Deloitte.

Technology & Digital Risk

Operational Risk Technology & Digital Risk

Clients. Consistency. Community. Collaboration.

Artificial Intelligence Act

About the regulation of Artificial Intelligence

2024

Deloitte Hungary

Context and objectives of the AI Act

The AI Act **lays down a legislative framework** to address artificial intelligence (AI) in the future to stimulate innovation and mitigate risks.

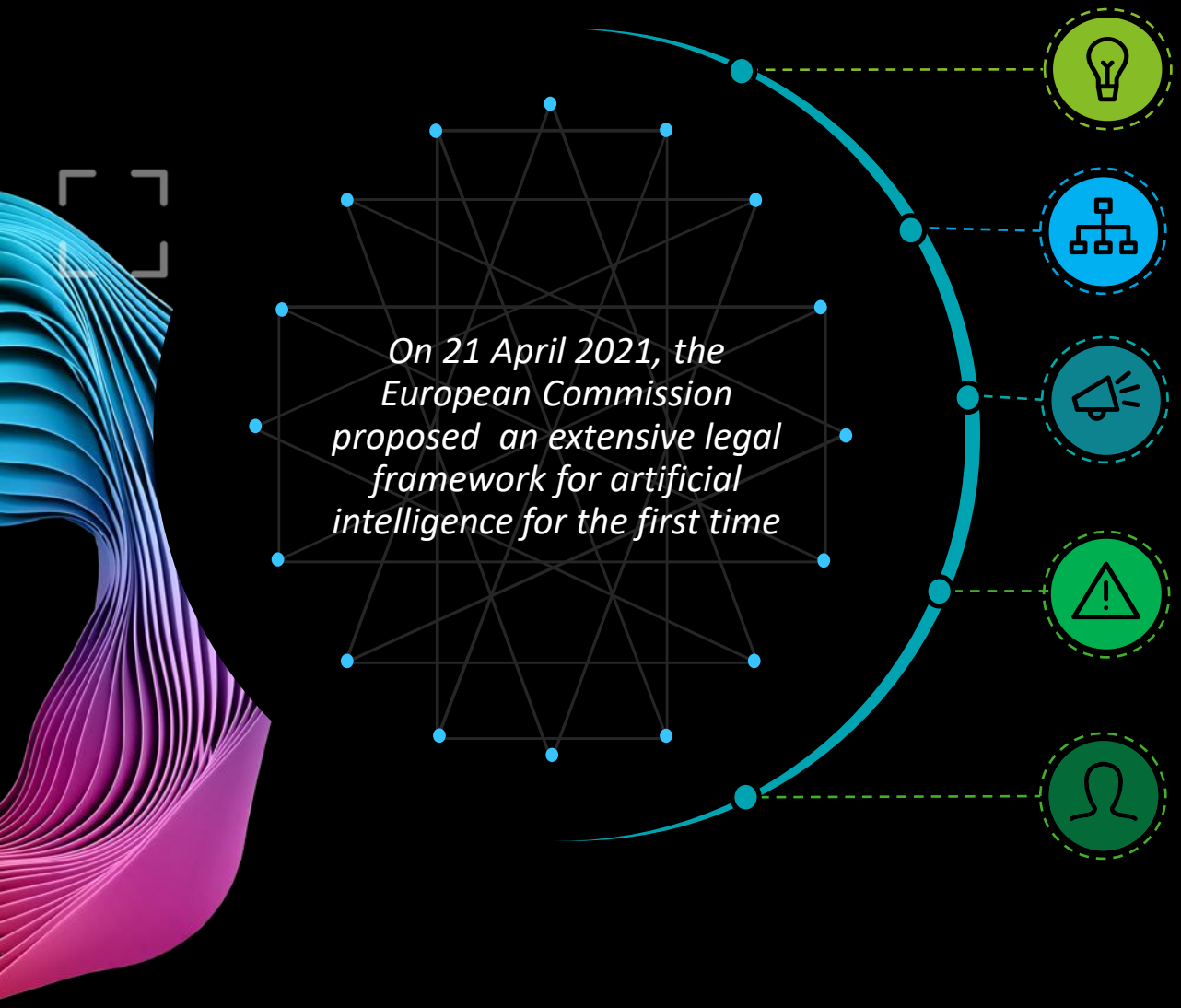
What is it about?

1. Transparent promotion of European values, emphasizing the **ethical use** of artificial intelligence.
2. Validation of the **quality** of the AI system when defining processes and roles, as well as during the entire life cycle.
3. Promoting cooperation between EU member states and a **level playing field**, as well as protecting the fundamental rights of EU citizens in the age of artificial intelligence.

What is the purpose?

- Ensuring that AI systems marketed and used in the EU are safe and respect existing legislation on fundamental rights and EU values. Non-compliance can mean an administrative fine of up to EUR 35 million!
- Creating legal certainty to promote investments in artificial intelligence and innovation involving artificial intelligence.
- Improving governance and effective enforcement of existing legislation on fundamental rights and security requirements for AI systems.
- Facilitate the development of the single market for legitimate, safe and trustworthy AI applications and prevent market fragmentation.

The AI Act
The regulation defines harmonized rules for artificial intelligence



What is the focus?
- Using a human-centered, risk-based approach to classifying AI-based systems

Who does it apply to?
- For providers, users, importers and distributors of AI systems within the European Union

When will it be applicable?
- From the beginning of 2027 (some provisions will be applicable already in 2024)

Why is it important to focus on it?
- It may occur that the companies already use AI solutions
- The non-compliance may result in a fine of **35 million EUR** or **7%** of the company's total worldwide annual turnover for the preceding financial year

What can we do?
- Raise awareness of the affected parties
- Preparation and developing competences within the organisation

Legal definition of AI

‘**Artificial Intelligence system**’ (AI system) means machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, 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.

‘general purpose AI model’ means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market;

‚general-purpose AI system’ means an AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems

The classification of artificial intelligence systems

The AI Act uses a risk-based approach to differentiate between four types of AI systems based on their potential for hazards and risk.

1 - Unacceptable Risk AI Systems

The following AI practices are prohibited:

- Manipulation of human behavior, opinions and decisions
- Classification of people based on their social behavior
- Real-time remote biometric identification (with certain exceptions)

2 - High Risk AI Systems

High-risk AI systems are defined in the regulation as:

- Products subject to EU product safety regulations
- A list of stand-alone high-risk AI systems identified in the act, such as AI systems that assess individuals' creditworthiness or are used in recruitment.

3 - AI with specific transparency obligations

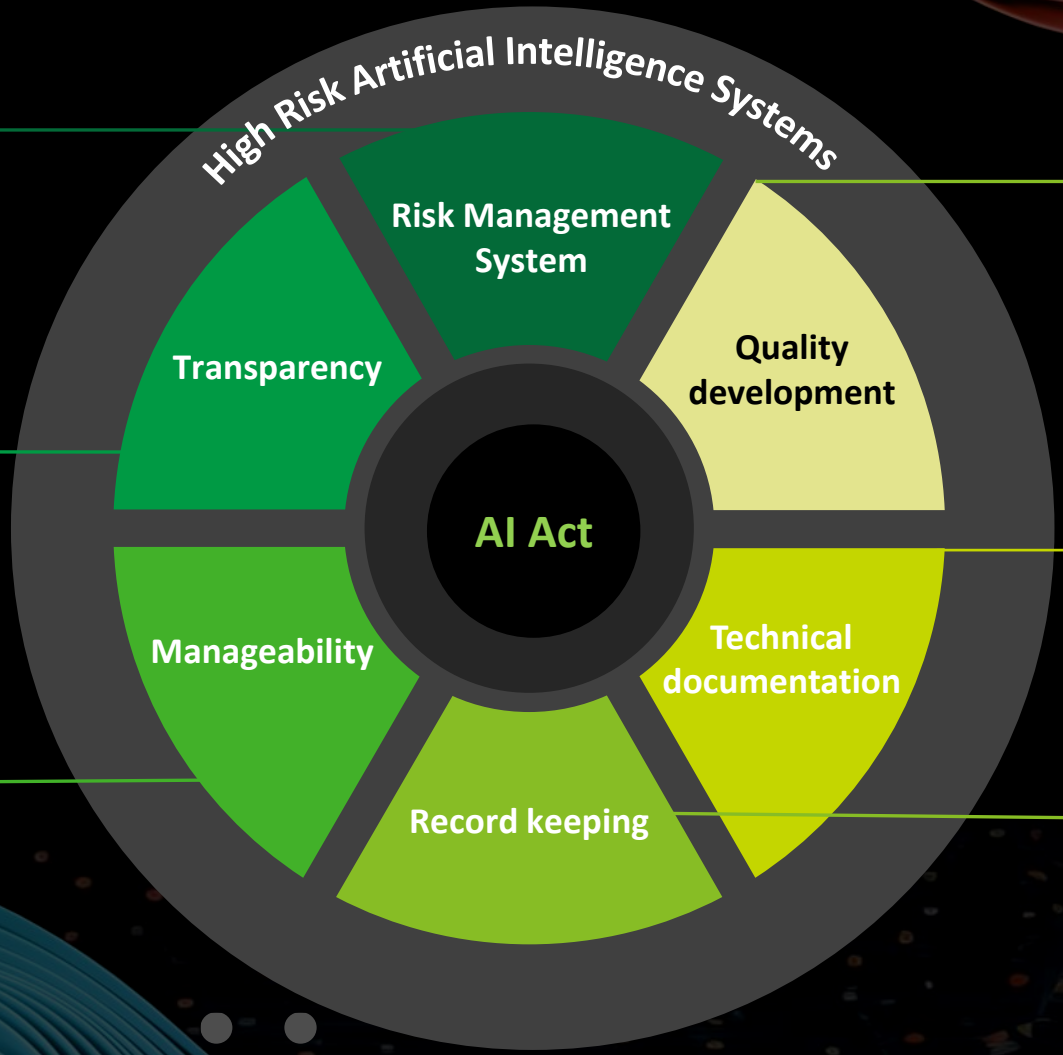
Some systems (such as chatbots) can deceive users who may think they are talking to a natural person. In those cases, the regulation only lays down transparency requirements to ensure that the person concerned is aware that they are communicating with an AI application on the other side.

4 - Minimal or no Risk AI Systems

Systems with minimal risk to humans are permitted without restriction, such as capacity forecasting, production planning, etc.

High Risk Artificial Intelligence Systems

High-risk AI systems must meet the following requirements:



Designed and developed to achieve the appropriate level of accuracy, stability and cyber security for their intended purpose and perform consistently throughout their entire life cycle.

All stakeholders are able to understand how their data is used and how AI systems make decisions about it. Algorithms, attributes and correlations are open for inspection.

It shall be designed and developed in such a way that their operation is transparent enough to allow users to interpret the output of the system and use it properly

Systems using techniques involving training models with data need to be developed based on training, validation, and testing datasets that meet defined quality criteria.

The technical documentation (operation, monitoring, risk management, etc.) must be prepared and kept up-to-date before the system is placed on the market or put into operation.

Designed and developed with capabilities that enable automatic recording of events while in operation. The logging capabilities must comply with recognized standards and industry practices.

Sanctions

1

Non-compliance with the **prohibition of the AI practices**

35M€

OR 7%

of its total worldwide annual turnover for the preceding financial year, whichever is higher

2

The infringement of the other provisions of the AI Act (list)

15 M€

OR 3%

of its total worldwide annual turnover for the preceding financial year, whichever is higher

3

The supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities

7,5M€

OR 1%

of its total worldwide annual turnover for the preceding financial year, whichever is higher

Steps Towards Compliance for AI Service Providers

Conduct a close examination of your existing assets and find out which ones use AI or qualify as AI under the new regulation

Determine potential risks (which potential risks (e.g. unacceptable, high or low risks)

Ensure design, development and quality management system are in compliance with the AI regulation

High risk AI systems must undergo a specified conformity assessment and must repeat this step if they are substantially modified

Write a Declaration of conformity for each (high risk) AI system and affix the CE marking

Placing the high-risk AI system on the market or into service

A high-risk AI system requires continuous monitoring

Are you ready?

Responsibility and ethical use

- The Act focuses on ethical application of AI,
- The practitioners are accountable for upholding stringent quality standards.

Strict control of applications

- It specifically highlights high risk applications and prescribes extensive disclosure accompanied by rigorous controls to ensure AI systems are robust & reliable.

Transparency, supervision

- Even for applications deemed lower risk, the Artificial Intelligence Act demands that AI systems are sufficiently transparent , alerting subjects to processing by AI, and that they are explainable enabling their designers to monitor them effectively.

Impartiality, fairness

- The Act includes general principles of fair & impartial treatment of subjects (regardless of the AI application),
- In addition, explicitly forbids certain apps (technologies that pose a clear threat to humans, e.g. "social scoring" by governments, exploitation of children's vulnerabilities, techniques that are not consciously perceptible, are therefore banned.).

Human oversight

- To ensure safe & secure operation of AI, the regulation demands human oversight, the ability to assume control or override the AI.

Protection of human rights

- The Act is grounded in the fundamental rights of the citizen, guarding against exploitation of vulnerabilities, ensuring due process, defending the rights of children, among others.
- It preserves privacy by outright forbidding applications of AI for the live, remote surveillance of citizens.

How can Deloitte help?

Preparation of GAP analysis and implementation of legal requirements

With our artificial intelligence, technological and legal experts, we evaluate organizational processes and solutions in detail and prepare an action plan to achieve legal requirements, which our implementation project team efficiently delivers with the client's needs in mind.

Perform GAP analysis	Preparation of compliance action plan	Implementation support	Introduction of controls and tools	Preparation of policies, guidelines and operational procedures

Risk analysis

Innovative risk management services created by organizational digitization, which are typically valid for the entire data and system life cycle.

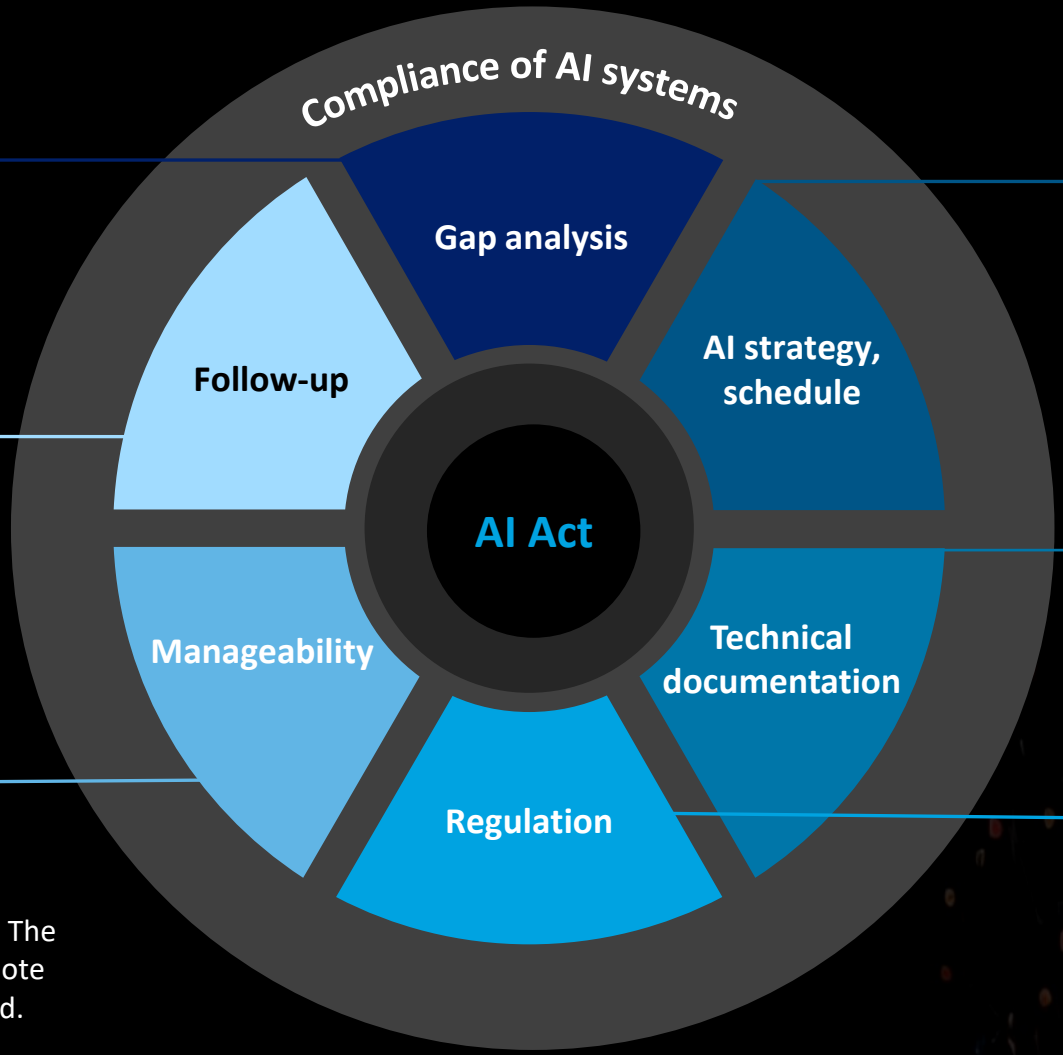
Development of a methodology for risk assessment and management	Preparation of risk analysis	Identify new risks	Action plan development for risk assessment	Supporting the implementation of risk management actions

Artificial intelligence consulting

Robotization and artificial intelligence offer new opportunities for transforming business processes. We support our clients to develop and apply the right AI strategy.

Development of AI strategy and roadmap Preparing	Development of processes for Data governance and Data management	Quality assurance of an AI implementation project	System development and integration	Implementation of emerging technologies: 5G, IoT, Cloud

AI Act - compliance



We prepare an action plan to facilitate achieving the legislative requirements. The plan will be efficiently delivered by our implementation project team and in line with client needs.

Together with our artificial intelligence experts, technology specialists and legal consultants, we thoroughly evaluate organisational processes and solutions

Ensuring compliance with requirements imposed regarding high-risk AI systems

- Liabilities towards the authorities
- Inspection of unfair contract terms
- Fundamental rights impact assessment
- Reporting serious unexpected incidents and malfunctions

Preparing internal regulatory framework

Individual providers of AI systems, their representative organisations or both entities may establish codes of conduct. The purpose of a code of conduct is to promote compliance with the obligations imposed.

Why is it recommended start preparing now?

Design

The design of the AI system is in line with the provisions of the AI Act

Development

During the development phase, the requirements of the act will be implemented

AI systems

An adequate AI system will be developed

Legal compliance

- By the end of the preparation period, a legally compliant AI system will be in place
- There is no need to re-examine and redesign the already developed, established AI system in order to have a compliant solution
- Time and cost efficiency

Deloitte's Trustworthy AI™ framework helps manage and govern the risks of AI

Rooted in our Risk, Audit and Assurance heritage, Trustworthy AI™ helps responsibly harness the power of AI for the benefit of shareholders, our clients and society at large

Where ethical issues arise

Organization

Data

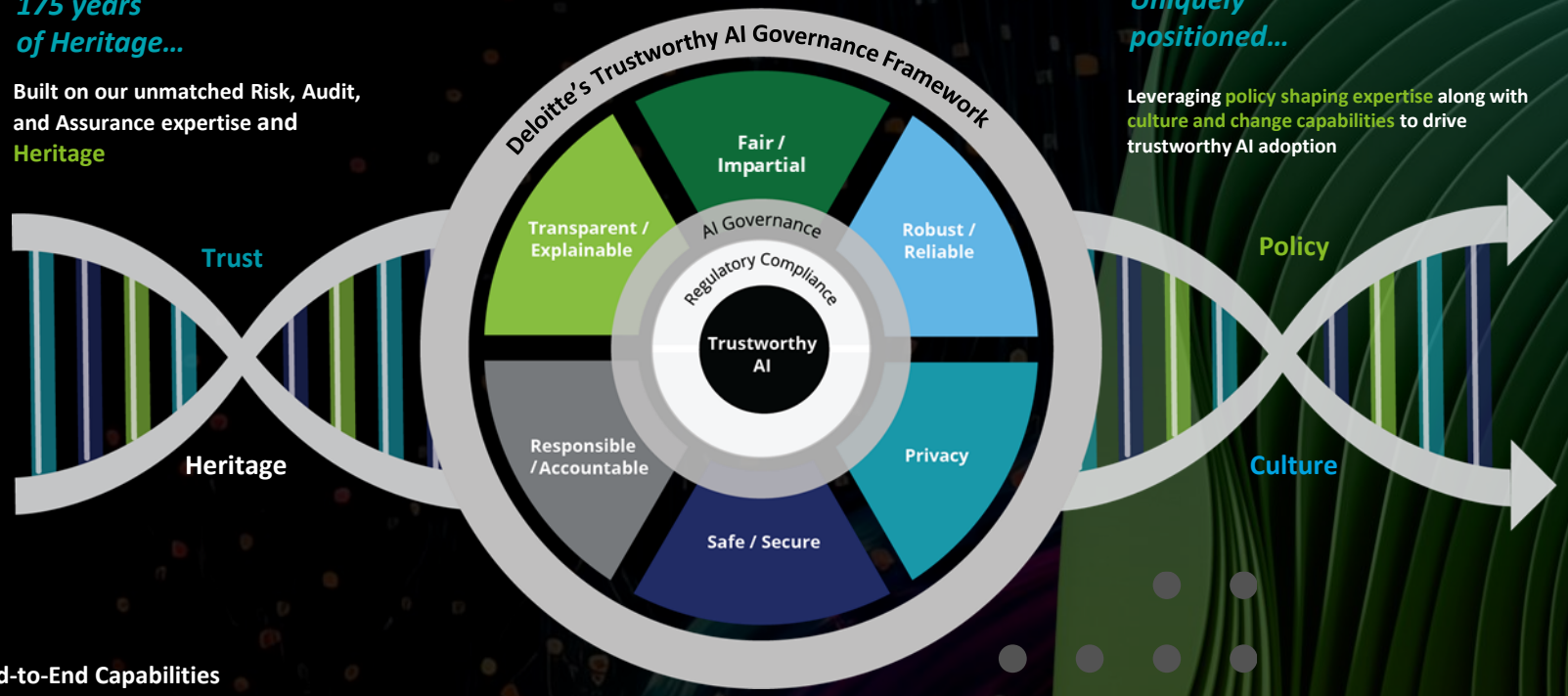
Algorithms

175 years of Heritage...

Built on our unmatched Risk, Audit, and Assurance expertise and Heritage

Uniquely positioned...

Leveraging policy shaping expertise along with culture and change capabilities to drive trustworthy AI adoption



End-to-End Capabilities

- AI Ethics and Strategy
- AI Governance
- AI Risk Management
- AI Testing
- Algorithm Assurance

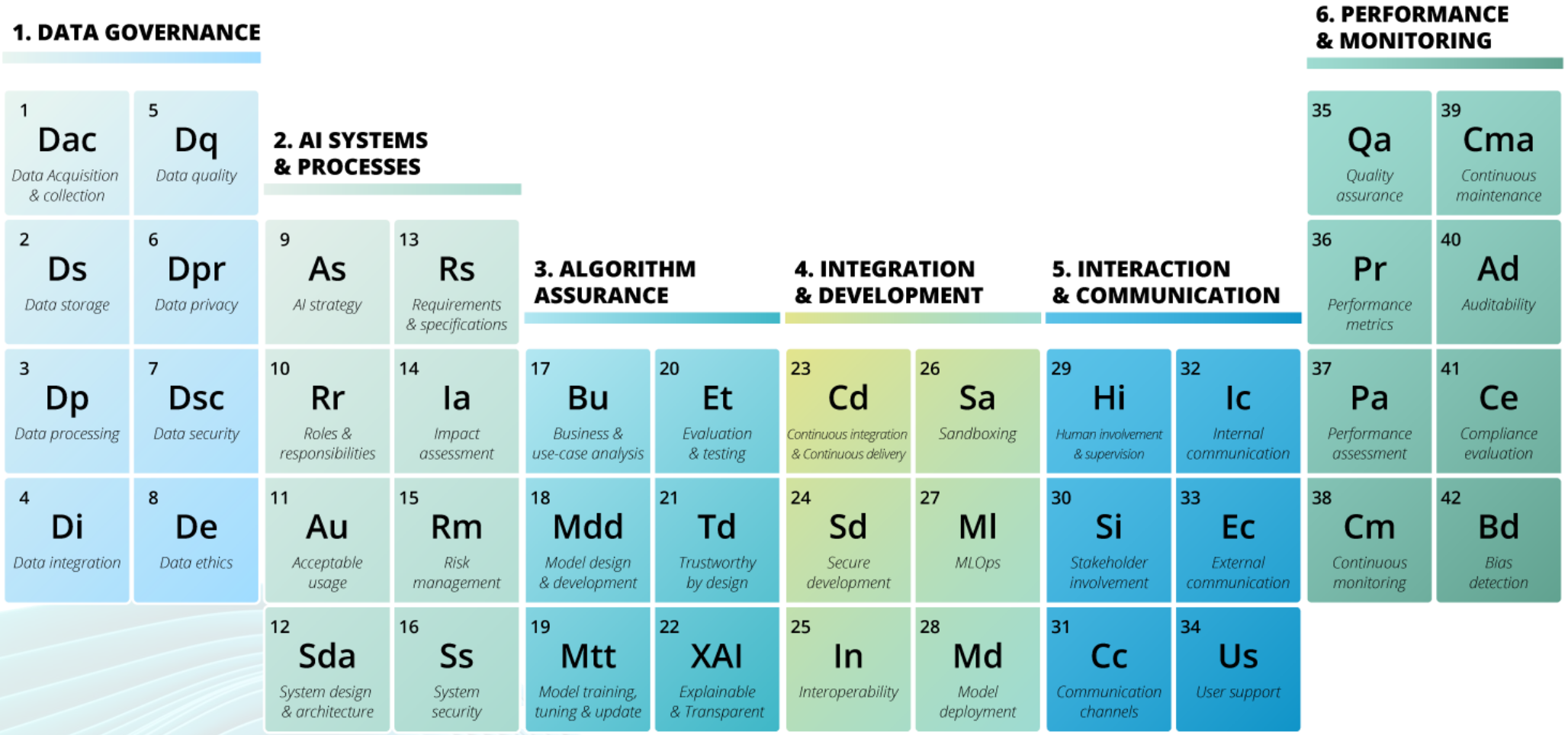
Culture, Change, and Organizational Design

Benefits of Trustworthy AI™

- Increased brand equity and trust leading to **new customers** and **employee retention**
- Increased likelihood that customers **opt in** to share their data creating a **valuable dataset**
- Increased revenue / reduced costs through more **accurate decision making** due to better data sources
- **Reduced cost from legal** and remediation activities
- **Positive impact on society** due to increased equality (e.g., lower carbon admissions from ridesharing)

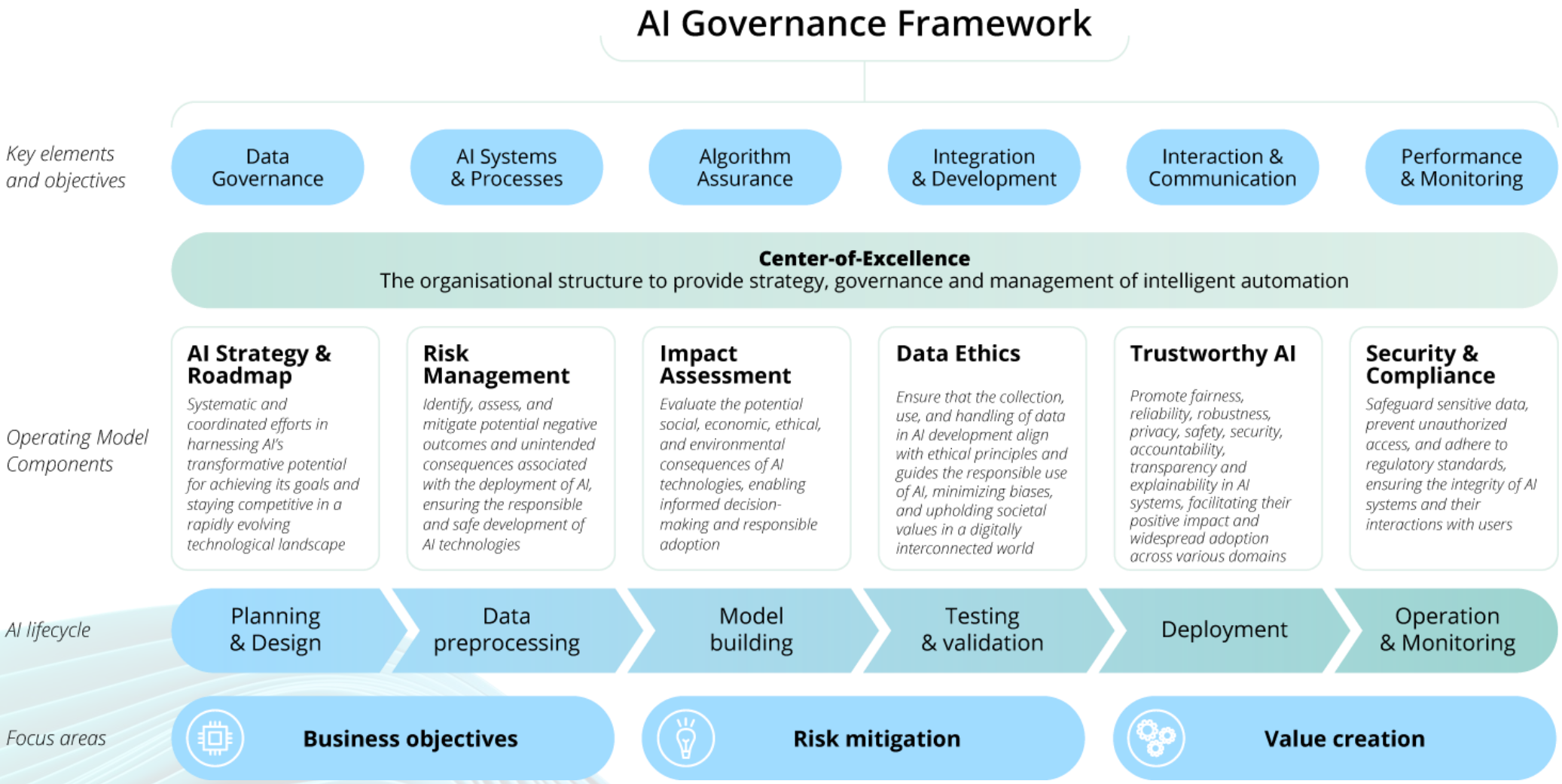
Deloitte AI risk management framework

Deloitte's unique risk management framework for AI applications incorporates market-leading trends, leading scientifical results, Deloitte's global experience and in-house knowhow, and industry standards throughout the AI development and operations lifecycle. Deloitte's AI Risk Management Framework provides 6 topics to help mitigate the risks posed by AI systems. Our experts in Hungary have full knowledge of the framework, having participated in its development.



Artificial Intelligence Governance Framework

The governance framework, developed by Deloitte CE experts, provides solutions spanning the entire AI lifecycle for all industries, from data management to complete monitoring of AI systems and models. The framework focuses on industry-leading practices and a strategic approach to seamlessly navigate complex subfields of the AI world, ensuring the deployment of ethical, responsible and safe AI.



Contact

Zoltán Szöllősi
Partner

zszollosi@deloittece.com
+36 20 910 7644

dr. Dániel Nagy
Managing Associate

dnagy@deloittece.com
+36 20 422 8978

Gergő Barta Ph.D.
Senior Manager

gbarta@deloittece.com
+36 20 328 1190

dr. Lili Albert LL.M.
Senior Associate

lialbert@deloittece.com
+36 20 259 7351

© 2024 Deloitte Hungary

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Legal means the legal practices of DTTL member firms, their affiliates or their related entities that provide legal services. The exact nature of these relationships and provision of legal services differs by jurisdiction, to allow compliance with local laws and professional regulations. Each Deloitte Legal practice is legally separate and independent and cannot obligate any other Deloitte Legal practice. Each Deloitte Legal practice is liable only for its own acts and omissions, and not those of other Deloitte Legal practices. For legal, regulatory, and other reasons, not all member firms, their affiliates or their related entities provide legal services or are associated with Deloitte Legal practices.

Deloitte Central Europe is a regional organization of entities organized under the umbrella of Deloitte Central Europe Holdings Limited, a member firm in Central Europe of Deloitte Touche Tohmatsu Limited. Services are provided by the subsidiaries and affiliates of Deloitte Central Europe Holdings Limited, which are separate and independent legal entities. The subsidiaries and affiliates of Deloitte Central Europe Holdings Limited are among the region’s leading professional services firms, providing services through more than 13,000 people in 42 offices in 18 geographies.

This communication and any attachment to it is for internal distribution among personnel of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms and their related entities (collectively, the “Deloitte organization”). It may contain confidential information and is intended solely for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, please notify us immediately by replying to this email and then please delete this communication and all copies of it on your system. Please do not use this communication in any way.

None of DTTL, its member firms, related entities, employees, or agents shall be responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2024 Deloitte Hungary