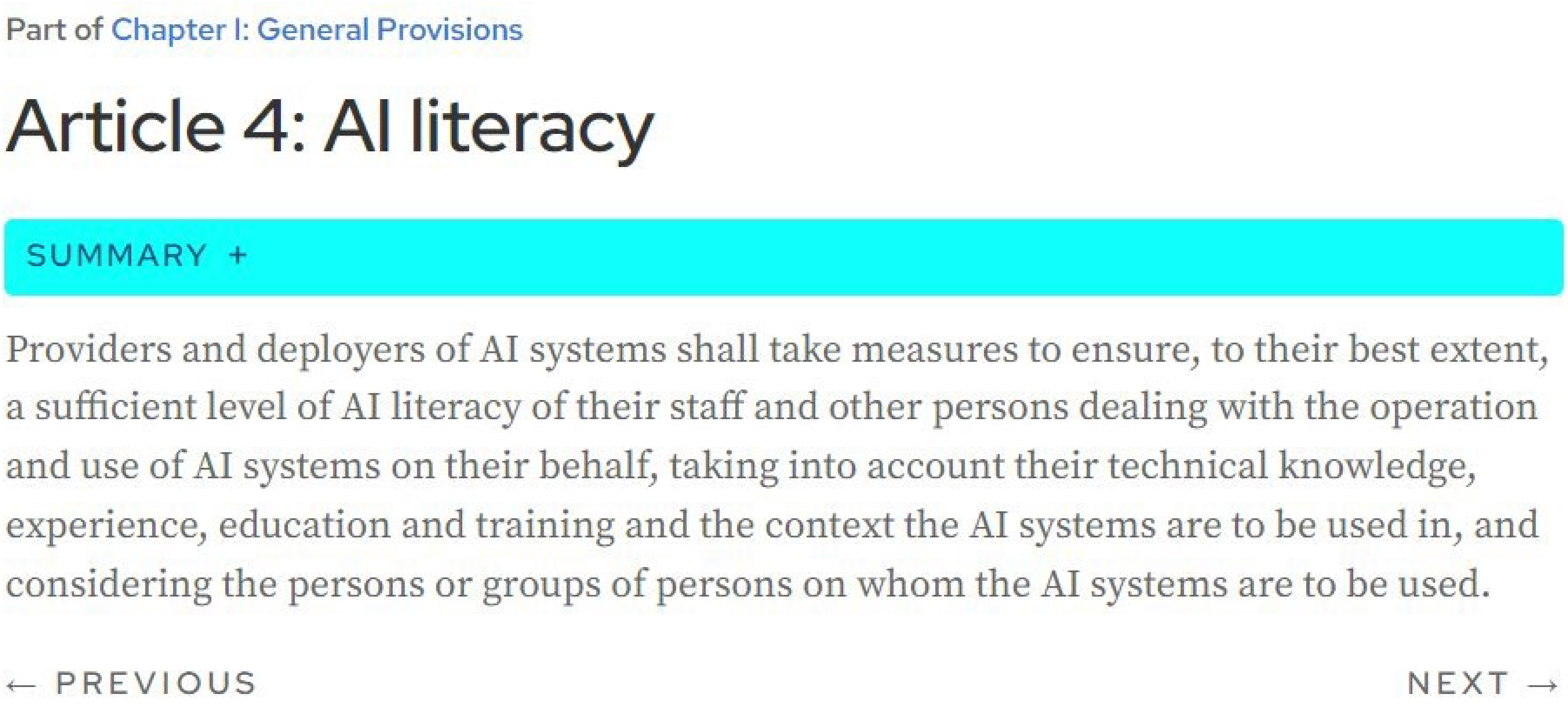
- Make sure your (existing or new) processes actively screen
- E.g. procurement, risk processes, product development, legal review,…

Focus

- Recurrent deep dives in areas where high risk AI is more likely
- E.g. HR, critical infrastructure, essential services

Training

- Teach people to recognize AI
- Teach about the importance of its visibility
- Give an easy way to flag it



Part of Chapter I: General Provisions

Article 4: AI literacy

SUMMARY +

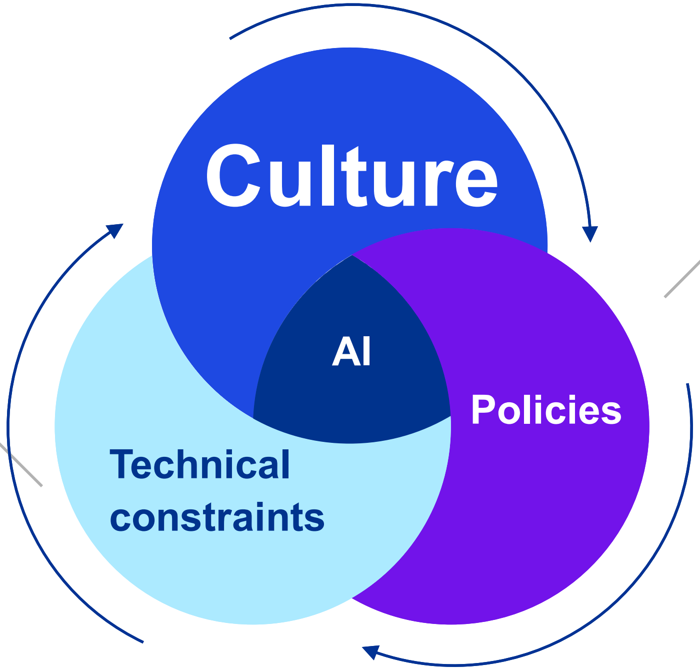
Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

← PREVIOUS

NEXT →

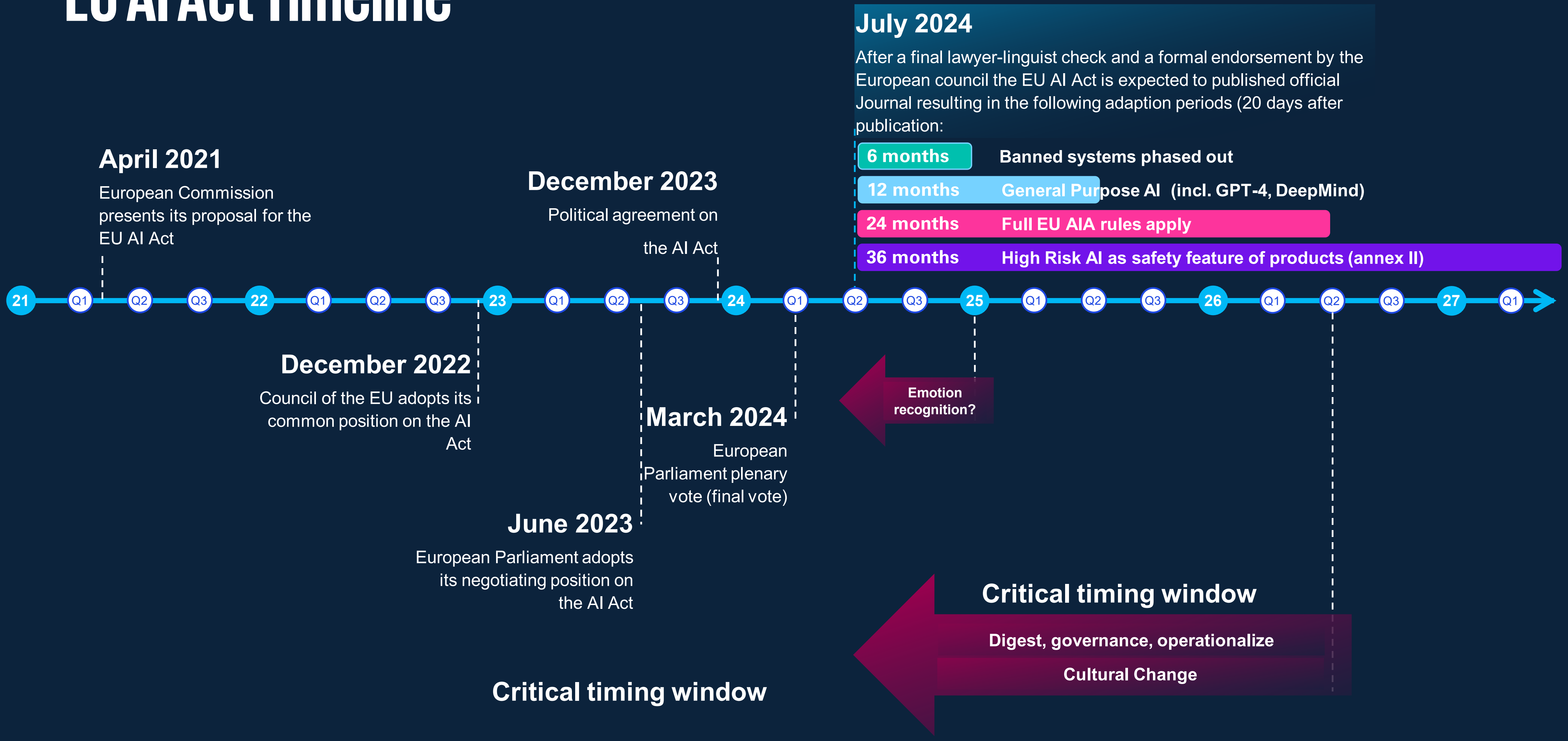
The most important?

- Restrict access
- Role-based differentiation
- Monitoring
- Physical security
- Tooling
- …



- Code of conduct
- Best practices
- Standards
- Security policies
- Training policies
- Transparency approaches
- …

EU AI Act Timeline



April 2021

European Commission presents its proposal for the EU AI Act

December 2022

Council of the EU adopts its common position on the AI Act

June 2023

European Parliament adopts its negotiating position on the AI Act

December 2023

Political agreement on the AI Act

March 2024

European Parliament plenary vote (final vote)

July 2024

After a final lawyer-linguist check and a formal endorsement by the European council the EU AI Act is expected to published official Journal resulting in the following adaption periods (20 days after publication:

6 months	Banned systems phased out
12 months	General Purpose AI (incl. GPT-4, DeepMind)
24 months	Full EU AIA rules apply
36 months	High Risk AI as safety feature of products (annex II)

Emotion recognition?

Critical timing window

Digest, governance, operationalize

Cultural Change

Critical timing window

Key Take Aways

Balance risk and pursuit of value

Check the essential building blocks

Your AI vision, ambition, risk appetite, strategy

Create visibility across the entire AI playing field

Work on knowledge and expertise

Train everyone, also yourself, and fill gaps by partnering with externals

And most important: start now!

KPMG

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia