Linklaters

Belgium-Japan Association
Chamber of Commerce
日白協会兼商工会議所

The EU AI Act:

Are you ready for the New World?

30 May 2024

Linklaters

AI - Regulatory Landscape

Guillaume Couneson
Tanguy Van Overstraeten

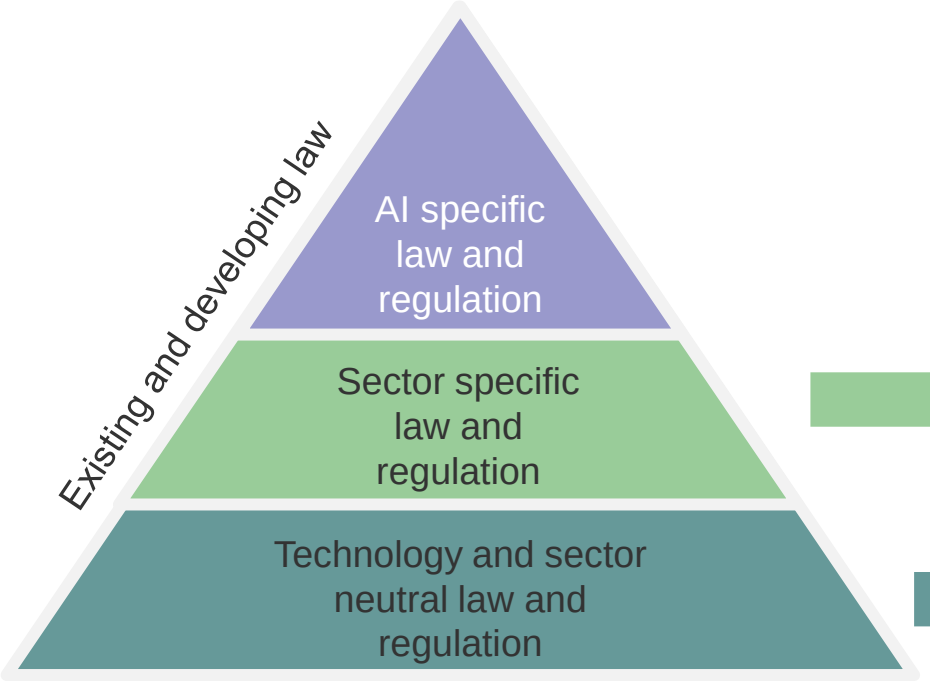
30 May 2024

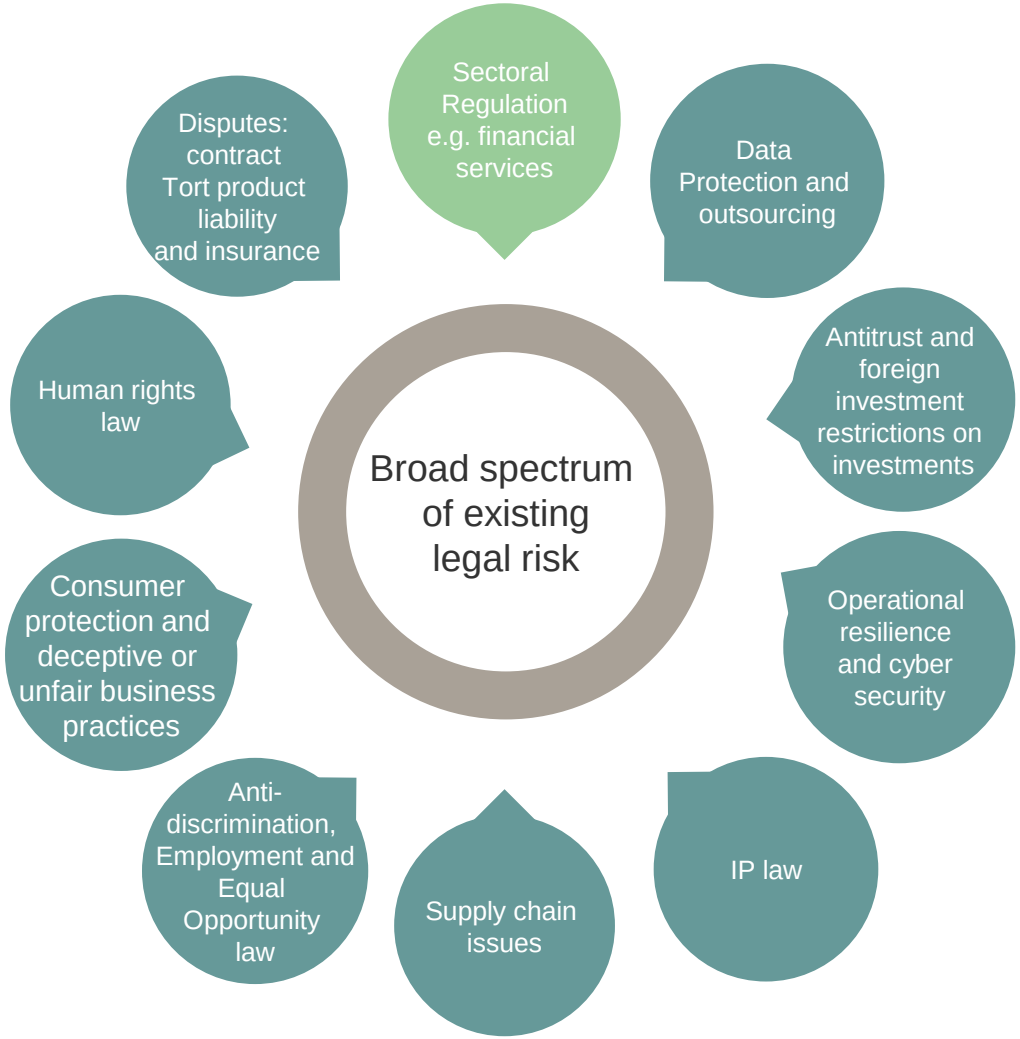
linklaters.com

Belgium-Japan Association
Chamber of Commerce
日白協会兼商工会議所

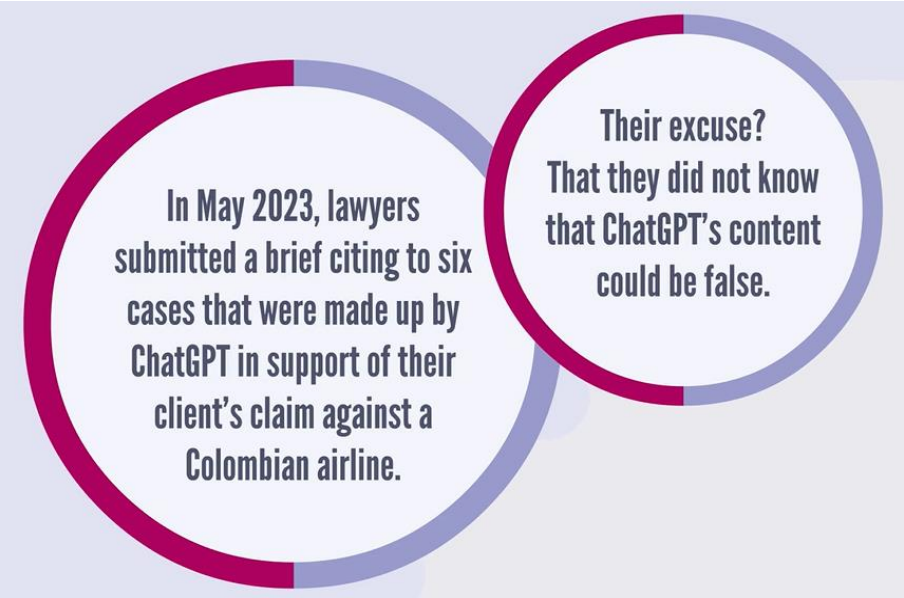
BJA

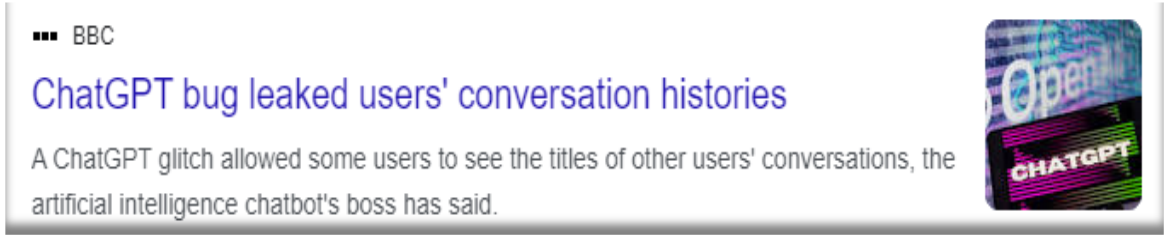
AI risks … the big picture





AI and related risks





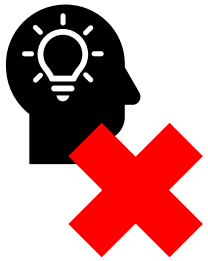
Pitfalls:

- Data protection
- Confidentiality
- Inaccuracies
- Hallucinations
- IP/copyright
- Bias and discrimination
- Etc.

AI and IP related risks

> GenAI models trained on large *data*sets
    > Training materials are frequently *original* works (copyrighted)
> Clash between AI developers and creative industries
> Ownership issues
> **Risk allocation** (developer vs user)

> *NB*: Copyright protects *expressions* of ideas, not ideas themselves



AI and IP risks

Input:

> **Risk of reproduction** of all or substantial part of copyrighted works (+ other IPRs) from materials on which AI tool was trained
  > The smaller the data set the higher the risk
  > *Illustration (Microsoft Copilot)*

Output:

> Right on generated content
  > Is it protected?
  > Who owns it?

September 7, 2023

Today, we announced the Microsoft Copilot Copyright Commitment, a new benefit that extends our existing intellectual property indemnity support to commercial Copilot services and builds on our previous AI Customer Commitments. Starting October 1, 2023, Microsoft is offering to defend customers from IP infringement claims arising from the customer's use and distribution of the output content generated by Microsoft's Copilot services. Specifically, should a third party sue a commercial customer for copyright infringement for using a Microsoft Copilot service or the output they generate, we will defend the customer and pay the amount of any adverse judgements or settlements that result from the lawsuit, as long as the customer used the guardrails and content filters we have built into our products.

Limitation of liability: AI input & output

Who could be liable?

> The person/entity conducting the infringing activity?

> Significant disclaimers and limitations of liability in AI T&Cs

OpenAI:

You are responsible for Content, including for ensuring that it does not violate any applicable law or these Terms.

(b) **Disclaimer.** THE SERVICES ARE PROVIDED "AS IS." EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS MAKE NO WARRANTIES (EXPRESS, IMPLIED, STATUTORY OR OTHERWISE) WITH RESPECT TO THE SERVICES, AND DISCLAIM ALL WARRANTIES INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, NON-INFRINGEMENT,

(c) **Limitations of Liability.**

... OUR AGGREGATE LIABILITY UNDER THESE TERMS SHALL NOT EXCEED THE GREATER OF THE AMOUNT YOU PAID FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE OR ONE HUNDRED DOLLARS ($100).

AI and Data

Legal

- Personal data protection (GDPR, …)
  - Data minimisation, purpose limitation, …
  - Anonymisation/pseudonymisation
  - Case law (*e.g. recent CJEU SCHUFA-case*)
- Data Governance: DGA, Data Act, Non-personal data regulation, …
- Transparency: technical limitations vs. legal requirements

Limits and risks

- AI only as good as the data it is trained on
- Quantity and quality
- Human in the loop?
- Data “cleaning”: intense on time and resources
- Transparency issues

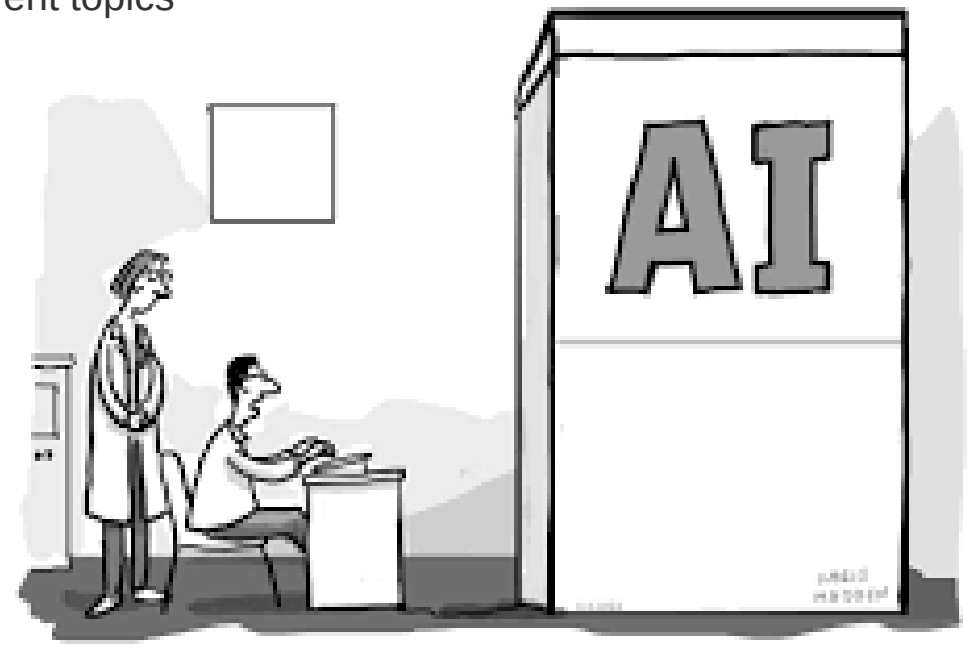
AI vs. Data Protection Authorities

What can a company do until the AI Act will be adopted?

- It seems like the GDPR is currently taking the strain as the “law of everything”
- The Italian DP regulator (Garante) banned ChatGPT:
  - Ban issued on an urgent basis on 30 March 2023
  - Service reinstated on 28 April 2023 after remedial measures by OpenAI
- The French DP regulator published guidelines on the training of artificial intelligence

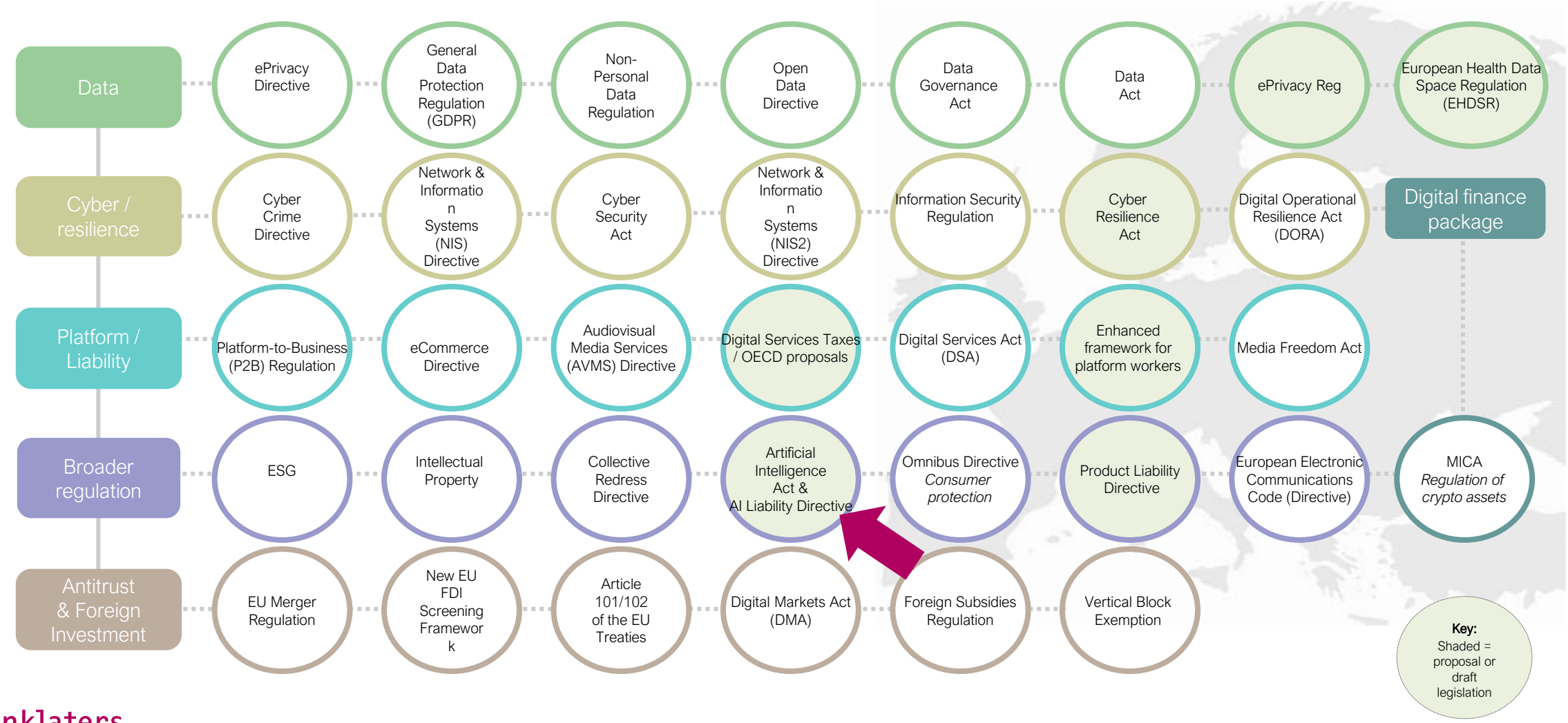
Systems while remaining GDPR compliant:

- Several sheets on different topics
- More sheets will follow



“We’ve got a problem. I’ve turned it on but I can’t turn it off again.”

European legislation



EU AI Act - Timeline

13 March 2024
EP vote

21 May 2024
Council vote

June 2024 (tbc)
OJ publication

OJ publication + 20 days
Entry into force

Entry into force + 6m (Q1 2025)
Banned practices

Entry into force + 9m (Q2 2025)
Adoption of codes of practices

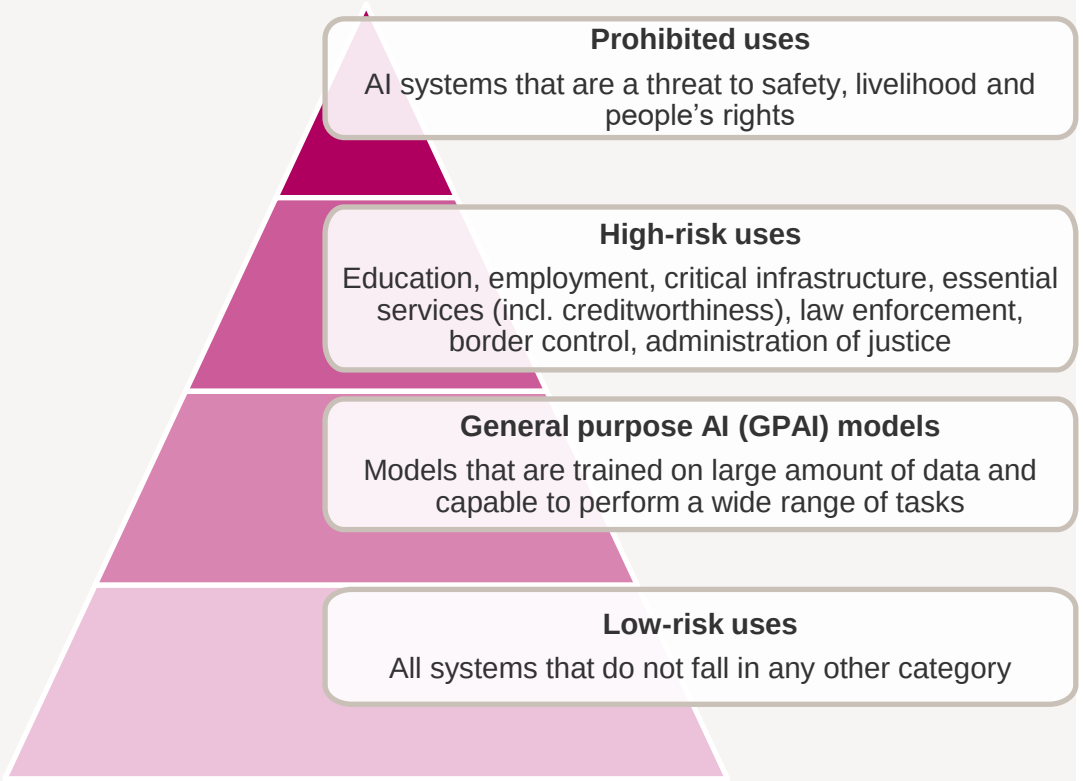
Entry into force + 1y (Q1 2026)
GPAI

Entry into force + 2y (Q1 2027)
Standalone High-Risk AI systems

Entry into force + 3y (Q1 2027)
Embedded High-Risk AI systems

The EU AI Act

Four tiers risk-based regulatory framework



Scope

- Definition of "AI system" aligned with the OECD
- Military, defence and R&D-only AI systems out of scope
- Exemption for free and open source (FOS) systems (unless high-risk)

Governance

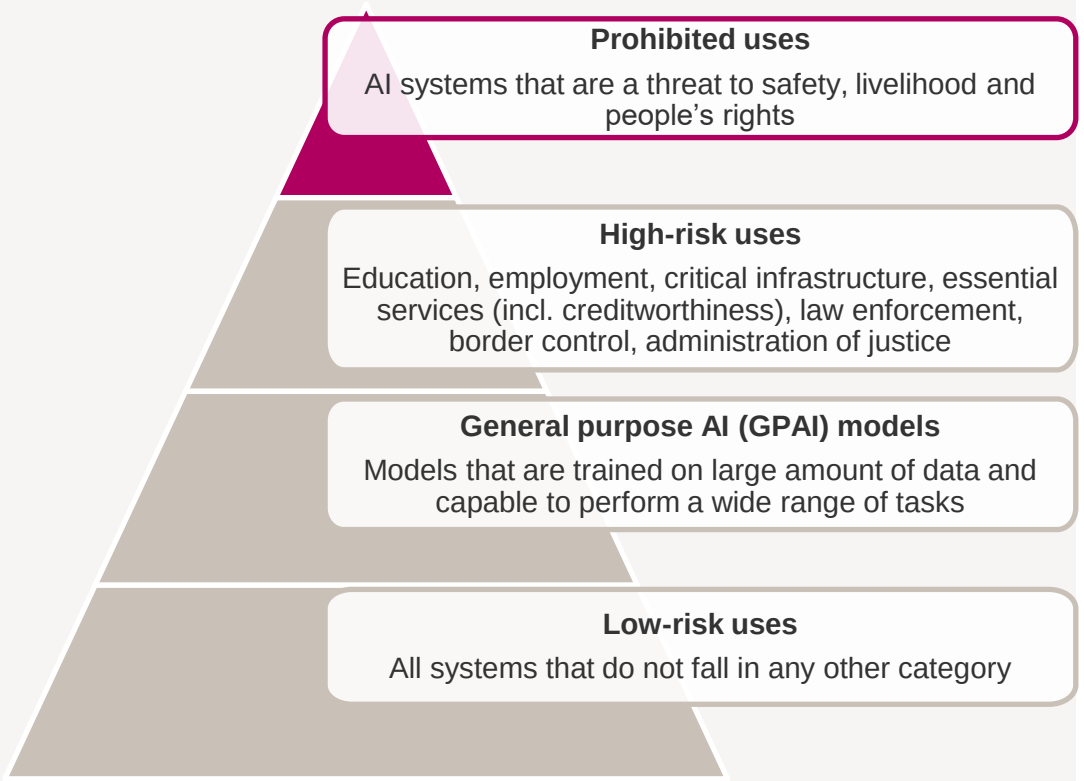
- New EU AI Office, within the EC, with a scientific panel of experts
- New AI Board with Member States' representatives
- New advisory body with industry, civil society, academia
- Member States to appoint national surveillance authorities and notifying authorities for 3rd-party conformity assessment

Fines

- Non-compliance with banned AI uses:
  - €35m or 7% of global turnover
- Non-compliance with other obligations:
  - max. €15m and/or 3% of global turnover

The EU AI Act

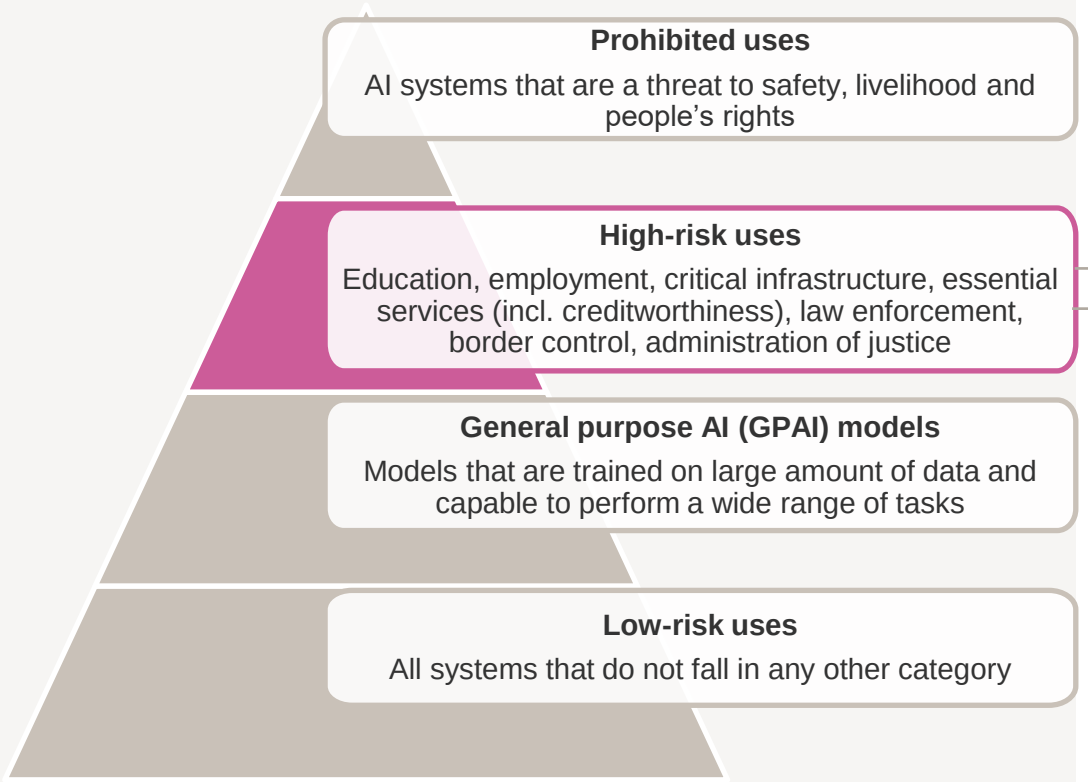
Four tiers risk-based regulatory framework



- Manipulative techniques
- Systems exploiting vulnerabilities
- Social scoring
- Untargeted facial scraping of CCTV
- Emotion recognition in workplace and education (with exception for safety reasons)
- Predictive policing
- Biometric categorisation based on sensitive characteristics (race, political orientations…)
- Real time remote biometric identification (RBI) in public spaces for law enforcement (with exception)
- Ex-post RBI (except for targeted search of a suspect).

The EU AI Act

Four tiers risk-based regulatory framework



An AI is high-risk if: (i) it is a safety component of a product covered by EU harmonised legislation and must undergo mandatory 3rd party conformity assessment; or (ii) is part of the list of high-risk use cases.

***Exemption**:* when the system (i) is intended to perform narrow procedural tasks; (ii) is intended to review or improve the result of human activity; (iii) is intended to detect decision-making patterns; (iv) performs a preparatory task for the assessment of one of the high-risk use cases.

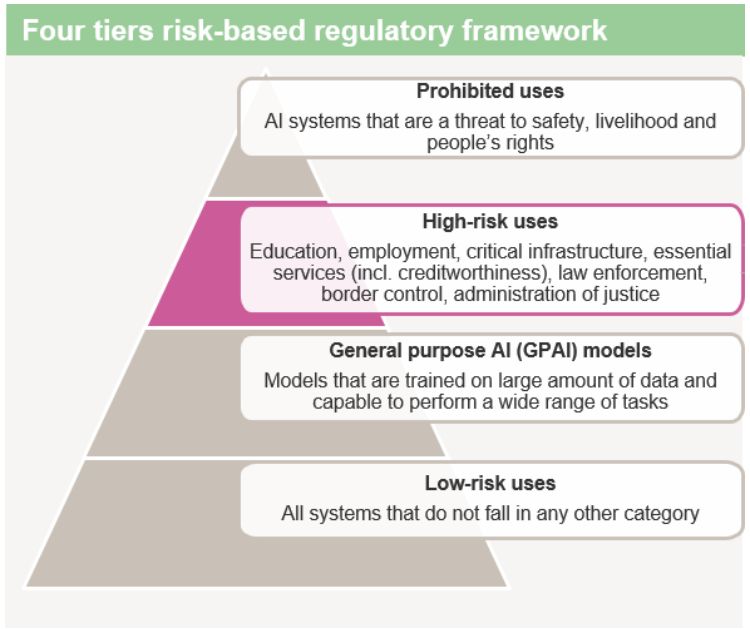
Model obligations: risk management, data governance, technical documentation, record-keeping, transparency, human oversight, cybersecurity.

Provider/importer obligations: Indication of trademark, quality management, provide access to AI's logs; registration into an EU database; conformity assessment based on internal procedure (if standards are available), or external procedure (if standards are not available).

Fundamental rights impact assessment for public bodies, providers of general interest services (hospitals), baking and insurance.

Sandbox: real world testing for 6+6 months maximum when approved by national surveillance authorities.

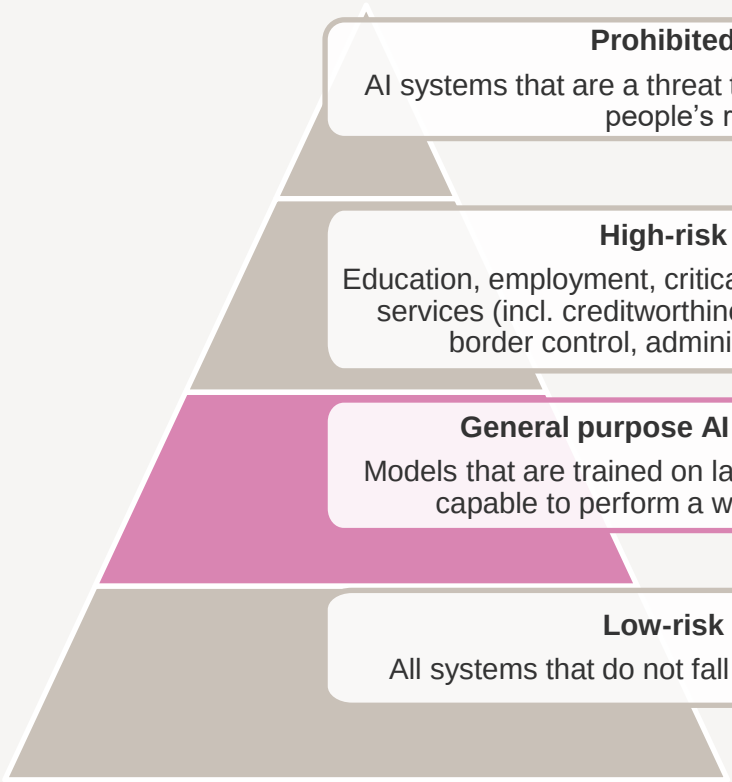
The EU AI Act



1. Register the system
2. Develop a risk management system
3. Use quality management system
4. Implement appropriate data governance
5. Maintain technical documentation
6. Keep log information
7. Human oversight
8. Accuracy, robustness and cybersecurity
9. Third party mandatory conformance assessment (CE marking) still under discussion

The EU AI Act

Four tiers risk-based regulatory framework



Prohibited uses

AI systems that are a threat to safety, livelihood and people's rights

High-risk uses

Education, employment, critical infrastructure, essential services (incl. creditworthiness), law enforcement, border control, administration of justice

General purpose AI (GPAI) models

Models that are trained on large amount of data and capable to perform a wide range of tasks

Low-risk uses

All systems that do not fall in any other category

Codes of practice: providers can demonstrate compliance by adhering to Codes of practice until harmonised standards are in place

Two-tiered approach: horizontal transparency obligations for all GPAI, with specific obligations for high-capacity, 'systemic risk' GPAI models.

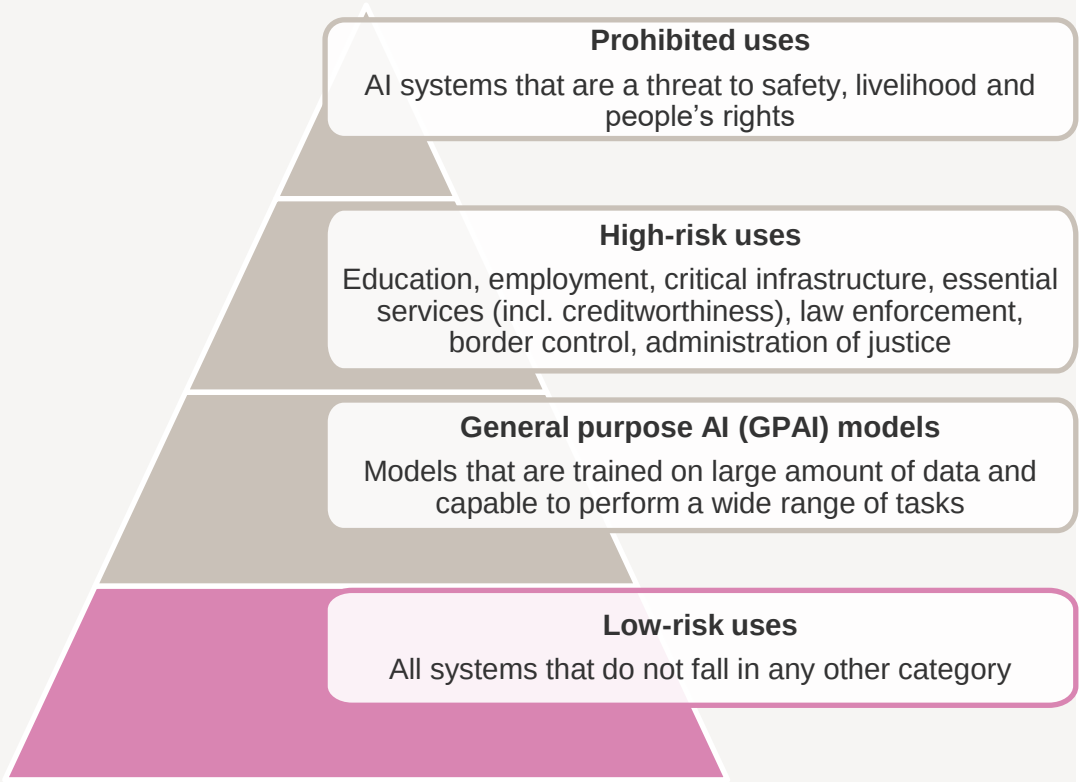
GPAI are systemic risk models when trained on >10~25 FLOPs; or can be designated ex-officio by the Commission or based on a recommendation from the AI Office's scientific board, based on business users and number of parameters. Rebuttal of designation is possible.

Horizontal obligations: technical documentation, respect of TDM opt-out under EU Copyright Directive (both policies and tech), collaboration with downstream deployers

Systemic risk obligation: cybersecurity, model evaluation and adversarial testing, risk mitigation, incident reporting to the AI Office

The EU AI Act

Four tiers risk-based regulatory framework



Transparency obligations in case of:

- Human interactions with AI
- Deepfakes

Potential roles under the AI Act

Provider

Develops AI systems or general purpose models

and

places them on EU market OR puts them into service under own name or trademark

Product Manufacturer

Embeds AI system in product under own name or trademark

Deployer

Uses an AI system under its authority

Importer

Places on the EU market AI system with name or trademark of person outside EU

Distributor

Person other than provider or importer making AI system available on EU market

Operator (generic name)
the provider, the user, the importer and the distributor

AI Liability Directive

AI Act

> Preventive scope = avoiding AI-related damage from occurring

A new rebuttable presumption of causality

AI Liability Directive

Specific rules on disclosure of evidence

> Issued end of September 2022
> Aimed at helping compensate those that have nonetheless suffered damage
> By ensuring that persons claiming compensation for damage caused by AI systems enjoy similar protection as those incurring damage from other products
> Only addresses non-contractual civil liability, not contractual or criminal liability
> Relies on definitions of AI Act
> Still subject to change!

Risk management

10 steps to risk management:

Other typical obligations:

- Model evaluation and adversarial testing
- Data governance
- Transparency and technical documentation
- Record-keeping and reporting
- Human oversight
- Accuracy and quality management
- Cybersecurity

Examples of common compliance elements

1	2	3	4	5
Registers	**Risk assessments**	**Governance**	**Notifications**	**Contracting**
ROPA (GDPR), asset management (NIS2), inventory (DORA), list of use cases (AIA)	DPIA (GDPR), risk assessments (NIS2/DORA/AIA)	DPO (GDPR), Board (NIS2/DORA), Quality management system (AIA)	Data breach notification (GDPR), (serious) incidents reporting (NIS2/DORA/AIA)	DPAs (GDPR), supply chain (NIS2), ICT third-party service providers (DORA), model contracts (AIA)

Your Speakers

Guillaume Couneson

Partner, Data, Cyber and Digital, Brussels

Tel: +32 494 36 48 36
guillaume.couneson@linklaters.com

Tanguy Van Overstraeten

Partner, Data, Cyber and Digital, Brussels

Tel: +32 478 40 15 69
tanguy.van_overstraeten@linklaters.com

Questions?

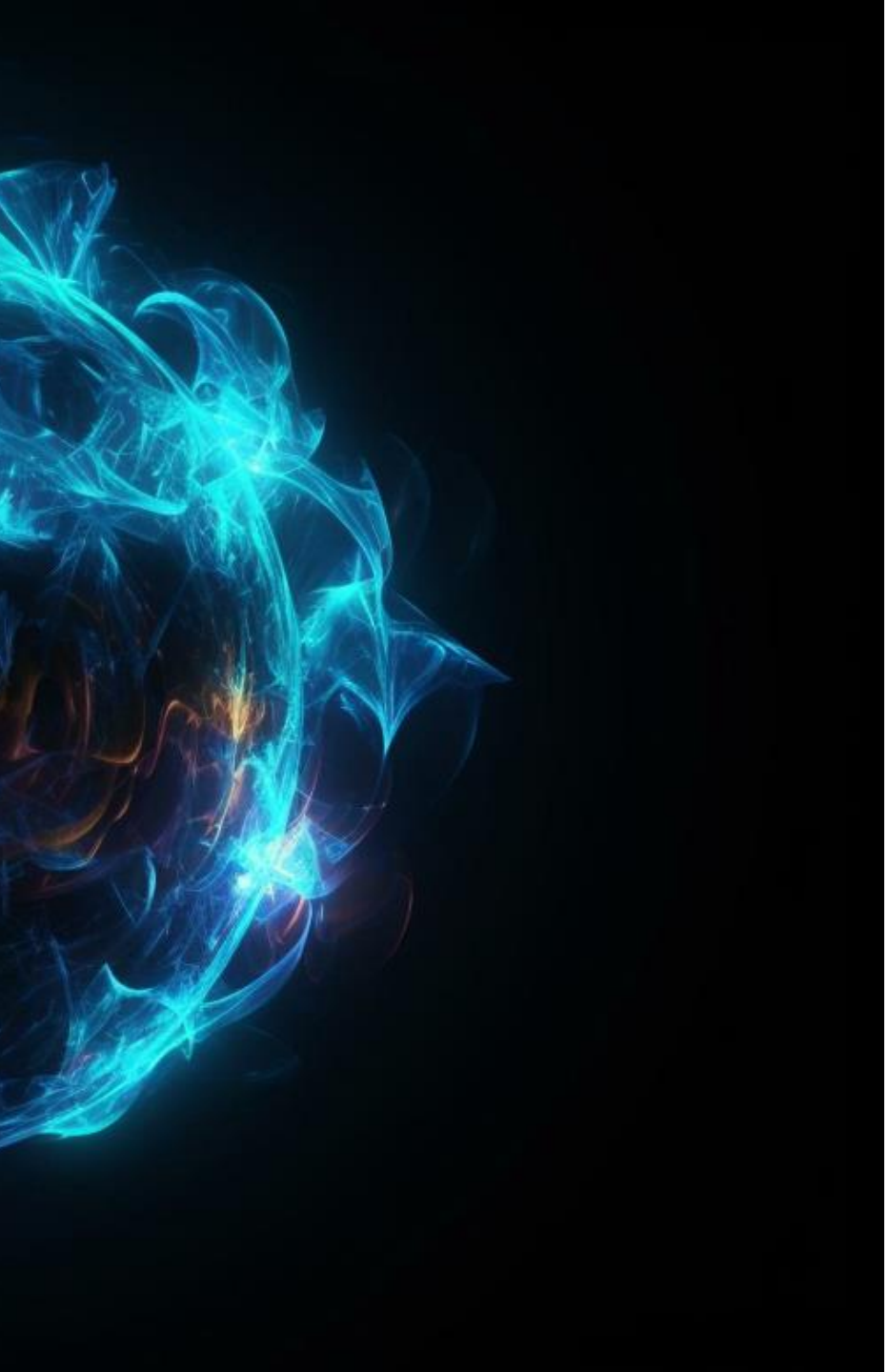
Linklaters LLP

Rue Brederode 13
B - 1000 Brussels
Belgium
Tel: +32 2 501 94 11
Fax: +32 2 501 94 94
www.linklaters.com

Deloitte.

BJA event: ready for the EU AI Act

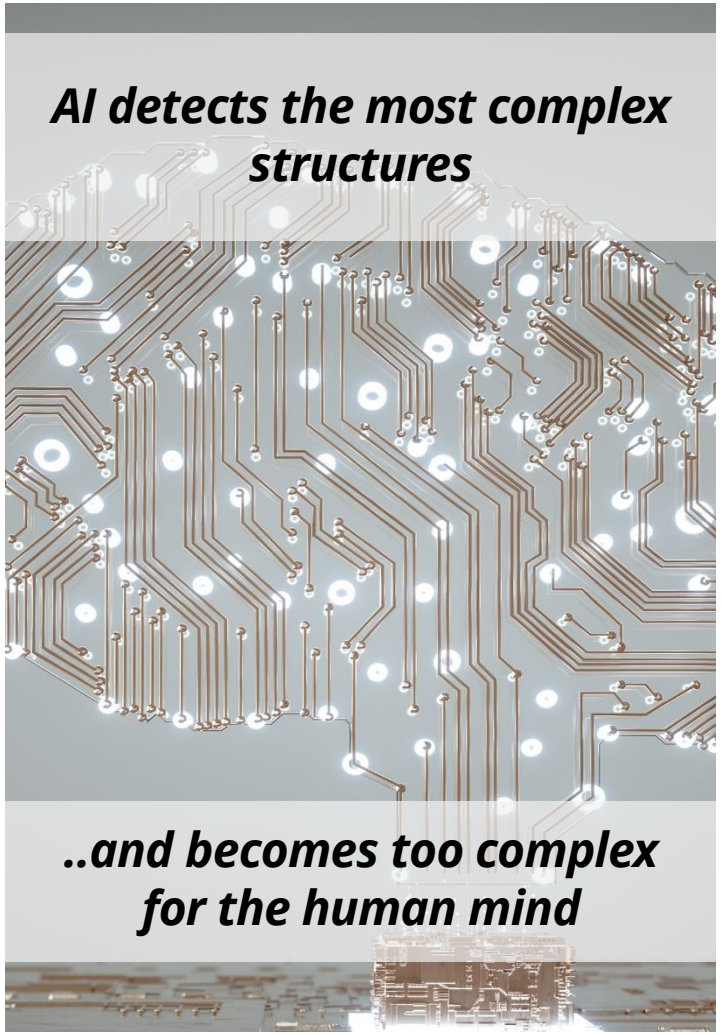
30 May, 2024

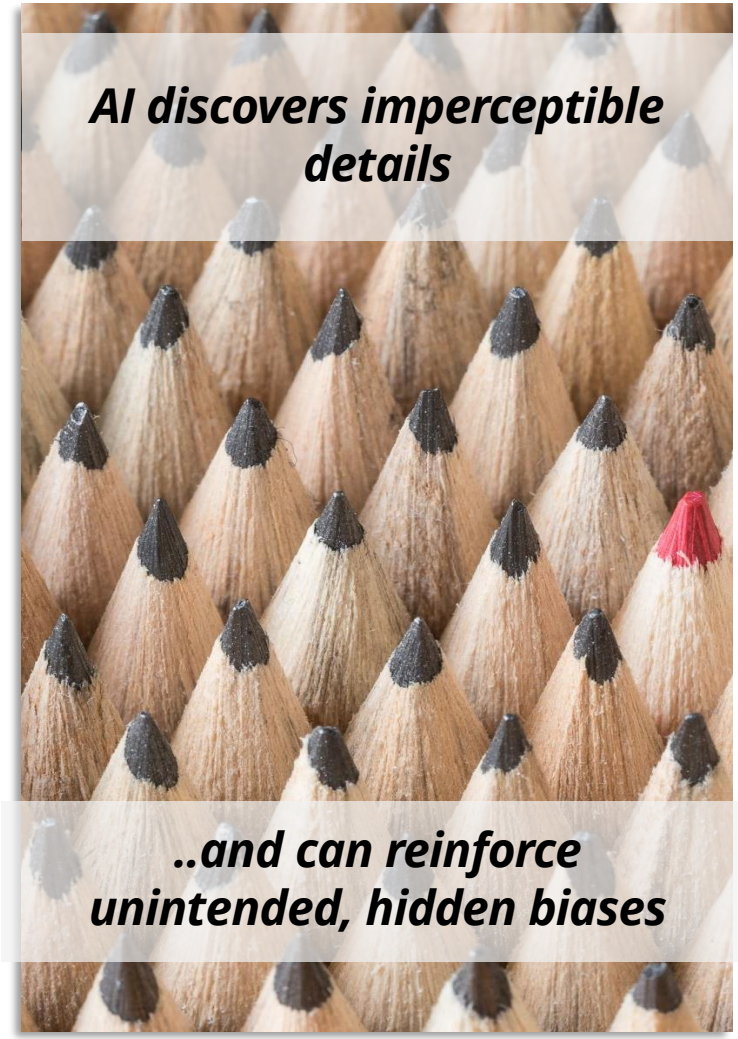


Our Agenda for today

1	**Applying AI: Benefits & Risks**
2	**Lessons learned from practical cases**

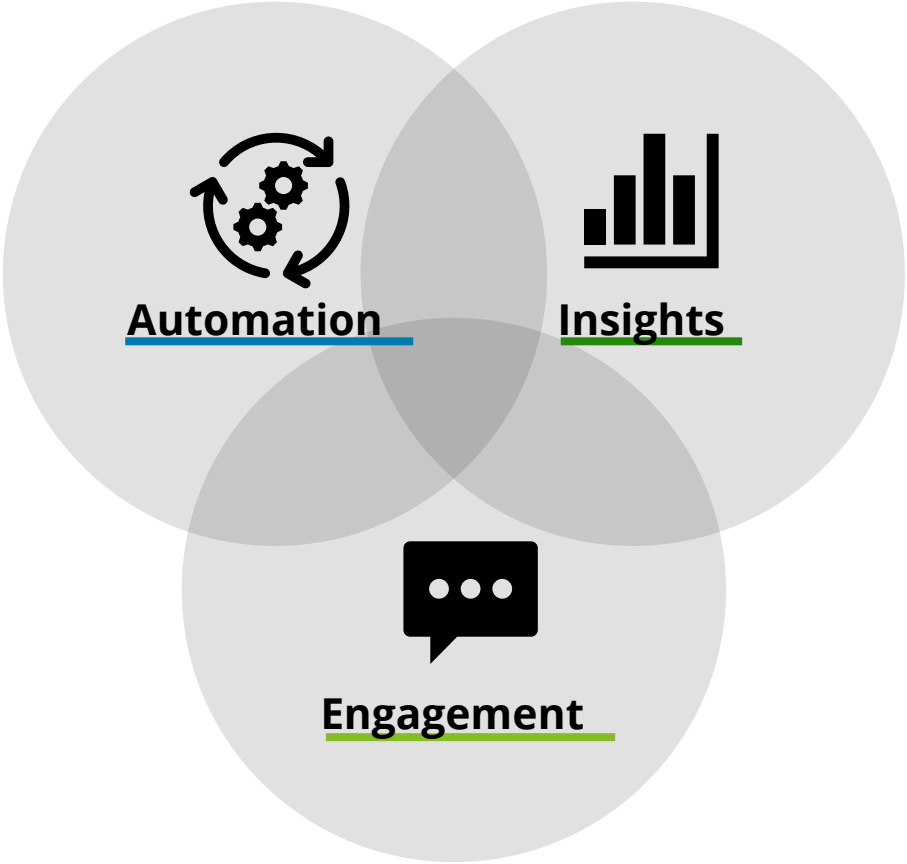
Nature of AI comes with benefits and risks





Value creation with AI…

AI can help surpass previously imagined value creation opportunities, by generating value across three key levers



Automation

Computerize processes, workflow, and decisions

- Perform repetitive tasks
- Structure tasks neatly
- Autocomplete tasks
- Always monitor
- Resolve instantly
- …

Insights

Reveal insights that improve speed and quality of decision-making

- Know what happened
- Identify patterns
- Compare and optimize
- Predict what might be
- Discover what sticks out
- …

Engagement

Create attractive and human-like digital interactions

- Chat with your data
- Respond personally to all
- Answer dull questions
- Reply more empathetic
- Provide instant facts
- …

… with a trustworthy code of conduct

Inaccuracy | Bias | IP Violation | Privacy | Unethical Use

Fair/Impartial

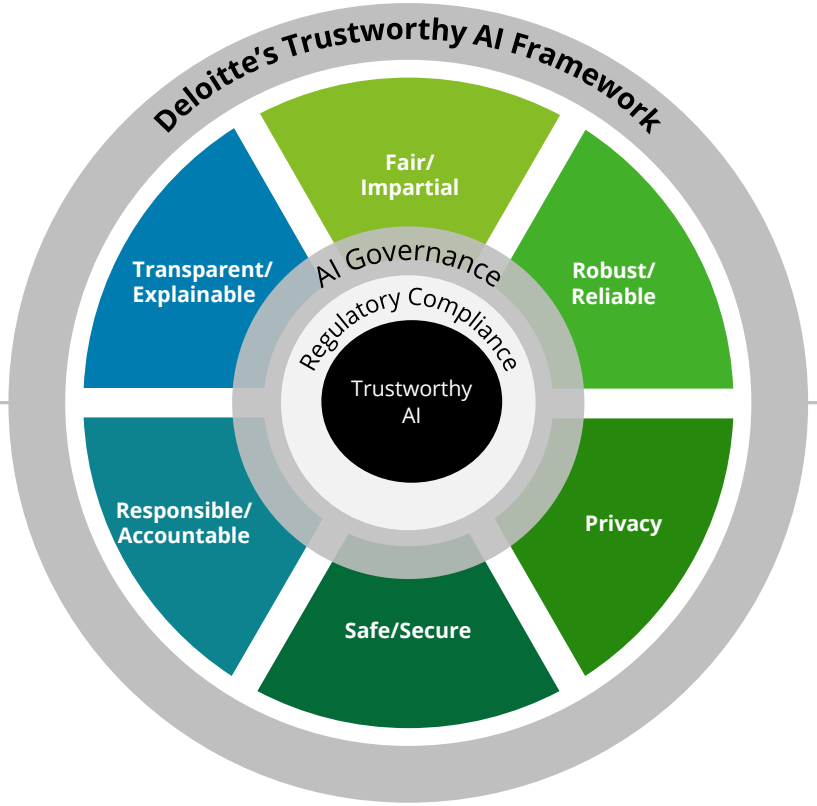
AI applications include internal and external checks to help ensure equitable application across all participants

Transparent/Explainable

All participants are able to understand how their data is being used and how AI systems make decisions; algorithms, attributes, and correlations are open to inspection

Responsible/Accountable

Policies are in place to determine who is held responsible for the output of AI system decisions



Robust/Reliable

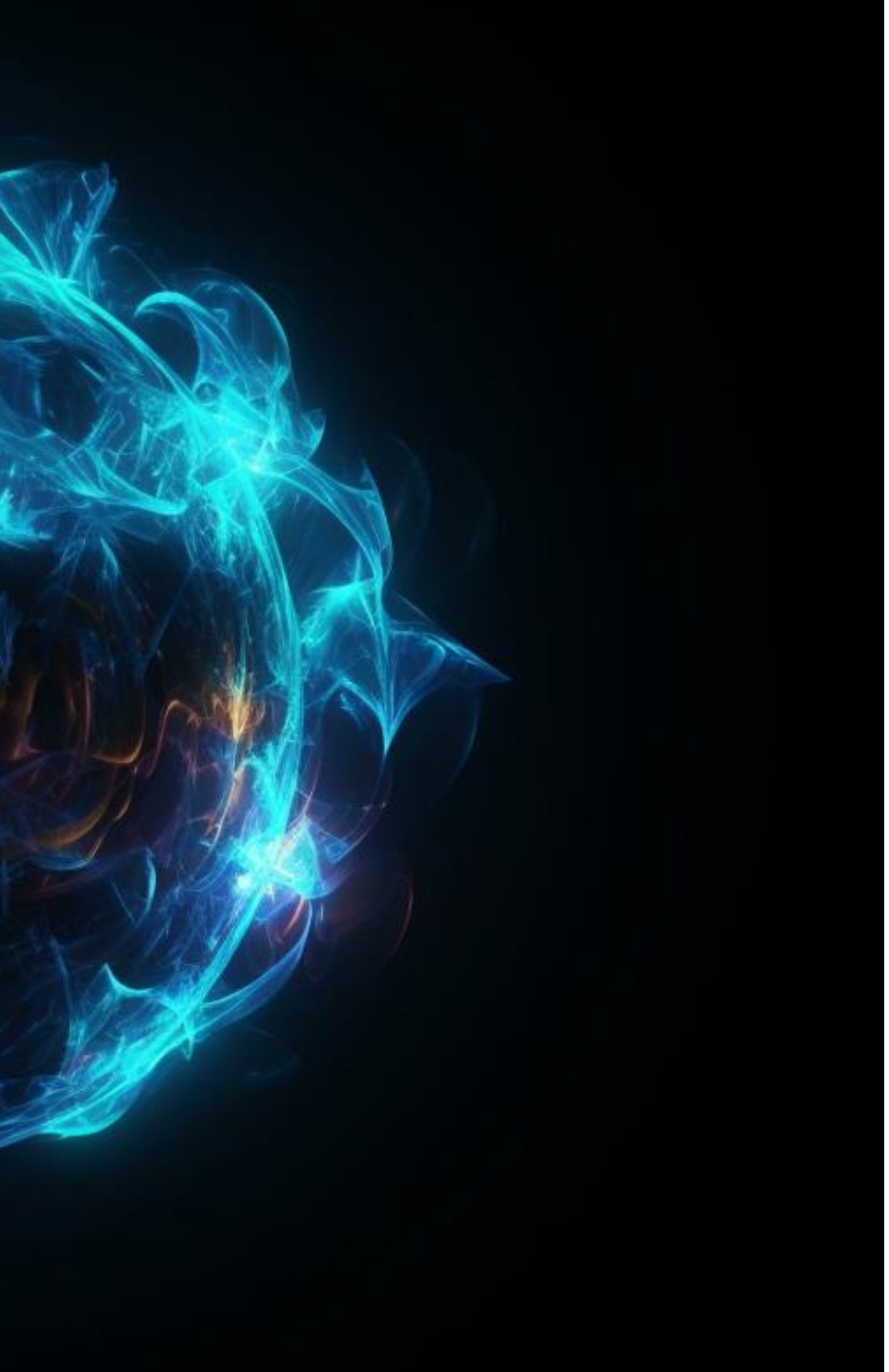
AI systems have the ability to learn from humans and other systems and produce consistent and reliable outputs

Privacy

Consumer privacy is respected, and customer data is not used beyond its intended and stated use; consumers are able to opt in/out of sharing their data

Safe/Secure

AI systems can be protected from risks (including Cyber) that may cause physical and/or digital harm



Use Case:

How to generate new revenue streams with AI?

Monetizing your AI investments starts by addressing a customer need or pain point

PRINTING EQUIPMENT MANUFACTURER

- Add-on AI services package:
  - making the customer equipment more efficient
  - extending machine lifetime

- Benefit sharing commercial model

MEDICAL DEVICE MANUFACTURER

- Stand-alone AI software module
- Improving medical analysis and decision-making process

- Separate license fee based on benefits and willingness-to-pay

WATER CHEMICALS PROCESS MANUFACTURER

- Total solution offering, with integrated AI capabilities
- Real-time monitoring and steering of dosage to minimize chemicals usage

- Integrated it unit price / kg

FERTILIZER PRODUCER

- Dedicated digital app for end users
- Supporting tool for precision farming to maximize benefits from product usage

- Free of charge app for top segment customers

Companies with commercial AI success have addressed the following business challenges in the right way

PRINTING EQUIPMENT MANUFACTURER

MEDICAL DEVICE MANUFACTURER

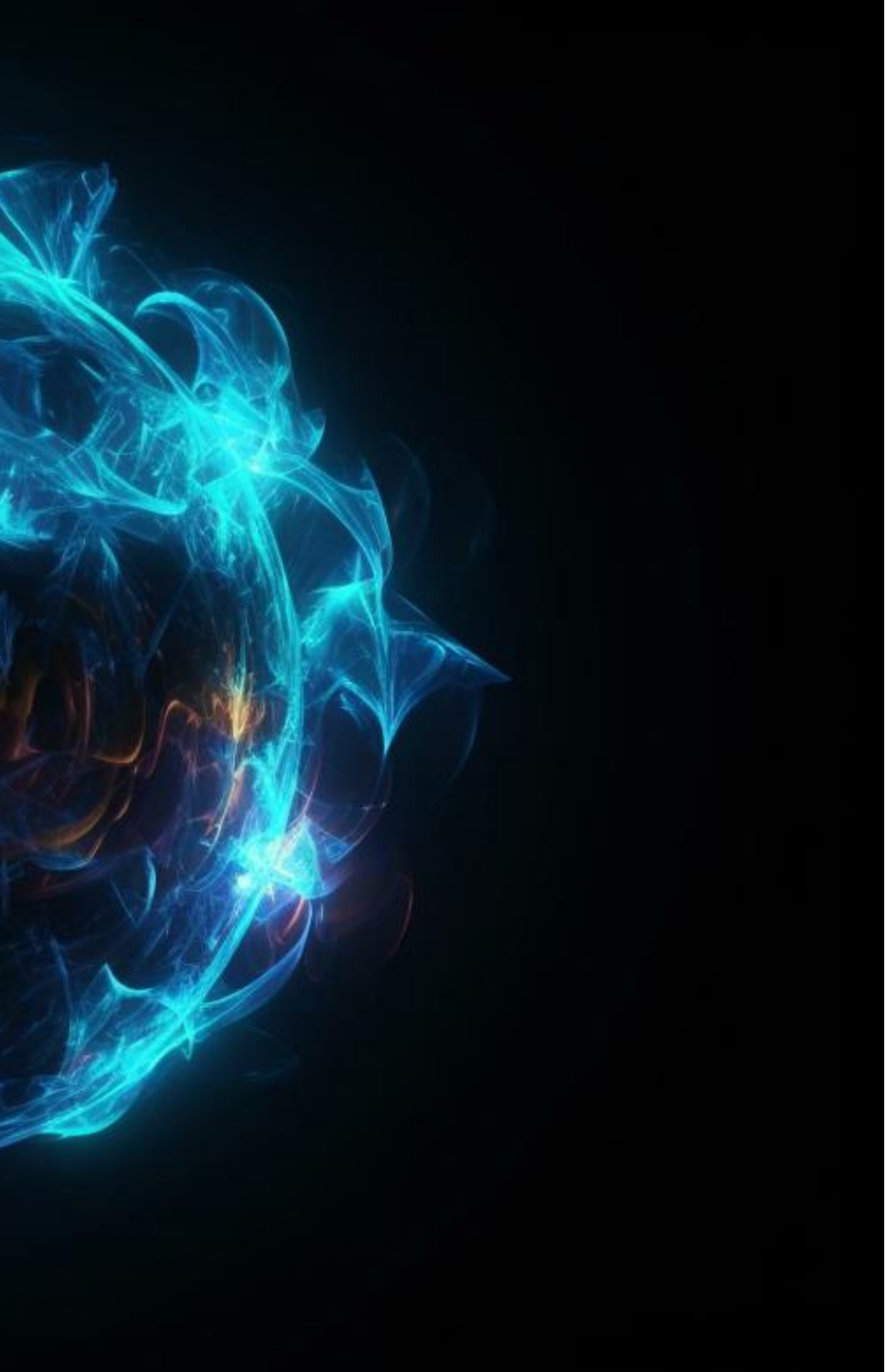
WATER CHEMICALS PROCESS MANUFACTURER

FERTILIZER PRODUCER

Selecting the right pricing model

Installing effective customer data feedback loops

Incremental improvement of your value proposition



Use Case:

How to boost my company’s effectiveness and efficiency with (gen)AI?

We defined how AI can bring value to our Deloitte organization

1 Service Delivery Transformation

Re-define work across our Businesses and Service Delivery to create AI value

- Understand GenAI impact
- Transform services for faster speed to value
- Accelerate QR compliance for GenAI deployment

2 Market Activation

Launch new Generative AI assets, services and solutions in the market

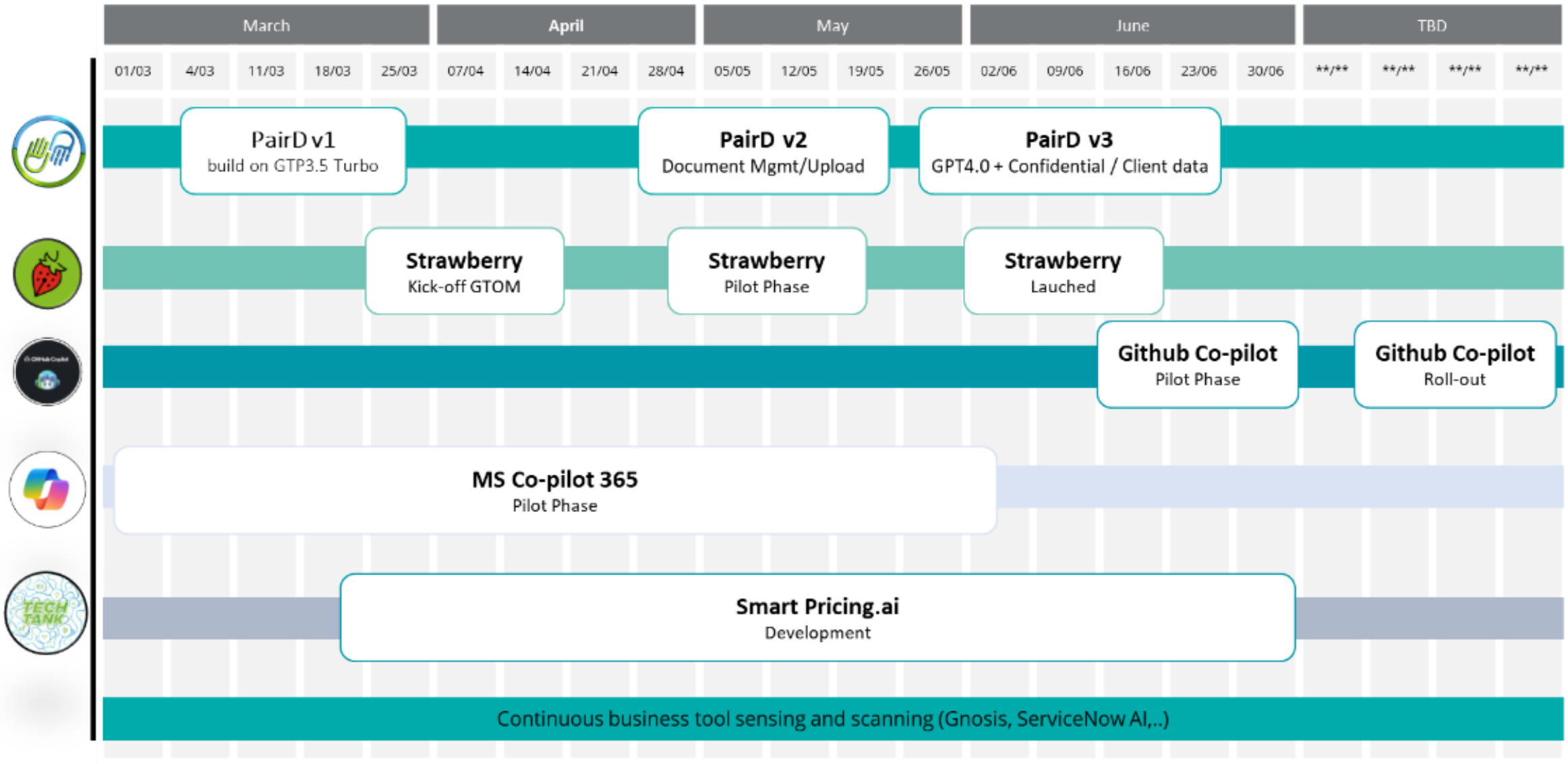
- Create GenAI Fluency and activate our people as AI ambassadors
- Launch the Belgian chapter of the GenAI Institute
- Activate our existing Growthplatforms in collaboration with our Alliance Partners

3 Innovation

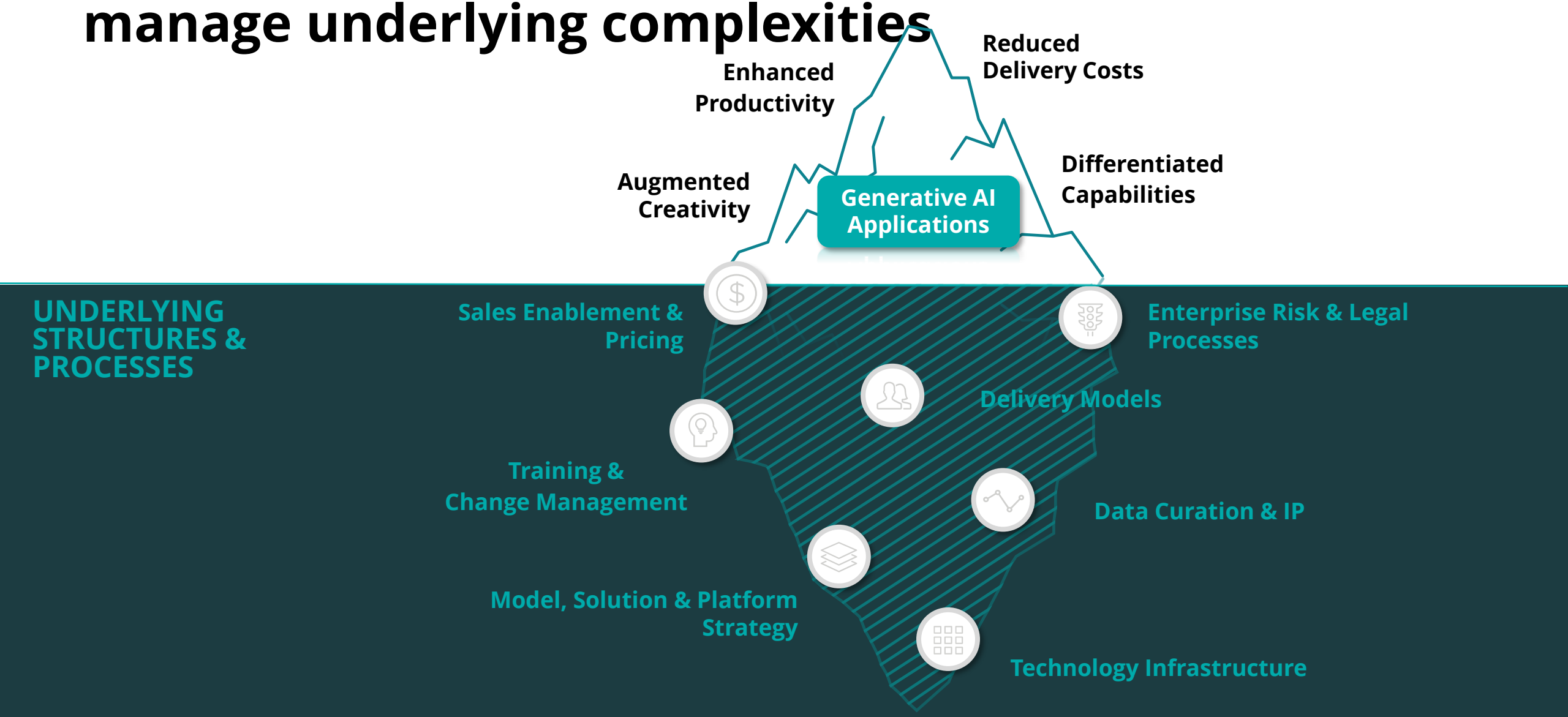
Shape new businesses in emerging markets with Generative AI

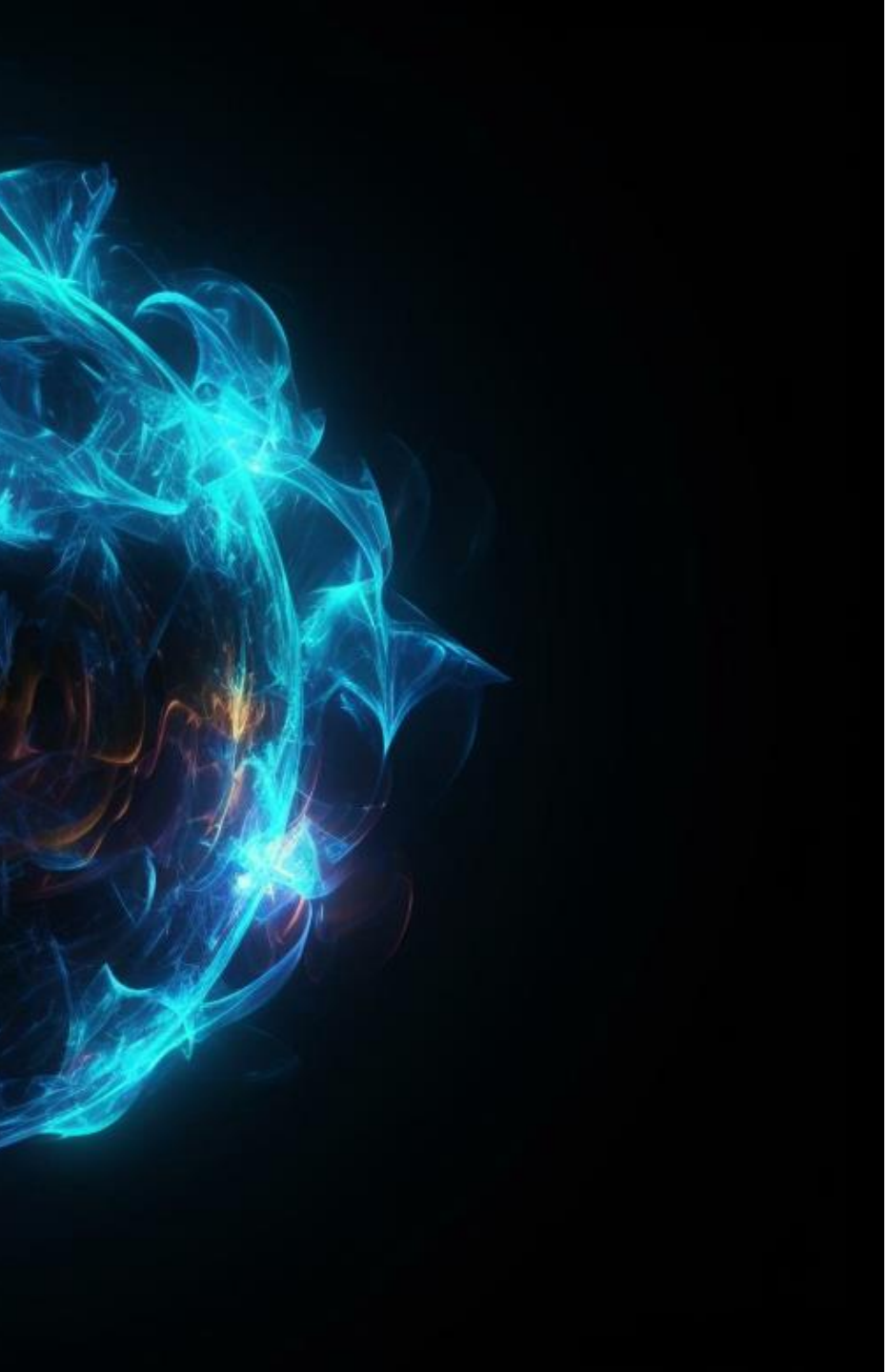
- Build GenAI driven architecture and infrastructure
- Build assets to support new AI driven services and business models
- Collaborate with the Global GenAI Innovation network

Launch of GenAI tools at Deloitte



To scale our transformation with GenAI, one must manage underlying complexities



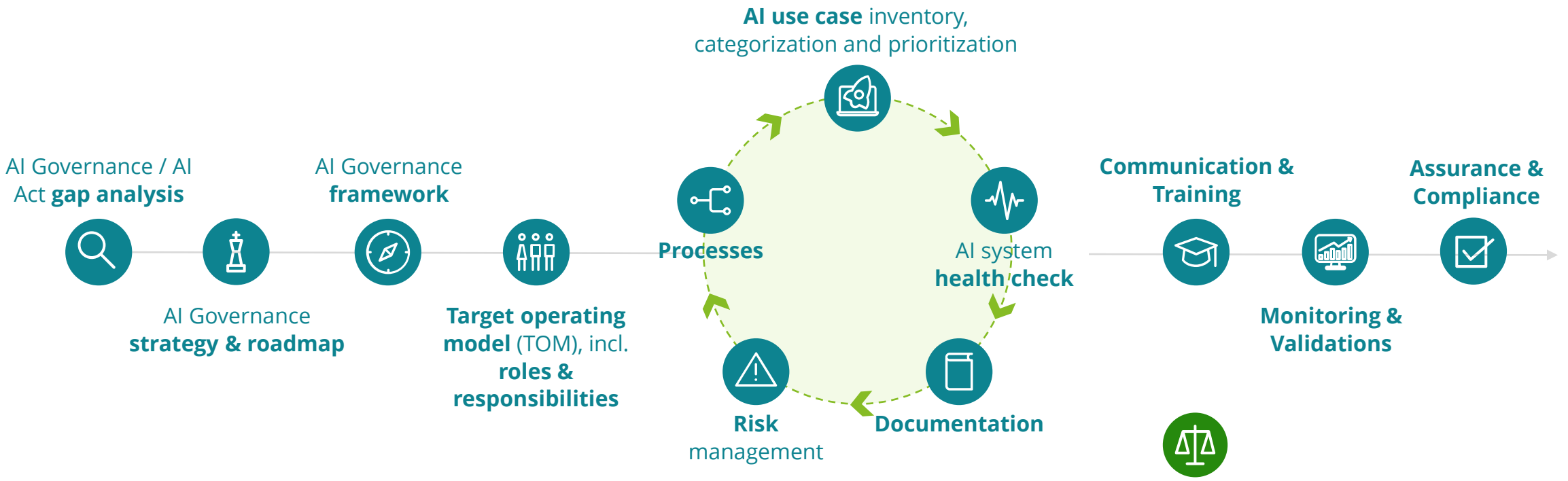


Use Case:

How to ensure we roll out trustworthy AI solutions and be compliant with regulation?

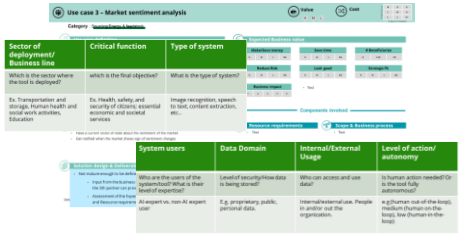
The EU AI act requires organizations to get more structured around their AI initiatives

AI brings forth a **multitude of business, technical and social challenges**

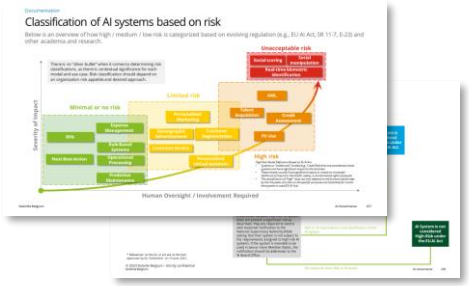


Incl. **legal advisory services** on the AI Act application, regulatory risk categorization and compliance justification

A structured approach to identify and classify AI models



AI system inventory



AI Act risk classification

AI use case inventory, categorization and prioritization

AI Governance / AI Act **gap analysis**

AI Governance **framework**

AI Governance **strategy & roadmap**

Target operating model (TOM), incl. **roles & responsibilities**

Processes

AI system **health check**

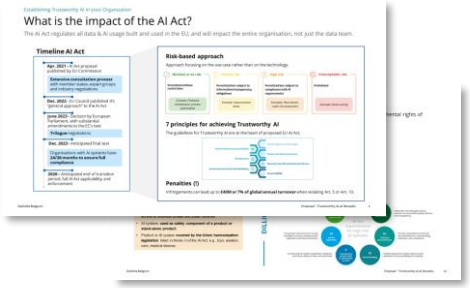
Risk management

Documentation

Communication & Training

Monitoring & Validations

Assurance & Compliance



AI governance model and RACI

Incl. **legal advisory services** on the AI Act application, regulatory risk categorization and compliance justification

Contact:

Kristof Boodts, Senior Director, Deloitte Consulting & Advisory

kboodts@DELOITTE.com