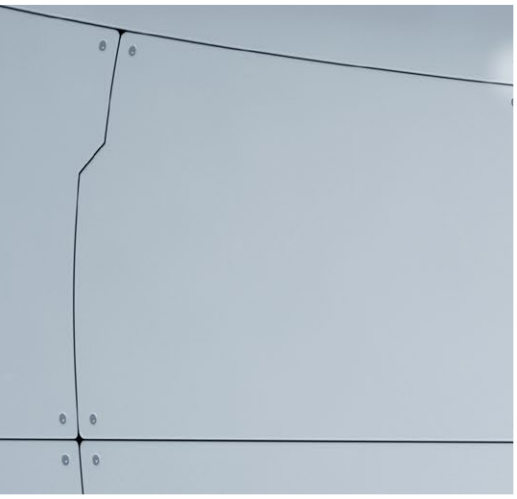
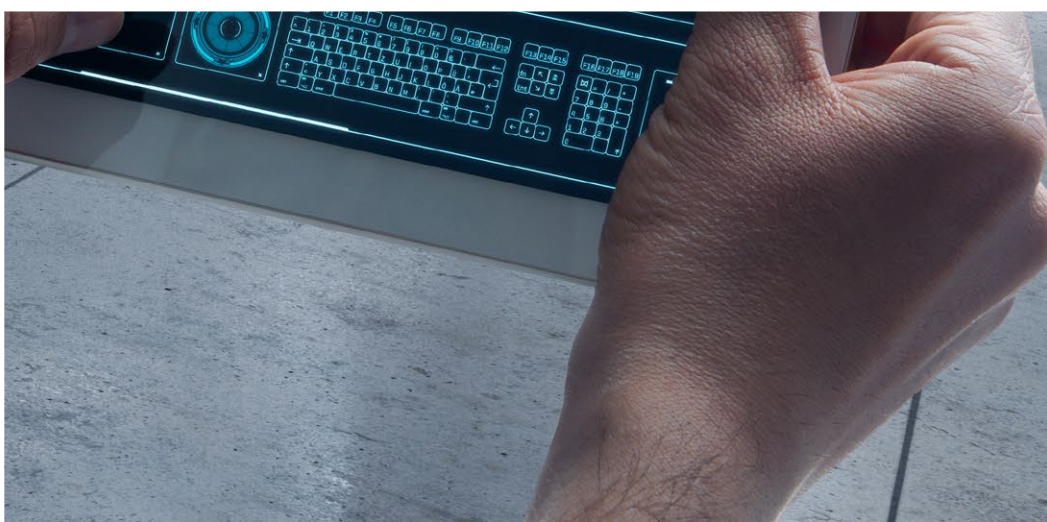


Trusted Artificial Intelligence of Things

The key to tomorrow's sustainable digital products.

pwc



Content

1 Introduction

Global warming and resource constraints are two of the century's major threats to our future, but digital transformation offers new opportunities. The answers to these threats are well known: humanity must optimise its consumption of natural resources and find sustainable digital business models. Companies are under considerable pressure. Artificial Intelligence (AI) improves and extends the functions of established products to help solve the challenges of our time.

However, achieving the necessary technological breakthroughs requires customers' trust in both the B2B and B2C sectors. We believe that those companies that can become the first to refine their products with trustworthy AI will set new standards and reach the top of the market, while others will fall behind.

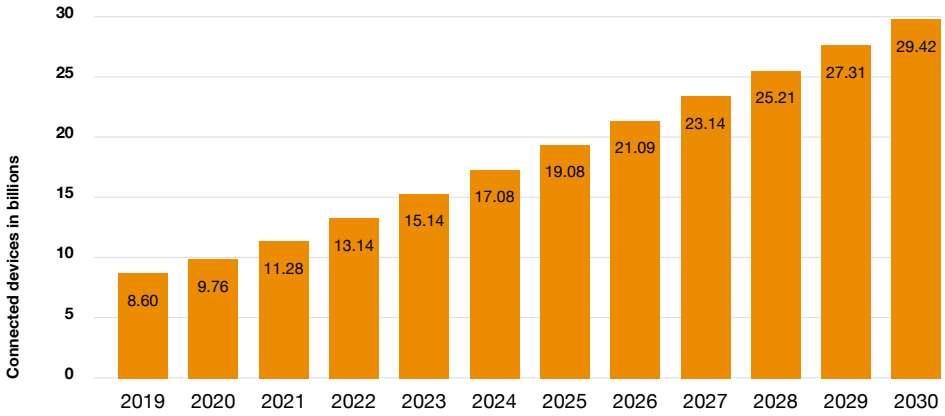
In the following chapters, we have gathered the relevant information, perspectives, and approaches to Artificial Intelligence to prepare your company to start the race in the pole position.

1.1 The Internet of Things is just the beginning

Since 2019 there have been more devices connected to the Internet than there are people on the planet. By 2028, connected devices will likely outnumber people threefold (see fig. 1). The fusion of the digital and physical worlds is further accelerating. Networked devices, termed the Internet of Things (IoT), are a core driver of this exciting landscape of increased possibilities.

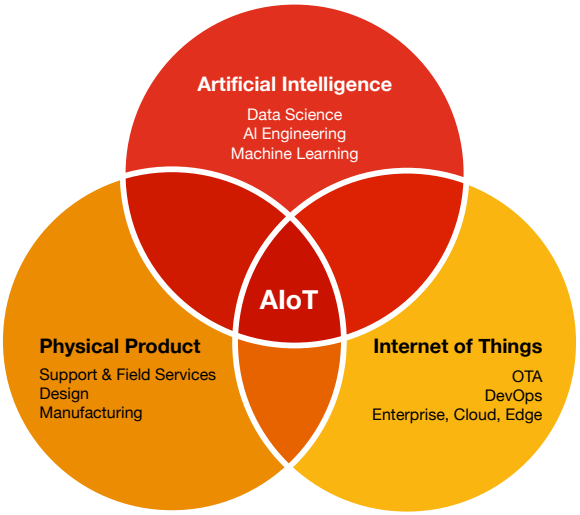
A promising, IoT-related concept is the development of networked devices to create intelligent systems using AI. New processors and optimised algorithms make it possible to move more AI-powered functions to edge devices (see fig. 2).

Figure 1: Increase in the number of networked devices worldwide[1]



1 Transforma Insights. "Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2021, with Forecasts from 2022 to 2030 (in Billions)." Statista, Statista Inc., 1 Jul 2022, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Figure 2: AIoT as a combination of a physical product, IoT and AI



1.2 Artificial Intelligence of Things – the future of Cyber-Physical Systems

Artificial Intelligence is increasingly enhancing connected devices. This concept is known as Artificial Intelligence of Things (AIoT).

Large technology companies[2] have recognised AIoT's potential and its many applications, from smart production and decentralised energy supply over smart buildings and cities to wearables in the health sector. Consequently, countless smart devices are unleashing their potential along companies' and customers' entire value chains, showing that enabling devices with AI-supported functions is a promising step for companies' future viability.

By transferring AI-supported functionality to an edge device, the advantages over separate IoT and Cloud AI—such as real-time capability, high availability, enhanced privacy protection, and reduced networking costs—pave the way for new use cases with increased economic potential (see fig. 3).

However, to leverage these advantages and transform and extend market-ready products, many companies must overcome extensive time and planning effort, greater development complexity, and difficulties in ensuring error-free functionality throughout the entire lifecycle.

1.3 Digital Trust – the decisive factor

Companies and users need to trust Artificial Intelligence in an increasing number of situations, from professional to personal life. However, surveys show that most users do not yet trust the technology sufficiently[3]. Users' main concern is uncertainty over the accuracy and performance of AI, as AI systems seem to lack transparency and are difficult to verify.

There are also doubts about AI systems development being based on ethical values such as integrity. The degree of digital trust lies in the users' confidence in a company's ability and willingness to create secure and functional AI-enabled products. A critical factor in increasing trust in a company's competence to build and operate trustworthy AI solutions is demonstrating safety, privacy, security, reliability, and data requirements.

It follows that a central challenge for companies is to scale up users' digital trust in AIoT-based products, as a lack of confidence can severely limit the economic performance of related solutions and market potential.

"At PwC Germany, our mission is to establish digital trust as an enabler of sustainable and scalable value creation by applying the trusted AIoT-Lifecycle."

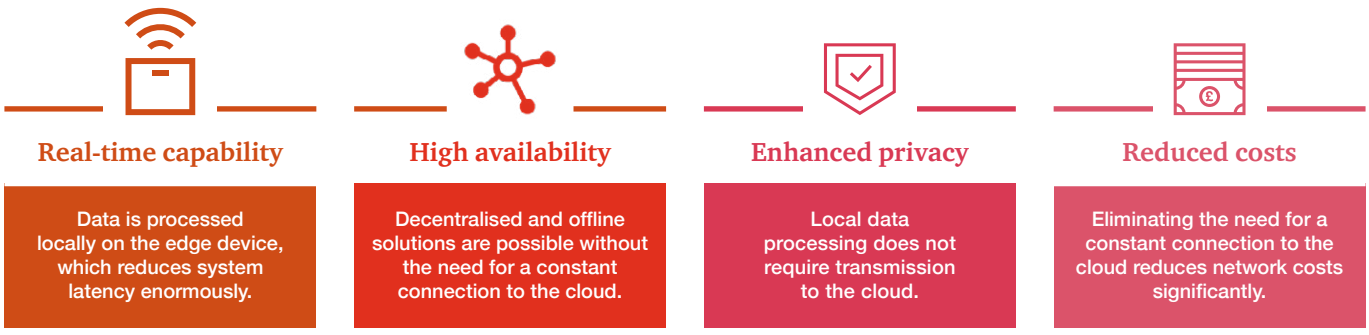


Figure 3: Advantages of transferring AI-supported functionality to edge device

2 https://www.bosch-presse.de/pressportal/de/de/aiot-bosch-kombiniert-vernetzung-internet-der-dinge-iot- und-kuenstliche-intelligenz-ai-227989.html

3 https://assets.kpmg/content/dam/kpmg/au/pdf/2021/trust-in-ai-multiple-countries.pdf

Smart Manufacturing

Smart Manufacturing promises cost savings and efficiency gains through automation and optimisation by using intelligent sensor networks, actuators, and controls in any production step. Intelligent devices can support employees, by, for example, performing simple routine tasks or reducing the time of more complex tasks. As a result, these smart devices can increase workplace productivity and efficiency. Smart Manufacturing also reduces waste and costs by detecting errors in production processes or providing an optimised control scheme.

Compared to AI-based quality assurance systems, manual and conventional quality inspections are less reliable, more expensive, and difficult to scale. One example of an AI-based quality inspection is the application of image processing to automate real-time target-performance checks of produced goods on the production line. During the inspection at any stage of the production process, even the tiniest defects on a product's surface, which humans would usually miss, can be identified. Consequently, quality assurance can be integrated more efficiently, accurately, and seamlessly into production processes.

The quality of products is often affected by the machine operators' capability to handle the machinery. The better qualified they are, the faster they can identify potential problems. However, as production environments are typically fast-changing, rapid adaptability to new conditions is necessary. By supporting machine operators with AI-based systems, they will be able to respond more efficiently to unexpected changes and maintain stable performance.

This agility can be accomplished by providing specific use case explanations and recommendations to assist employees to the extent required. For instance, an AI-supported drilling machine can recommend necessary parameters and process steps changes if a drill hole deviates from the defined placement. This way, an employee's knowledge can be expanded while simultaneously avoiding production waste. Moreover, instead of manually fine-tuning machine parameters, an AIoT system can automatically adjust the parameter settings, thereby reducing machine downtime.

For individualised recommendations, personal data about the operators and their work performance is required. An adequate explanation of the necessity and added value of analysis and data processing is essential to alleviate employees' and labour unions' concerns over employee monitoring and performance. This explanation will help lay the foundation for the acceptance of working with AIoT-based systems and ensure consistent product quality through human-machine collaboration.

Sufficient **digital trust** must be established to achieve the benefits of expanded knowledge, safer processes, and higher quality.

Smart City

The term Smart City refers to various applications that combine urban infrastructures networking and digitisation with the support of AI, leading to more sustainable, efficient, and resource-saving city life. First use cases have already been successful, for example, a smart and efficient waste management system in Regina, Canada[4]. Sensors measure the quantity of waste in bins and analyse possible patterns. AI is then used to determine optimal collection times and routes. This information enables the city to provide demand-oriented and resource-efficient waste management.[5]

In addition to municipal household waste disposal and other governmental activities, Smart Buildings offer opportunities to apply AIoT. By integrating sensors into technical building equipment, parameters such as movement patterns, air quality, and temperature are registered, automating the necessary changes to, for example, room conditions.

Furthermore, it is possible to analyse and forecast the future state of a building, determine parameter adjustments, and identify patterns. By these means, AIoT-based systems can provide a comprehensive and intelligent building control, monitoring and management solution, achieving cost savings, increasing energy efficiency and improving user comfort. An example of such a smart building is The Cube[6] in Berlin.

Both examples highlight that AIoT systems will create a high awareness among citizens of AI with the presence of AIoT in their future everyday life. Therefore, it is vital to start building digital trust today by creating transparent and secure AIoT applications and systems.

Citizens' concerns may arise as smart infrastructure processes personal data and derives patterns from them. The potential exists, for example, for systems to investigate residents' dietary consumption and behavioural profiles. Direct processing on edge devices could ensure trustworthiness by aggregating and pseudonymising sensitive data before making it available to companies and government agencies.

4 Omara, A.; Gulen, D.; Kantarci, B.; Oktug, S.F. Trajectory-Assisted Municipal Agent Mobility: A Sensor-Driven Smart Waste Management System. J. Sens. Actuator Netw. 2018, 7, 29. https://doi.org/10.3390/jsan7030029

5 Cheema, S.M.; Hannan, A.; Pires, I.M. Smart Waste Management and Classification Systems Using Cutting Edge Approach. Sustainability 2022, 14, 10226. https://doi.org/10.3390/su141610226

6 https://3xn.com/project/cube-berlin

Smart Gadgets

From smart homes to wearables, smart gadgets have made people's daily lives easier, more efficient, and more connected by allowing users to access information and automate different aspects of their lives.

Today, worldwide manufacturers of electronic products are expanding their capabilities and providing a better user experience by utilizing AI. With the increasing use of smart gadgets, the trustworthiness of data privacy as well as algorithms have become key issues for many people. This is especially important to consider as smart gadgets collect and analyse large amounts of information about their customers and their environment, including personal data like locations, images or voices.

For example smart refrigerators, equipped with cameras, microphones or other sensors, may collect data about the types of food and drinks their customers consume, the frequency of their grocery purchases, and their preferred grocery stores. Thereby, it may learn the users' preferences and suggest what to buy based on what they typically eat. Another example are smart doorbells, potentially collecting data about the people who visit their customers' homes, the frequency of their visits, and the duration of their stays. Companies could use that data to create detailed movement profiles of their customers for targeted advertising.

Therefore, linking data privacy protection with smart gadgets is important, as users are often unaware of what data is being collected and how it is being used. To enable digital trust, manufacturers need to prioritise privacy, which includes being transparent about their data collection practices and providing clear privacy policies. Foresighted, assuring customers that AI enhanced electronic products are trustworthy is the new major challenge for B2C and B2B2C companies. Addressing this challenge now, companies have to embed privacy and security considerations into their product development process from the very beginning to ensure digital trust by design and to mitigate the potential risks of expensive security breaches or damage to reputation caused by privacy violations.

However, AI brings opportunities to enhance privacy with the help of edge computing to keep sensitive data secure and confidential, while still gaining valuable insights from the analysis of that data on the device. In this way, risks of handling and transferring sensitive data can be mitigated by deriving more abstract representations that can be uploaded to the cloud without any privacy concerns. In addition, machine learning algorithms can be trained to recognize anomalies that may indicate a security threat, allowing for early detection and response to privacy breaches. This approach not only protects individuals' privacy but also ensures compliance with data protection regulations, creating a safer and more secure environment for all.

Smart gadgets are already an essential part of our daily life, providing convenience, and sustainability benefits such as reduced food waste and energy consumption. The key factor for B2B2C electronic companies' future success is to ensure trustworthiness of their products and services.

2 Core challenges for companies to enable and leverage digital trust in AIoT

The examples in the previous chapter showcase AIoT's far-reaching impact on people's personal data and lives. Allowing companies to use AI in smart manufacturing, smart cities, or other areas to access personal information without proper supervision and control poses a significant risk. It may not be a beneficial trade-off for the general public. **The decisive factor is digital trust.** We often get the question: what are the challenges for companies to ensure all aspects of digital trust across the entire AIoT lifecycle? Based on our IoT and AI know-how, we identified four challenges:

1 Complexity

The complexity of AIoT-based systems arises from integrating different technologies—such as AI, IoT and cloud computing, and big data—in one application while ensuring security and privacy, real-time processing and interoperability against a backdrop of limited hardware resources. Combined with a large number of contributors across various companies, departments and responsibilities, it may lead to insufficient systems implementation and maintenance, causing inefficiencies, system failures and potential security breaches.

2 Transparency

Transparency of AIoT-based systems ensures that individuals know what types of data are collected and how it is used, stored, and shared to keep track of their personal information. Transparency also ensures they are aware of the system's decision-making process and its resulting impact on their lives, the environment and society. Companies are asked to provide explicit and understandable explanations on how they will use this information and why it is essential to the system's functionality.

3 Robustness & Security

Robustness & Security includes cybersecurity aspects such as protecting hardware, software, and data from unauthorised access and manipulation. AIoT systems also need to have the resilience to withstand and quickly recover from potential malfunctions to maintain the integrity and availability of connected devices, services, and data. The challenge is to develop the topics holistically and define appropriate reactions to unexpected events.

4 Scalability

The Scalability of AIoT systems is based on the ability to effectively manage and integrate many connected devices, provide and maintain well-tested software, even over the air (OTA), and trouble-free end-to-end data processing. Fundamentally it is about well-defined processes and interfaces along the whole AIoT lifecycle. Enhanced scalability should not lead to increased complexity.

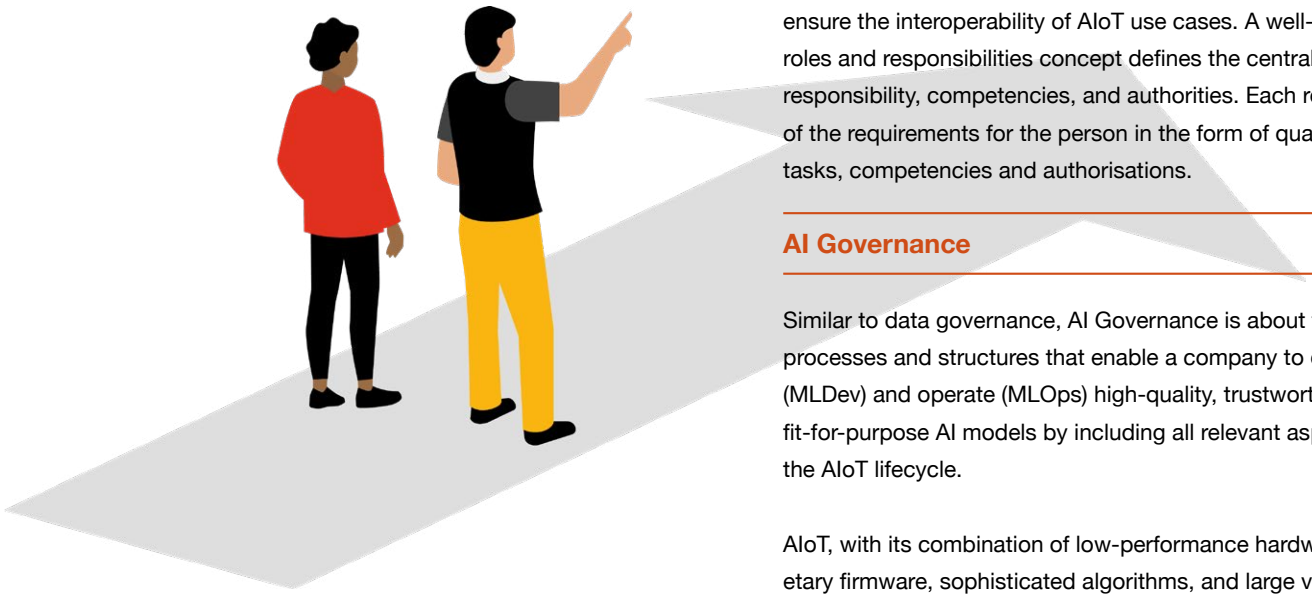
Tackling these challenges requires a holistic strategy, which we will discuss in the following chapter.

3 Success factors for trusted AIoT

The critical challenges for companies to enable and leverage digital trust and unleash the potential of AIoT-based products are **complexity, transparency, Robustness & Security** and **scalability.** These could be considered and worked on individually. However, attempting to solve these challenges one by one can easily lead to impractical processes, delays, and confusion of responsibilities.

Instead, the challenges must be viewed holistically to exploit the synergies.

Governance, risk, and compliance **(GRC)** offers the correct approaches to tackle AIoT trust challenges. Specifically, two crucial governance areas emerge for implementing AIoT successfully.



Data Governance

The underlying data is the basis for—and a decisive success factor in— any AI development. Data management must ensure the necessary quality of the data to guarantee the functionality of the AI. It is not enough to keep the data sets technically clean (Clean, Consistent, Accessible, Secured and Understood). Other organisational processes and structures are needed. These include policies on how data is collected, processed, and stored and what access rights different user groups have.

The handling and encryption of data in motion and at rest must be considered. AIoT concepts significantly alleviate data handling by reducing and anonymising data streams directly at the source. Furthermore, standardisations for data formats and the conversion of data formats and interfaces are established to ensure the interoperability of AIoT use cases. A well-established roles and responsibilities concept defines the central areas of responsibility, competencies, and authorities. Each role consists of the requirements for the person in the form of qualifications, tasks, competencies and authorisations.

AI Governance

Similar to data governance, AI Governance is about the processes and structures that enable a company to develop (MLDev) and operate (MLOps) high-quality, trustworthy, and fit-for-purpose AI models by including all relevant aspects into the AIoT lifecycle.

AIoT, with its combination of low-performance hardware, proprietary firmware, sophisticated algorithms, and large volumes of data, requires well-coordinated concepts, processes and teams.

Not only during development but also operation, a large number of potential problems arise due to the high complexity of the overall system. It is recommended to take a holistic approach, especially regarding roles and responsibilities.

AI model development is an interdisciplinary project involving many contributors with different expertise and understanding. The scalability of AIoT systems is essential for market success. AI Governance offers the necessary steps to lay the foundations for scaling from concept to adoption.

"A good AI governance strategy provides the framework for successful scaling, reduces complexity, and enables transparency. Nevertheless, to show its full potential, it must be tailored precisely to the company's circumstances and use cases."

Risk Management

A comprehensive risk analysis is part of every product's development process. Various protection goals are defined, such as protecting life and limb, material and financial property, the environment, fundamental human rights and ethical aspects. Potential violations by the AIoT system are analysed, categorised, and finally assessed.

The goal is to find appropriate mitigation measures for each risk. AIoT-specific risks, such as the unconscious collection of private data, faulty and incomprehensible control of devices or the deliberate manipulation of the system, might not always be obvious to the public. This makes it even more important to communicate their implications and ensure the effectiveness of the chosen countermeasures.

Compliance

With the upcoming regulatory framework for digital and AI-based products, fulfilling the requirements of a company, product, or system is more crucial than ever. These requirements will be based on laws, regulations, and underlying standards for their implementation.

For AIoT digital trust aspects inside the European Union, two of the significant regulations are the General Data Protection Regulation (GDPR)[7] and the soon-to-come EU AI Act[8]. Compliance is demonstrated by having your AIoT-System validated by an independent and trusted third party and obtaining the necessary regulatory market approval.

The principal challenge for companies is to factor in future compliance requirements while very few best practices are available now, and most standards have yet to be developed. Bridging the gap from well-established frameworks and standards to emerging technologies like AI is a core component for sustained business outcomes. Today's market approvals for cyber-physical products do not consider AI, or only to a very limited extent. Expanding these and creating new market approvals for AI components is essential to developing basic customer trust in AIoT products.

In our experience, following these principles will help your company overcome the challenges associated with the lack of trust in the context of the development and operation of AIoT products

7 https://eur-lex.europa.eu/eli/reg/2016/679/oj

8 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

4 Conclusion

AI will bring new facets to a wide range of cyber-physical systems and influence our lives dramatically for better or worse. We have shown how deeply AIoT systems already advance into users' private lives and highlighted the importance of digital trust. Based on the need for digital trust, we introduced the four core challenges for companies, namely transparency, complexity, scalability, and Robustness & Security.

Tackling these challenges one by one may seem straightforward at first, but this leaves companies with the complexity of interdependent and opaque tasks. Overcoming this complexity demands a holistic GRC approach along the whole AIoT lifecycle. Establishing proper processes, roles and responsibilities across different groups, departments, and even companies can be difficult, but they create the basis for transparency and scalability and reduce complications.

"There are no simple and universal answers to these questions, but with competent and experienced support, these complex challenges become a real opportunity to foster confidence in the safety, privacy, security, and reliability of your AIoT products and services."

Gaining customers' trust in AIoT systems and unlocking the market potential offers an enormous opportunity for companies and society. In Europe, we have the chance to become a pioneer for trusted AIoT and a global role model.

It is essential to recognise that strategies to create digital trust depend on the business and use cases, which leaves decision-makers with a list of critical questions:

- **How can AIoT enhance my products and services?**
- **How do I establish practical AIoT governance along the whole lifecycle?**
- **What are the interdependencies of the departments involved in practical AIoT governance?**
- **How do I manage my AIoT initiatives?**
- **How do I minimise the need for personal data in my use cases?**
- **What are my AIoT-related-risks, and how can I mitigate them?**

Our experts

Hendrik Reese
Partner
Artificial Intelligence

+49 89 5790-6093
hendrik.reese@pwc.com

Jan-Niklas Nieland
Manager
Artificial Intelligence

+49 211 981 4915
jan-niklas.nieland@pwc.com

pwc