Deloitte.

Green Light for AI

How new EU regulations on AI are shaping the future of the automotive industry

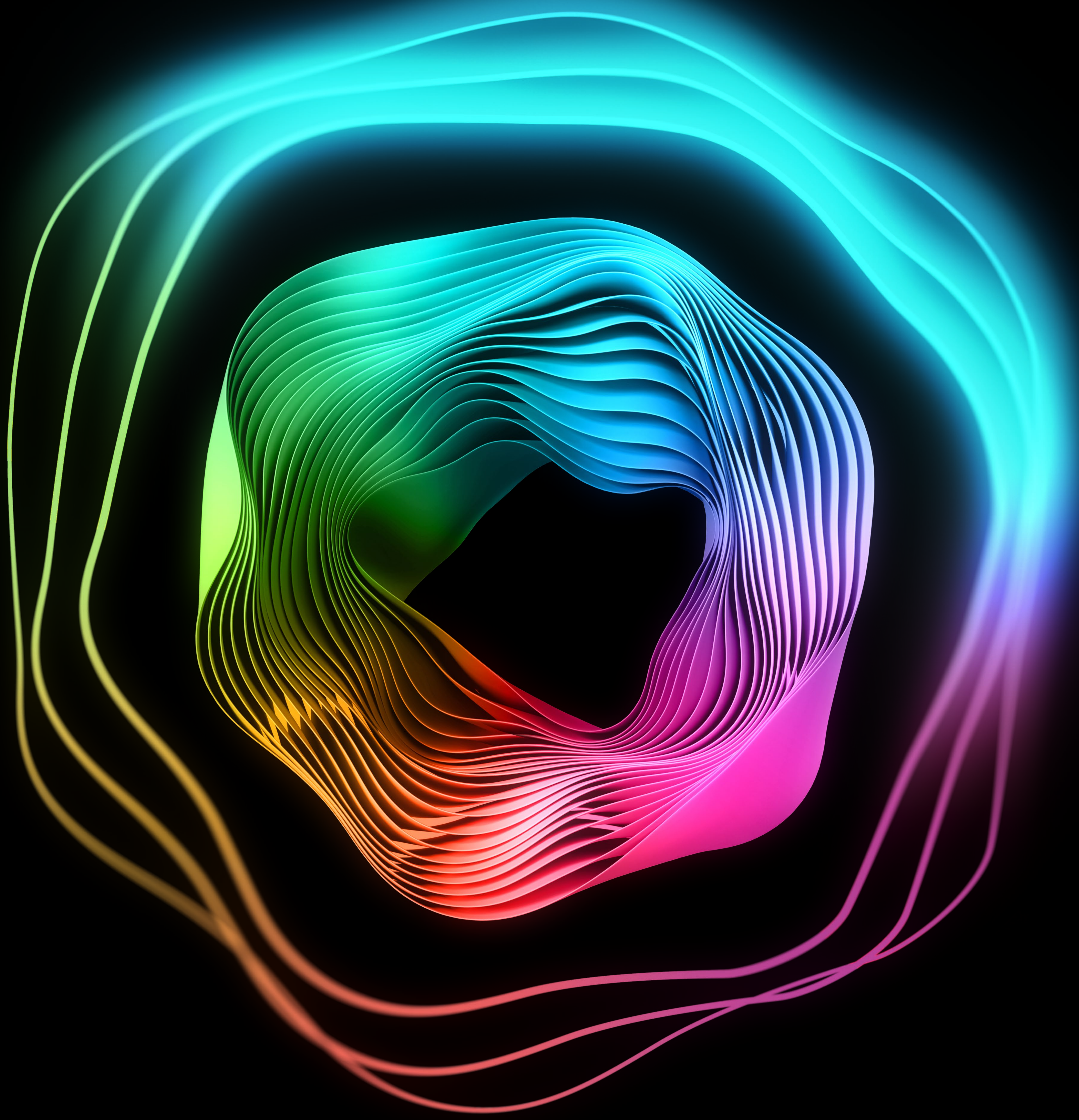


Table of contents

1 **Status quo:** the AI Act

In the fast-changing regulatory landscape on artificial intelligence (AI), the European Union (EU) has been at the forefront of the efforts to establish a comprehensive framework that addresses all of the complexity and risk potential of AI systems. One of the EU Commission's biggest priorities for the 2019–2024 term has been to set Europe up for success in the digital age.[1] Backed by this ambitious agenda, more than ten major digital regulations have been proposed in areas such as the data economy, cybersecurity and online platforms. The EU regulation laying down rules on artificial intelligence ("AI Act") is a key component of the EU's digital regulatory agenda. While the following article focuses mainly on the AI Act itself, we trust you will see it in the broader context of European digital regulations.

Under the new AI regulation, European-based companies are expected to utilize AI in a trustworthy and transparent fashion while also safeguarding the fundamental rights of European citizens. They must establish governance structures as well as an effective AI risk management system to monitor compliance with the new rules and avoid severe penalties of up to 7 percent of annual global turnover or 35 million euros.

The AI Act also provides a set of policies designed to establish safe, transparent and ethical standards for the digital landscape in the European Union. In line with Europe's broader digital regulatory agenda, the AI Act adopts a risk-based approach to standard market entry and operational procedures for single-purpose AI (SPAI) systems and makes sure it is applied consistently across all EU member states. The classification system used in this approach categorizes all AI systems according to their use cases and the associated risks.

In its broad definition of AI systems, the Act covers technologies designed to make forecasts, recommend content or take decisions that impact both the physical and the virtual world. All AI vendors and users within the EU are subject to the act, as well as those outside the EU whose systems impact EU users. Military applications, scientific research and personal non-professional activities are exempt from the law.

[1] European Commission (accessed on Aug. 8, 2024)

Status quo: the AI Act

The AI Act classifies AI systems in four risk levels (see Fig. 1):

Unacceptable risk

Banned practices include AI systems used for manipulating human behavior or social scoring. It is illegal to operate these systems because of the critical potential for harm.

High-risk AI systems

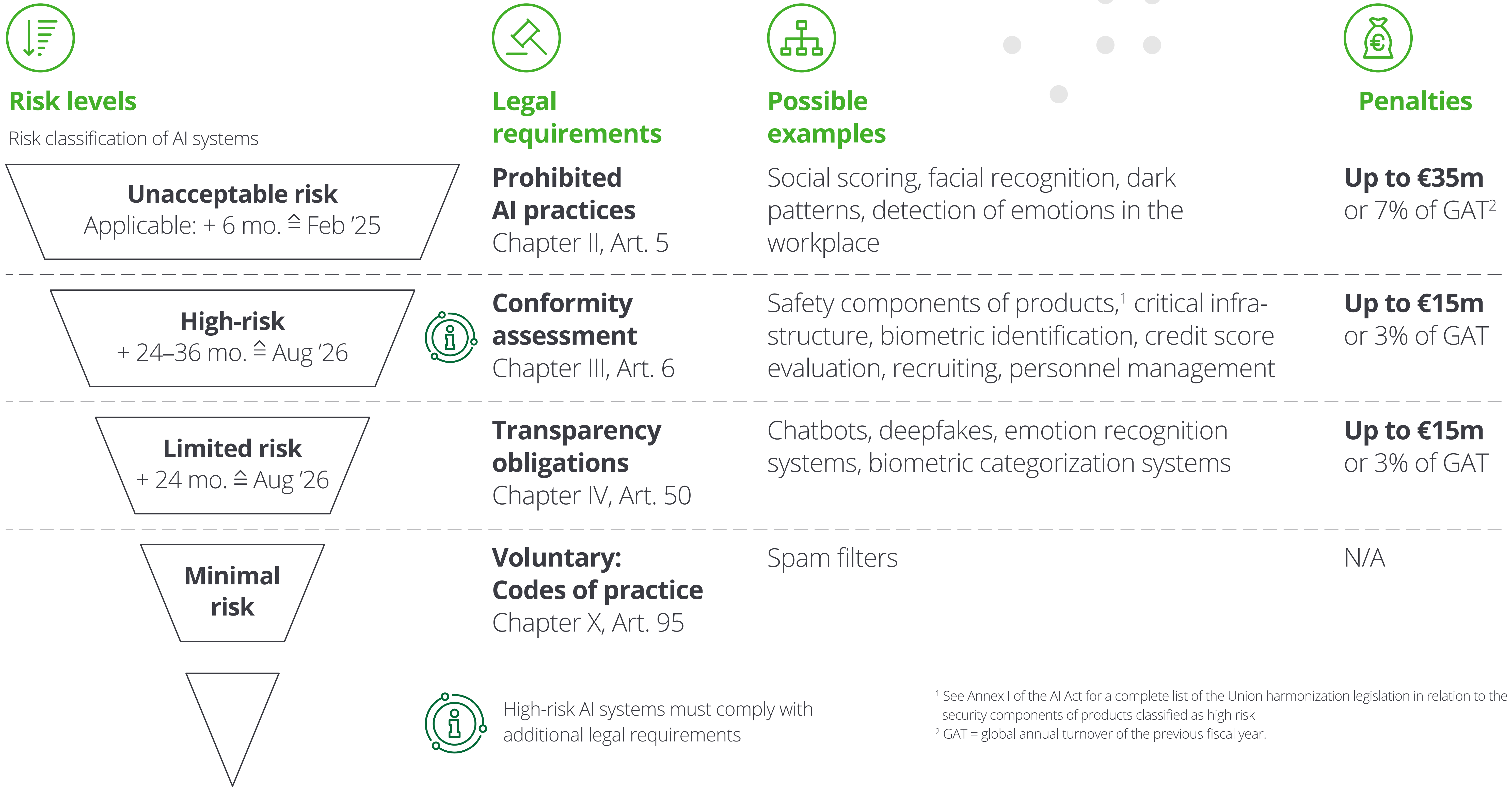
Systems that impact safety or fundamental rights are classified as high-risk. Due to the high potential for harm, these systems must meet strict compliance requirements and undergo a conformity assessment before initial operation.

Subject to transparency requirements

AI systems that interact directly with humans are subject to special transparency rules, e.g., a duty to inform the relevant persons that they are interacting with an AI-supported system.

Low/no risk

AI systems in this category do not pose a serious risk. Providers may, on a voluntary basis, establish codes of practice and governance policies for these systems.



Risk levels Risk classification of AI systems	**Legal requirements**	**Possible examples**	**Penalties**
Unacceptable risk Applicable: + 6 mo. ≙ Feb ’25	**Prohibited AI practices** Chapter II, Art. 5	Social scoring, facial recognition, dark patterns, detection of emotions in the workplace	**Up to €35m** or 7% of GAT[2]
High-risk + 24–36 mo. ≙ Aug ’26	ⓘ **Conformity assessment** Chapter III, Art. 6	Safety components of products,[1] critical infrastructure, biometric identification, credit score evaluation, recruiting, personnel management	**Up to €15m** or 3% of GAT
Limited risk + 24 mo. ≙ Aug ’26	**Transparency obligations** Chapter IV, Art. 50	Chatbots, deepfakes, emotion recognition systems, biometric categorization systems	**Up to €15m** or 3% of GAT
Minimal risk	**Voluntary: Codes of practice** Chapter X, Art. 95	Spam filters	N/A

ⓘ High-risk AI systems must comply with additional legal requirements

[1] See Annex I of the AI Act for a complete list of the Union harmonization legislation in relation to the security components of products classified as high risk

[2] GAT = global annual turnover of the previous fiscal year.

Figure 1 *Risk classification and risk management rules under the AI Act*

Status quo: the AI Act

The Act sets out specific responsibilities for different actors including providers, users, distributors and importers, with a focus on establishing risk and quality management systems, conducting conformity assessments and ensuring transparency.

The AI Act targets high-risk AI systems in the majority of the mandates and safeguards provided by the law. High-risk AI systems are defined as those with the potential to adversely impact the safety or fundamental rights of European citizens and are therefore subject to certain rules before deployment and throughout their lifecycle. There are two methods of classifying AI systems as high-risk: the specific applications listed in Annex III of the Act or the safety components of products listed in Annex I. Actors in sectors specified in Annex 1 must determine whether their products contain an AI system covered by the Act, i.e., whether, as a safety component it is subject to third-party conformity assessment. The rules for high-risk AI systems as defined in Annex I apply 36 months after the Act comes into effect.

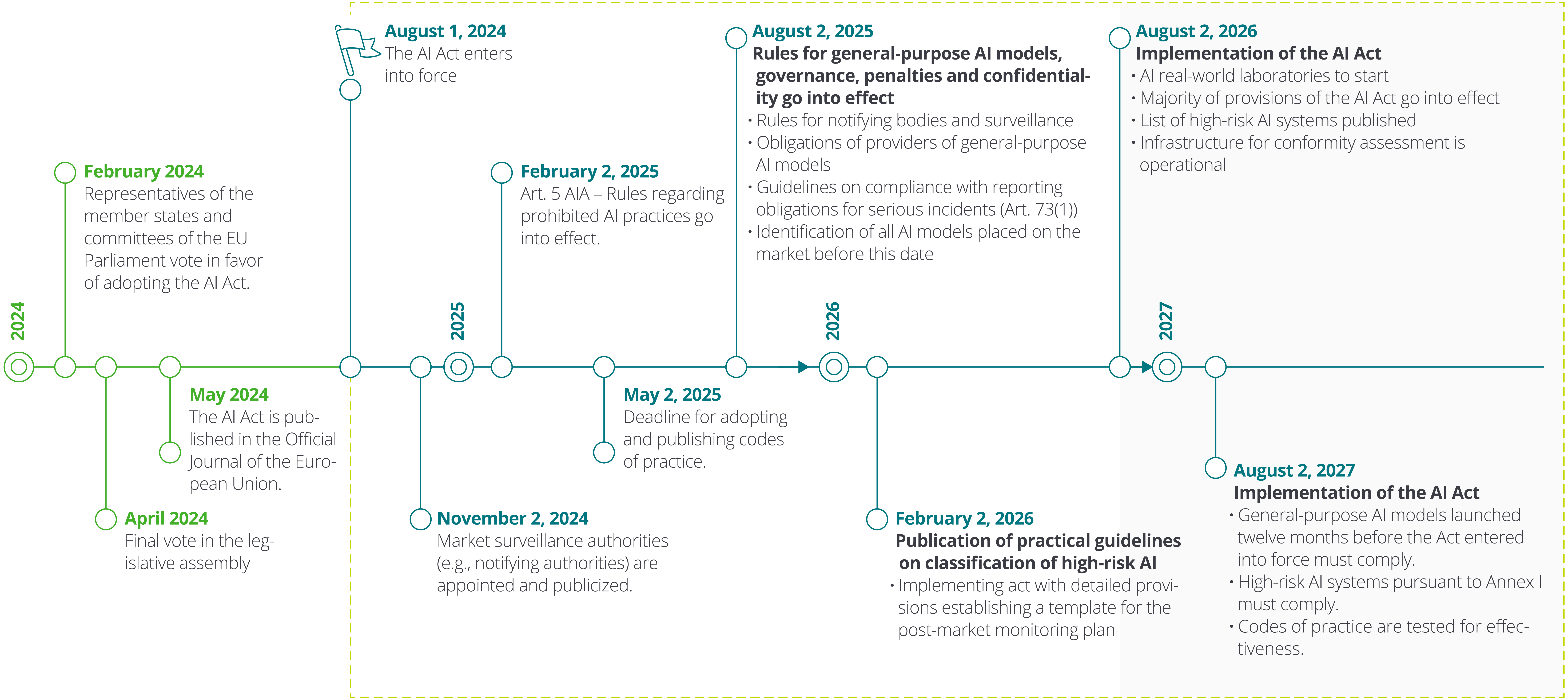
The Act also regulates general-purpose AI models, which it defines broadly as self-supervised models with a wide range of uses that are capable of competently performing a wide range of distinct tasks regardless of the area of application and that can be integrated into a variety of downstream systems or applications. AI models classified as general purpose are required to provide detailed technical documentation and detailed summaries of the content used to train the AI model. AI models for research and development prototypes are exempt from these provisions.

The lawmakers assign stricter requirements to those general-purpose AI models that pose a systemic risk, e.g., those with high-impact capabilities evaluated on the basis of appropriate technical tools or those which the European Commission deem to have equivalent capabilities or impact based on specific criteria. When the amount of computing power used for training a model measured in floating point operations is greater than 10^25, these models are also classified as high-risk. These models must observe the rules that apply to all general-purpose AI models and meet additional requirements including notifying the Commission within two weeks of meeting the criteria, performing model evaluations and attack tests, assessing and minimizing systemic risks at the EU level, reporting serious incidents and introducing robust cybersecurity measures.

In an effort to foster innovation while also ensuring compliance, the AI Act encourages providers to avail of regulatory AI real-world laboratories—controlled environments where they can test and validate their AI systems prior to market launch.

Status quo: the AI Act

Timeline and adoption phases for the gradual implementation of the AI Act



February 2024
Representatives of the member states and committees of the EU Parliament vote in favor of adopting the AI Act.

April 2024
Final vote in the legislative assembly

May 2024
The AI Act is published in the Official Journal of the European Union.

August 1, 2024
The AI Act enters into force

November 2, 2024
Market surveillance authorities (e.g., notifying authorities) are appointed and publicized.

February 2, 2025
Art. 5 AIA – Rules regarding prohibited AI practices go into effect.

May 2, 2025
Deadline for adopting and publishing codes of practice.

August 2, 2025
Rules for general-purpose AI models, governance, penalties and confidentiality go into effect
- Rules for notifying bodies and surveillance
- Obligations of providers of general-purpose AI models
- Guidelines on compliance with reporting obligations for serious incidents (Art. 73(1))
- Identification of all AI models placed on the market before this date

February 2, 2026
Publication of practical guidelines on classification of high-risk AI
- Implementing act with detailed provisions establishing a template for the post-market monitoring plan

August 2, 2026
Implementation of the AI Act
- AI real-world laboratories to start
- Majority of provisions of the AI Act go into effect
- List of high-risk AI systems published
- Infrastructure for conformity assessment is operational

August 2, 2027
Implementation of the AI Act
- General-purpose AI models launched twelve months before the Act entered into force must comply.
- High-risk AI systems pursuant to Annex I must comply.
- Codes of practice are tested for effectiveness.

Figure 2 *Timeline and adoption phase for the gradual implementation of the AI Act*

Status quo: the AI Act

The AI Act entered into force on August 1, 2024 and will be implemented in stages. During the transition phase, enterprises will have time to prepare for compliance and ensure the process runs smoothly. This legislation represents a major step in the regulation of AI in the EU, aiming to strike the right balance between fostering innovation and ensuring safety as well as ethical standards. Companies must take the necessary steps to comply with these regulations and engage in responsible development so that EU citizens can trust these AI systems.

By 2035, self-driving vehicles will account for one out of every three car rides in German cities. Experts are forecasting EUR 16.7 billion in sales for mobility services with self-driving capabilities.[2,3]

[2] Deloitte (2019): Data Nation Germany. Urban Mobility and Autonomous Driving in 2035: How robotaxis will affect cities and automakers. Accessed on August 29, 2024.

[3] Statista (2023): Artificial Intelligence – Statista Dossier (in German). Accessed on August 29, 2024.

2 **Sector perspective:** The AI Act and its impact on the automotive sector

AI technology has become an everyday reality in our world. Whether it is voice assistants, image and facial recognition, smart IoT devices or personalized recommendations, the list of pioneering AI-driven applications goes on and on. The rise of generative AI technology (GenAI) in content creation, for example via chatbots, has pushed AI into the spotlight.

For some time now, AI-powered systems have been in use across the entire automotive industry value chain in various secure and tested areas of application: from raw material processing to the dealer-ready vehicle and even after-sales services. This AI technology is often embedded in standard software designed to support or optimize existing systems. Thanks to the rapid advances of the recent years, AI technology is playing a more prominent role in self-driving applications, connectivity, smart manufacturing, innovative R&D, design, infotainment and other aspects of the current and future mobility landscape. The objective has always been to make the vehicle a more efficient, user-friendly and safer product for all road users in addition to optimizing the production process itself. We expect AI to lead to advances in other areas of application in the future as well, particularly in automation and Industry 4.0.

The exponential improvement in AI performance and the wide range of applications made possible by the technology offer enormous opportunity for the automotive industry, but a massive disruption like this also raises important and legitimate concerns. Unresolved regulatory issues, such as how to deal with hazards and risks, are particularly relevant for automotive OEMs and suppliers in the context of self-driving vehicles or advanced production technology. Urgent calls for a binding legal framework are more than justified—and European lawmakers have now responded with the AI Act.

The risk levels outlined at the start of the AI Act and the focus on high-risk AI systems have sparked vigorous debates within the automotive industry. The debates among sector players have been particularly contentious when it comes to the definition of "safety components" in Art. 3(14) and the "classification rules for high-risk AI systems" in Art. 6 of the AI Act. To be considered a "safety component" under the law, it must serve a safety function for a product or AI system or have the potential to endanger the health and safety of persons or property in the event of a failure or malfunction.

This suggests that a large number of the AI systems already in use in our vehicles could be classified as high-risk. For example, if an AI system is used as a safety component of a vehicle part that is already subject to approval today (in accordance with the EU harmonization legislation outlined in Annex I of the Act), it would automatically be classified as high-risk and subject to stricter legal requirements. This very broad definition of what constitutes a safety component has the potential to create uncertainty and stunt innovation within the automotive industry. It remains to be seen—and sector players will be watching closely—whether the EU will adopt a delegated act or sector-specific amendments to the existing EU type approval rules for registered vehicles (Regulation 2018/858 on the approval of motor vehicles) to provide more detailed guidance for cases such as these.

We will use two representative and simplified AI-related case studies to illustrate the regulatory impact of the AI Act on the use of AI in the automotive space.

Case study 1: Advanced self-driving and driver assistance systems

The five levels of driver assistance systems describe the forward movement or control of a vehicle in terms of driver involvement, right up to self-driving systems at level 5. In this context, no one system operates on its own. The vehicle draws on a variety of data designed to adapt its driving behavior to the prevailing circumstances with driver assistance and safety systems from lane departure warnings and automatic distance control to emergency brake assistance. Other information generated in response to environmental factors enrich the existing data, giving the driver assistance system a 360-degree view and assessing the behavior of other road users to determine and execute the ideal driving performance. AI technology is what enables these functions to develop their full potential, for example in camera sensors that combine classic image processing algorithms with AI tools.

Based on the harmonization legislation mentioned above, advanced driver assistance systems could automatically be classified as high-risk AI systems if they are deemed to be safety components as defined in Article 3(14) of the AI Act. Adaptive cruise control systems could be one example here. As the failure or serious malfunctioning of this system could pose risks to the health of passengers, we have to assume that this AI-supported system will be classified as high-risk under the law as it currently stands. All of the driver assistance systems used in self-driving applications, which have similar implications in the event of failure or malfunctioning, would therefore also be classified as high-risk AI systems.

For some manufacturers, there would be a considerable administrative burden involved in meeting the regulatory requirements for AI systems classified as high-risk.

Case study 2: Voice recognition and smart infotainment systems

Another important area of application for AI is voice assistants and smart infotainment systems, which enable seamless interaction between the driver and the vehicle, improve the user experience and help keep our roads safe. Voice assistants in a vehicle use advanced voice recognition and natural language processing to understand and respond to driver commands and requests. Drivers are less likely to be distracted in this scenario, because they can keep their hands on the wheel and their eyes on the road while operating other vehicle features with their voices. These systems use AI technology to learn from the driver's preferences and habits as well as provide personalized recommendations, for example in terms of route planning, music or news. By the same token, smart infotainment systems go beyond simple voice commands and offer a range of AI-supported services such as real-time traffic information, weather forecasts, third-party apps and even predictive maintenance. The ability of these systems to collect and analyze data on an ongoing basis ultimately gives drivers a more comfortable ride and makes vehicles more efficient.

For this case study, we assume that the driver regularly interacts with the AI-supported voice assistant in the car. The assistant could malfunction and make misleading statements to the driver, which might distract them while they are driving and cause an accident with the potential of physical harm to the driver or other persons. In this case, the malfunctioning of the voice assistant would only be indirectly responsible for the accident, as the driver's reaction remains an essential element of the causal chain.

The voice assistant in this example could be classified as a non-safety-related component.

3 Creating the necessary systems to comply with the AI Act:
AI governance and its inclusion in existing programs

Compliance with the AI Act is more of a marathon than a sprint. We should also note that the AI Act not only applies in relation to the vehicle itself; in principle, we must always consider the law when it comes to protecting people from the harmful effects of AI systems and above all safeguarding the health, safety and fundamental rights of EU citizens.

As a result, in addition to predictive maintenance activities for the vehicle in after sales, AI-supported customer analytics and communications would also be covered by the AI Act. Human resources is another area where companies will have to comply with the provisions of the Act, whether it relates to AI-supported recruitment, employee evaluation or management activities. If a company uses AI technology to support and assess its employees, these AI systems will be considered high-risk. Likewise, the financial services division of an automotive OEM will also be subject to the regulations pertaining to high-risk AI systems if they use the technology to determine the creditworthiness or credit standing of loan applicants, as they determine which consumers receive access to financial resources.

So, companies need to take a systematic approach in order to meet the implementation requirements of the AI Act over the long term and respond accordingly when things change.

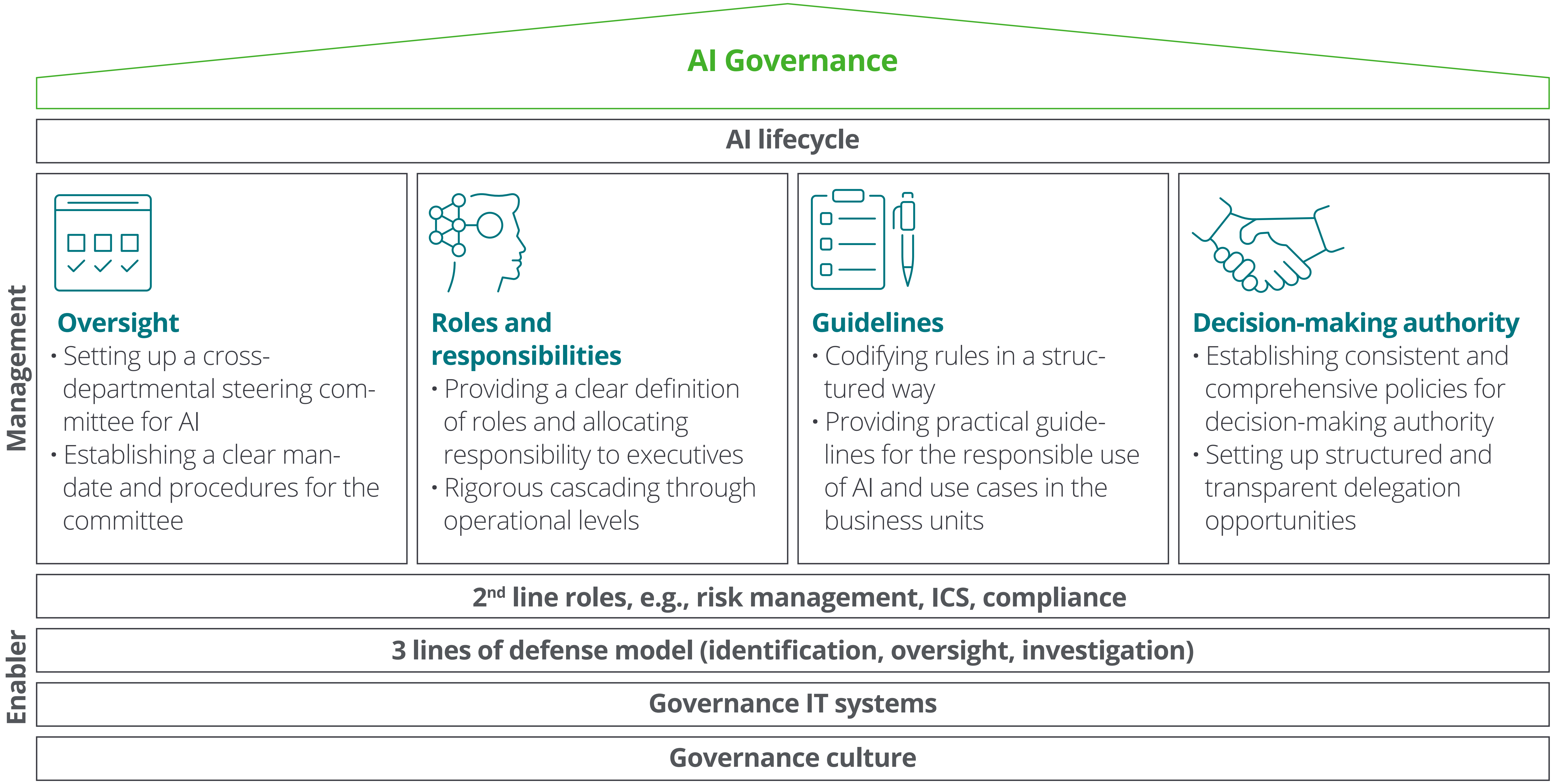
(Further) development of AI governance

AI governance lays the foundation for an enterprise-wide, systematic approach to AI. It provides a structured framework companies can use to gain a broad overview of their AI systems and make sure they are both transparent and compliant in their use of AI. The key components include creating a clear governance model including steering committees to manage AI adoption; defining relevant roles and responsibilities; developing suitable guidelines and operating procedures as well as a uniform process and technology infrastructure. This provides companies with the tools they need to manage and standardize the AI lifecycle from conceptual design to data preparation and model development and from production to roll-out and continuous oversight. AI governance makes it easier for companies to operate AI systems profitably within the regulatory framework and makes them agile enough to adapt should the regulatory situation change. A centralized governance solution benefits the individual business units as well, giving them peace of mind and the confidence to develop and use innovation-driven AI for their specific priorities.

Interplay with data governance

Data governance is the strategic management and oversight of data resources within an enterprise, using reliable data to maximize business value while mitigating risk. In the context of AI governance, data governance has a key role to play in sourcing the necessary data to develop and operate AI models and AI systems in compliance with the AI Act. Of particular note here are the "data and data governance" provisions for high-risk AI systems outlined in Art. 10 of the AI Act, which stipulate that all high-risk AI systems must utilize high-quality, representative and error-free datasets. The law lays down certain data governance procedures, including data collection, processing, evaluation and monitoring, which will identify any biases present in the AI system and take corrective action.

Thanks to data governance, companies are also in a better position to comply with the data-related rules for general-purpose AI models, including those with systemic risk. This includes the requirement, for example, to prepare and publish a detailed summary of the training data for an AI model that uses proprietary software. For AI models with systemic risk, additional rules apply, from performing model evaluations to introducing dedicated risk management and cybersecurity measures for the models and the infrastructure. Other interdisciplinary aspects of data governance also play a data protection role with AI models and AI systems that rely on sensitive personal data.



AI Governance

AI lifecycle

Management

Oversight
- Setting up a cross-departmental steering committee for AI
- Establishing a clear mandate and procedures for the committee

Roles and responsibilities
- Providing a clear definition of roles and allocating responsibility to executives
- Rigorous cascading through operational levels

Guidelines
- Codifying rules in a structured way
- Providing practical guidelines for the responsible use of AI and use cases in the business units

Decision-making authority
- Establishing consistent and comprehensive policies for decision-making authority
- Setting up structured and transparent delegation opportunities

Enabler

2nd line roles, e.g., risk management, ICS, compliance

3 lines of defense model (identification, oversight, investigation)

Governance IT systems

Governance culture

Figure 3 *AI governance structures*

Creating the necessary systems to comply with the AI Act: AI governance and its inclusion in existing programs

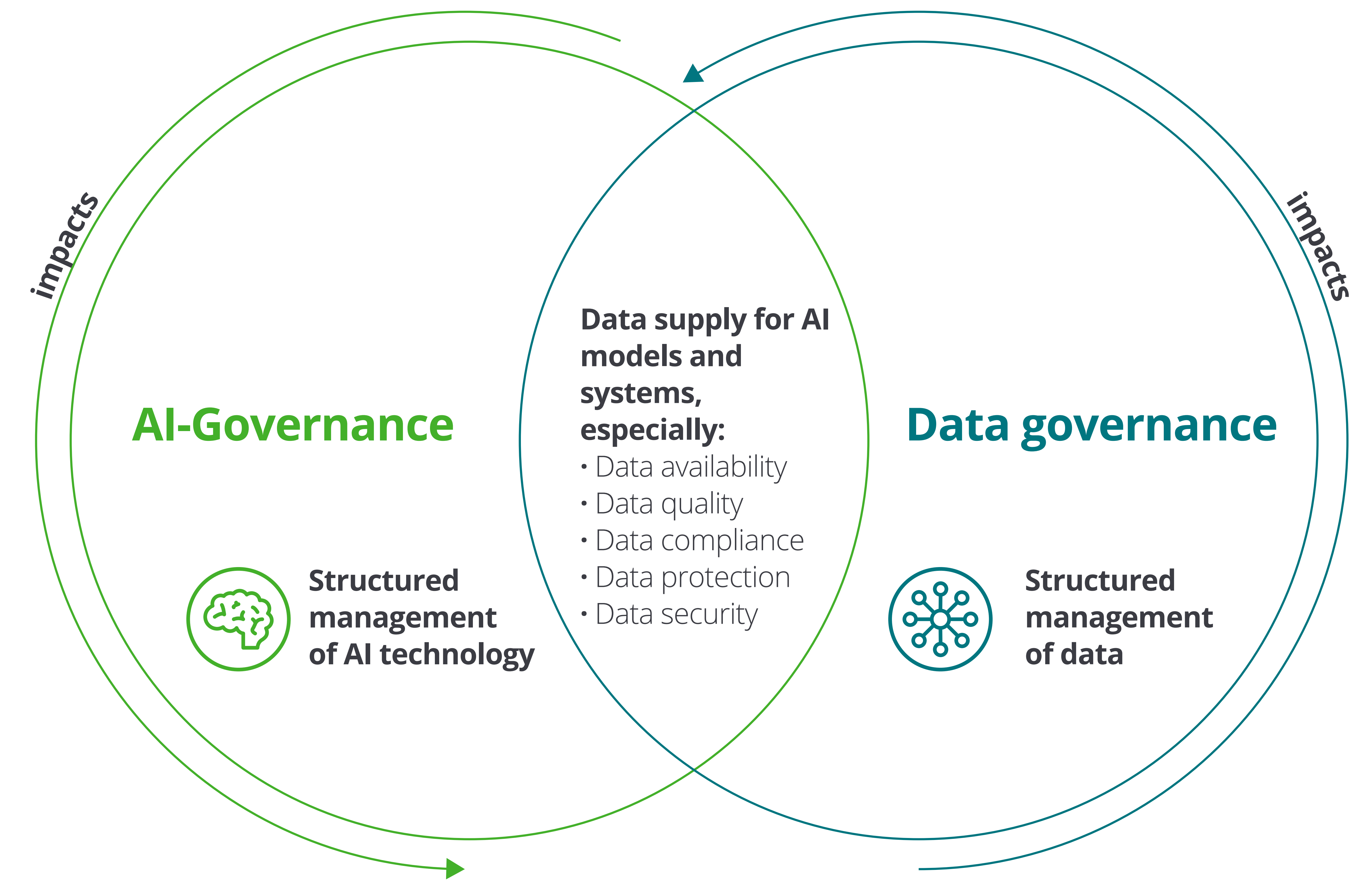


Figure 4 *How AI governance and data governance work together*

Including AI in governance, risk and compliance management systems (GRC)

Addressing AI in the enterprise-wide GRC framework is vital when it comes to comprehensive, consistent and effective compliance with the AI Act. A centralized overview of the GRC roles and responsibilities can also contribute to the efficient use of existing resources.

Governance

Governance provides companies with an internal framework for their risk management, internal control system (ICS) and compliance activities, among others. Establishing AI governance principles complements existing guidelines and control objectives across the entire AI lifecycle. It is also important to add AI-relevant aspects to existing standards as well as cross-departmental processes and ensure they are applied consistently to address future AI risks and avoid compliance violations under the AI Act. To ensure any roles and responsibilities created in the AI governance process are standardized and anchored in the expanded GRC structures, key GRC stakeholders will have to collaborate with the AI governance team in a coherent and consistent approach to AI adoption.

Risk management

Companies need a robust risk management system to systematically identify, analyze and assess potential risks. With targeted risk management measures and systematic oversight, they can reduce the potential for damage and determine which measures are most appropriate and effective.

There are various risk categories for AI that companies must address when including AI in their overall risk management activities. Initially, the main focus here is on managing compliance risks to ensure AI applications meet the basic requirements of the AI Act. In the broader context, this also includes the risk of data protection violations due to unauthorized processing of personal data and copyright violations in connection with the use of protected data. Another relevant category of risk here are unreliable AI results caused by hallucinations and bias that may lead to false conclusions and discrimination. Insufficient data quality is another risk factor that may affect the accuracy, completeness and timeliness of the data used for AI models. Security vulnerabilities pose an additional risk by providing a target for poisoning or theft of data and models, which can disrupt operations and jeopardize the integrity and confidentiality of sensitive information, among other effects.

Including AI in the enterprise-wide risk management and internal control system requires careful planning and implementation. The first step is to assess whether your current risk and control system covers AI and/or where the system design may need updating. As all of the AI risk categories are interdependent, it is important to establish a comprehensive management strategy capable of assessing the company's risk-bearing capacity and making consistent statements on the overall risk situation as it relates to AI.

Compliance

Compliance policies ensure a company operates in line with external legal regulations as well as internal guidelines. By establishing a standardized compliance management system (CMS), companies have a set of structured, sustainable and responsible policies. The new AI Act will present companies with additional regulations to follow, although a number of individual compliance issues will already be covered by the existing CMS.

Compliance departments have a lot of experience with the basic management of external regulations as well as systematic mechanisms for monitoring and verifying regulatory compliance. This provides companies with the basic tools they need to analyze and determine which provisions of the AI Act apply to the company, to make any necessary modifications or extensions to the CMS and to identify any oversight measures required from a compliance perspective. The compliance department is also responsible for monitoring any potential future developments relating to the AI Act. As a rule, the CMS will already have established links to other corporate officers. These links will be useful when it comes to introducing the requirements of the AI Act in the individual business units and providing advice on compliance with these regulations.

In light of the rapid technological advances of AI, training and awareness-raising play an important role. Compliance training courses with practical advice on the requirements of the AI Act will help staff acquire the knowledge and skills they need to comply.

We recommend using AI consistently within your GRC framework to maximize the benefits and synergies that arise when the individual GRC elements are viewed as an integrated system. Through systematic integration of AI, companies have a better chance of success in complying with the provisions of the AI Act, not only in an effective way, but above all in an efficient and sustainable way.

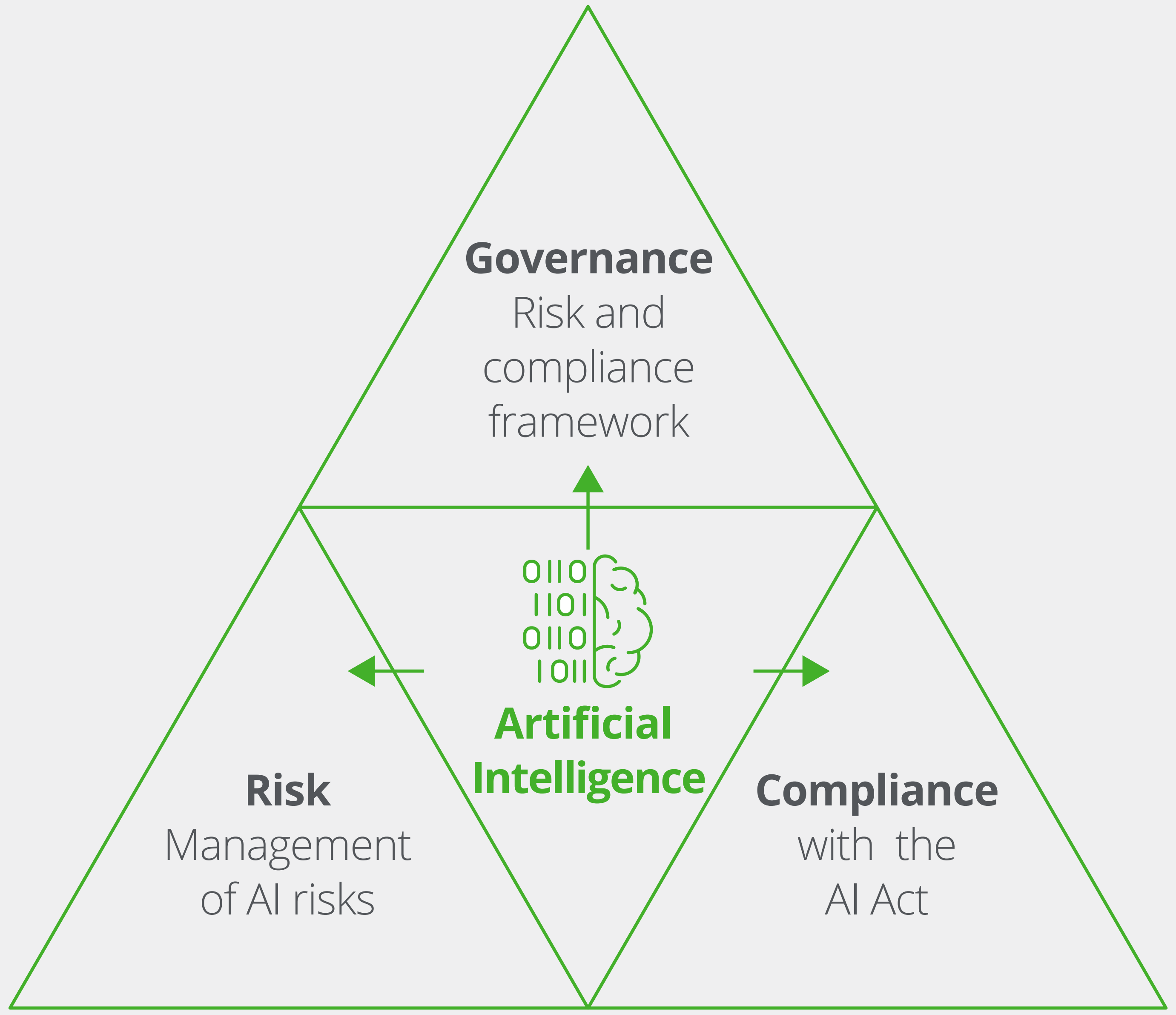


Figure 5 *Integrating AI in the enterprise-wide GRC framework*

4 Conclusion and outlook

The AI Act provides uniform and binding regulations for AI in Europe. As AI applications play an increasingly important role in our economy, this legislation not only aims to safeguard the fundamental rights and security interests of European citizens; it also aims to foster innovation and make European companies more competitive.

Among the main provisions for high-risk AI systems, the AI Act includes systematic risk management as part of a broader AI governance policy framework. The implications of the AI Act for the automotive industry and their impact on future mobility are significant, as AI applications are already in use along the entire automotive value chain, from raw materials to the dealer-ready vehicle and after-sales service.

The definition of AI systems as safety components and the classification of high-risk AI systems on a case-by-case basis are particularly relevant, as they could lead to numerous solutions already in use today being classified as high-risk. This is not to suggest that lawmakers will prohibit the use of these kinds of AI systems outright. However, the mandated conformity assessments could impose a substantial compliance burden on some manufacturers prior to deploying these systems. In addition, other AI practices classified as an unacceptable risk will be banned and AI systems with limited risk will have to meet certain transparency obligations.

Given the severe financial penalties and reputation loss associated with violations, companies must address compliance with the AI Act as a top priority.

After entering into force on August 1, 2020, the provisions of the AI Act will be implemented in stages over a period of six to 36 months. Now is the time for you to put your AI governance, data governance and GRC policies to the test and adopt suitable polices to ensure compliance with the Act.

Deloitte can help you successfully master the complex implementation requirements of the AI Act, gain an edge over your competitors and expand your innovation leadership in the rapidly evolving AI landscape. Don’t hesitate to get in touch—our experts are standing by to address all your questions and concerns.

Contacts

Christa Janhsen

Partnerin Enterprise Risk
Deloitte Österreich
Tel: +43 664 80537 4843
cjanhsen@deloitte.at

Matthias Kunsch

Partner Audit & Assurance
Deloitte Styria
Tel: +43 1 53700 3333
mkunsch@deloitte.at

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/de/UeberUns to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 457,000 people worldwide make an impact that matters at www.deloitte.com/de.

This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or 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.

Issue 10/2024