



Contents

Chapter

01

A changing world – thanks to AI

Page 5

02

AI's challenges for businesses and society

Page 6

03

Rules and standards for using AI

Page 8

04

Our services for using AI for innovation and to protect consumers – across sectors and internationally

Page 12

05

With our locations across the world, we contribute to the secure development of AI

Page 14

06

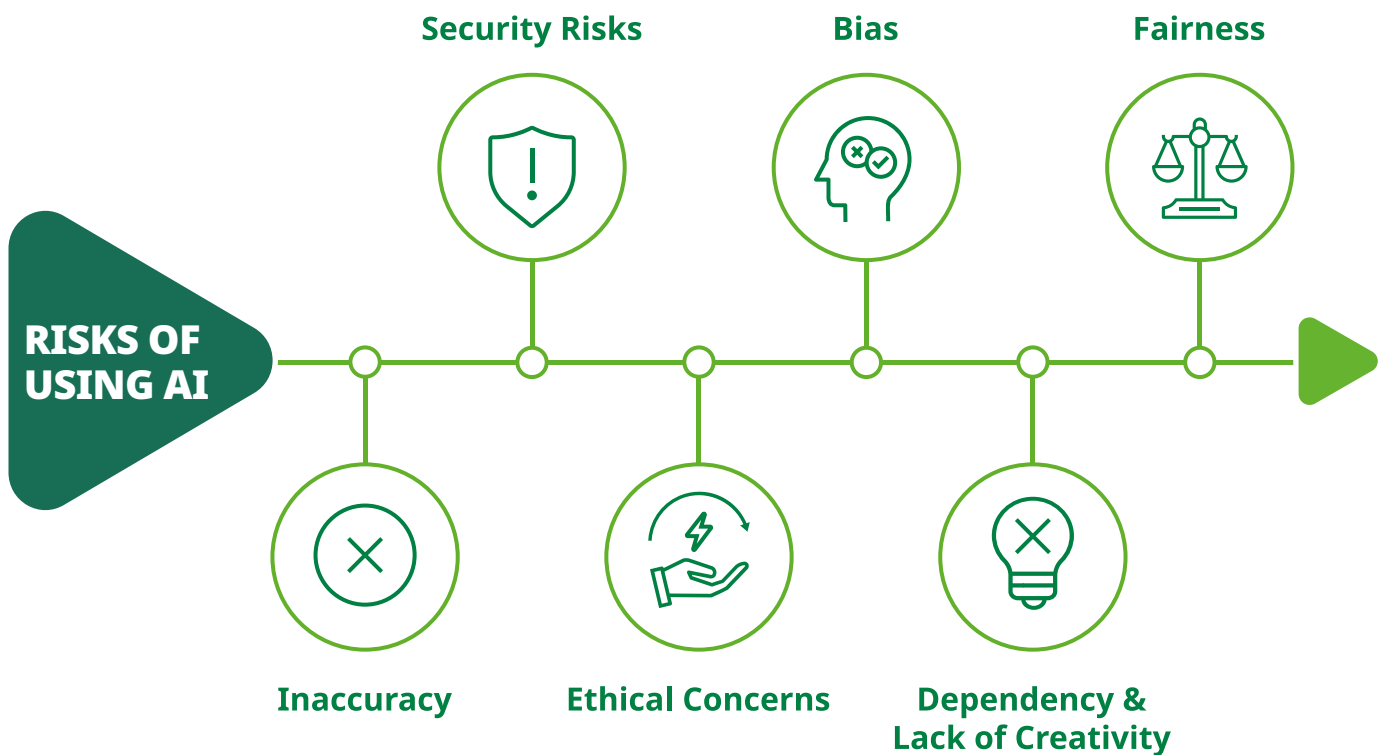
In focus: Cybersecurity

Page 15



2. AI's challenges for businesses and society

- The progressive introduction of AI systems holds great potential for social benefits, economic growth, and the promotion of innovation and global competitiveness, as well as sustainability both worldwide and within the EU.
- However, it is also clear that in certain cases, the specific characteristics of certain AI systems can pose new risks to democracy and fundamental rights. The systematic risks of powerful AI models that are used on a large scale are also well known.





Possible threats to **fundamental rights and democracy**

- Compromising security and impacting the protection of people: As AI technologies become more and more complex, the associated security risks and the potential for misuse and cyberattacks, including physical harm, may also increase. Manipulation and disinformation can also be caused by AI-generated deepfakes.
- Transparency: Lack of transparency due to the complexity and non-transparency of the data used.
- Discrimination: Algorithms can trigger or cement social prejudices.
- Data privacy: AI technologies often collect and analyze large amounts of personal data, raising privacy and data security concerns.
- Ethical issues: Ethical values are anchored in AI systems.

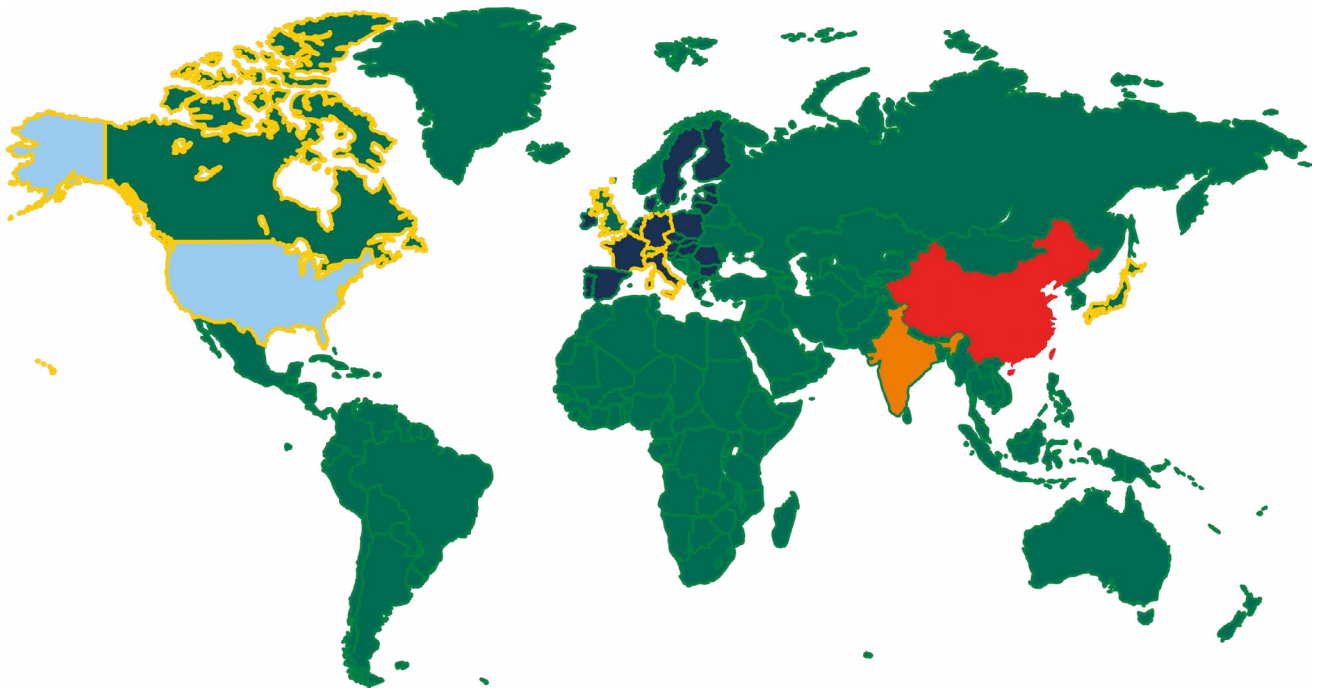
3. Rules and standards for using AI

“AI is nothing new – in view of the progressive global market penetration into all areas of life, companies and citizens increasingly need legal certainty and protection to enable and drive forward innovations. This is the essential prerequisite for the acceptance of innovations.

The aim should be to transform voluntary commitments into globally binding laws. The European Union has made a vital advancement here with the world’s first horizontal legislation: the EU AI Act.”

Examples of regulatory approaches in the field of AI

Overview of current regulatory initiatives (selection)*



Source: Own Illustration

- EU AI Act
- India – Non-regulatory approach to AI
- US Executive Order
- G7 AI Code of Conduct
- China – AI governance framework

* The information shown on this map is a snapshot from May 2024. Due to the dynamic and fast-moving nature of this area, changes may occur that are not reflected in this map.

G7 Code of Conduct for Organizations Developing Advanced AI Systems

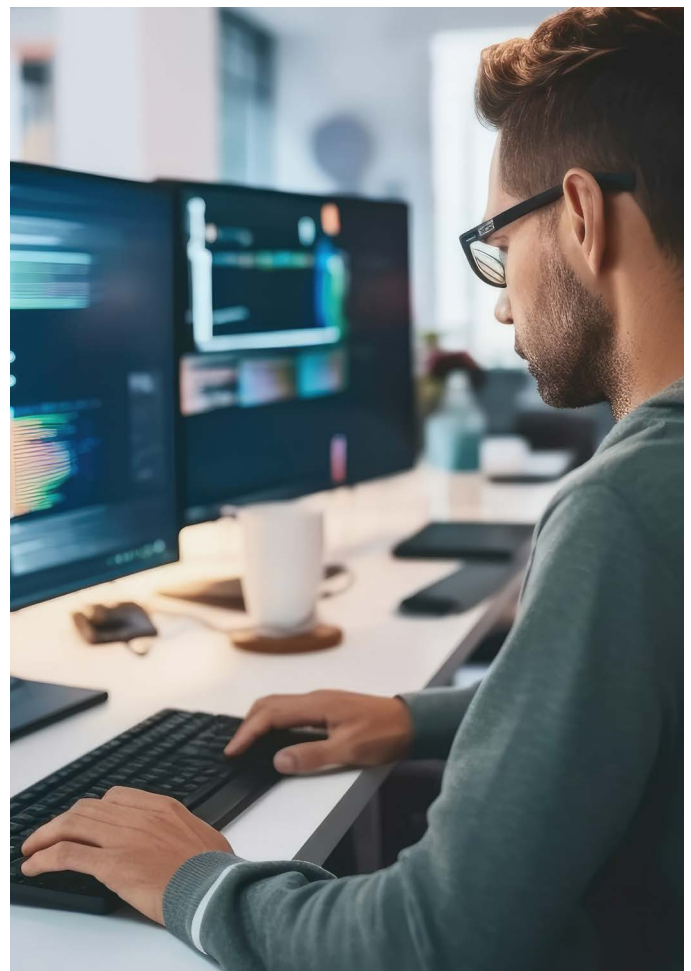
- The International Code of Conduct is intended to promote secure and trustworthy AI worldwide and to provide voluntary guidelines for action by organizations developing advanced AI systems, including the most advanced baseline models and generative AI systems.
- To this end, the G7 countries signed the Code of Conduct on October 30. By adhering to eleven principles, signatories agree to respect democracy and human rights. Data should be handled responsibly and protected, and copyright should be maintained.
- The signatories agree on a risk-based policy to ensure security in view of the risks associated with AI. It offers a platform for cooperation, but also mutual recognition of national differences.

Executive Order (EO) on AI by the US government, October 30, 2023 – legally binding in parts – focus USA

- The Executive Order sets out new standards for the security of AI – including protecting privacy, ensuring equality and civil rights, promoting innovation and competition, and much more.
- The developers of very powerful AI systems are required to share the results of their security tests and other important information with the US government. Furthermore, standards, tools, and tests are to be developed to ensure that AI systems are secure and trustworthy.
- More than 80% of the major AI models originated in the United States. The Executive Order (EO) is particularly relevant to the AI ecosystem in the US. This decree can build a bridge to EU legislation.

AI Safety Summit/Bletchley Declaration November 1, 2023 – voluntary declaration of intent

- Comprises 28 countries (including the US, China, and the EU) that have committed to working together on AI regulation. The Bletchley Declaration sets out requirements for the global tech industry to provide appropriate benchmarks

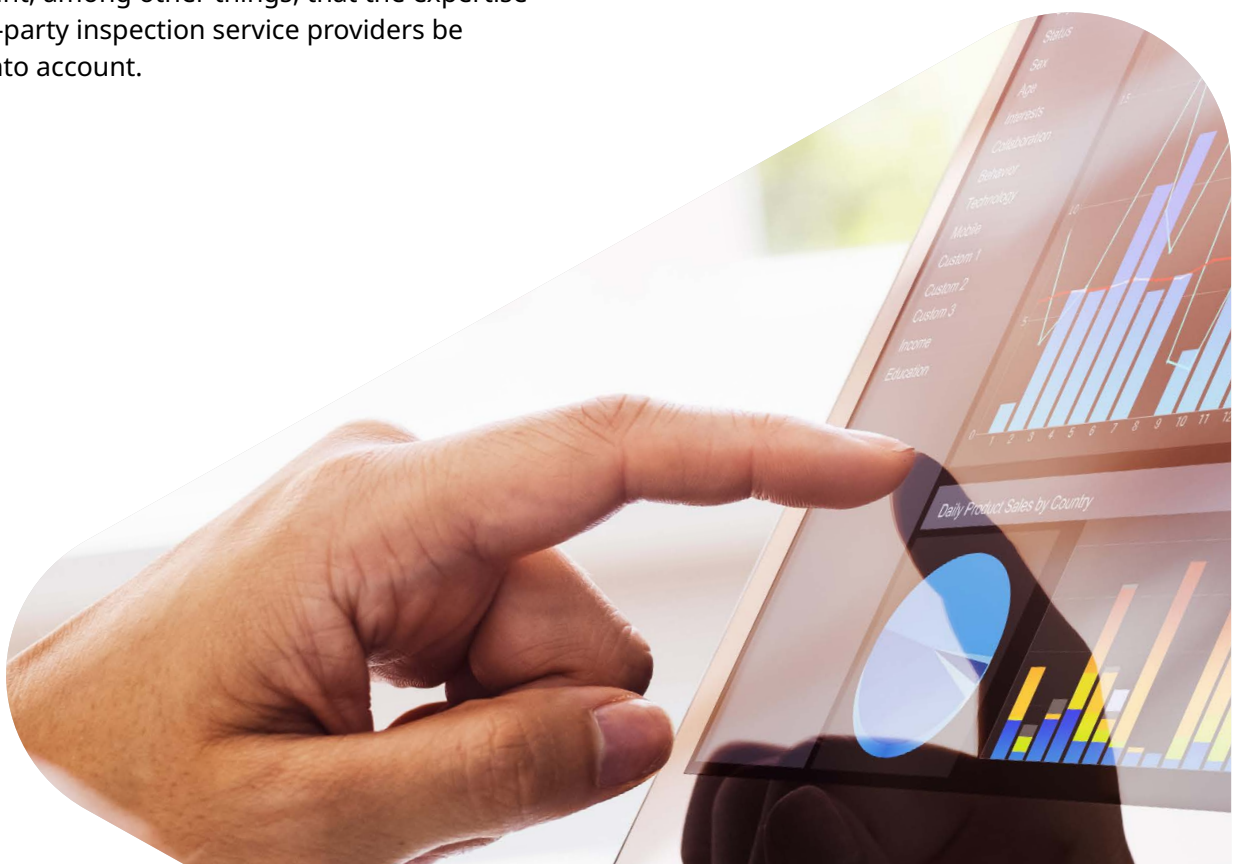


EU AI Act: Proposal of the EU Commission from 2021 – **legally binding for EU member states**

“As an independent testing organization, DEKRA fosters trust and is therefore an essential partner in implementing technological innovations – this includes all industries and sectors, from the automotive industry to the banking sector.”

“The EU AI Act will require a large number of adjustments and changes to the respective legal frameworks – including in the automotive sector, as well as the amendment of the EU type approval system.”

- On December 9, 2023, the European Commission, the European Parliament, and the 27 EU member states agreed in the Council on the world’s first horizontal legislation on the regulation of AI.
- The proposed Regulation (EU) 2021/206 follows a risk-based approach. Its aim is to introduce a proportionate and effective set of binding rules for AI systems. For the first time, the AI Act thus also lays down requirements for the protection of fundamental rights and functional security.
- DEKRA welcomes the envisaged strong legal framework, which enables conformity assessment procedures for new products to meet the highest monitoring, quality assurance, and consumer protection standards used by independent testing organizations.
- For its implementation at a national level, it is important, among other things, that the expertise of third-party inspection service providers be taken into account.
- AI law and type approval: AI will also play an important role in vehicles and will be used in driver assistance systems and autonomous driving, for example. With regard to the type approval of vehicles and in view of the potential risks of AI applications in AVs, AI systems should also be classified as safety components.
- Reference should be made here to UN Regulation 155 (Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system) and UN Regulation 156 (Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system), among others.



AI-related standards

“The EU AI Act also goes hand in hand with the development of new standards – the aim here is to take tried-and-tested standards into account and shape new ones. Common standards are the practical basis for daily business and are therefore intrinsically important.”

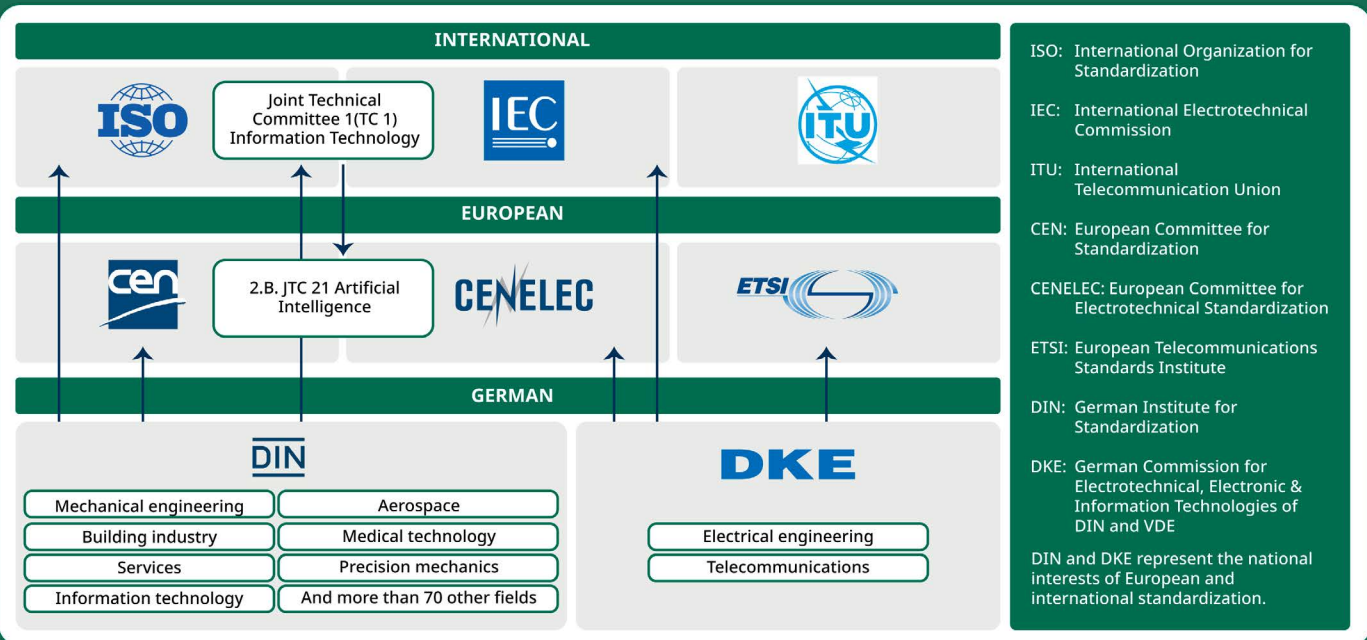
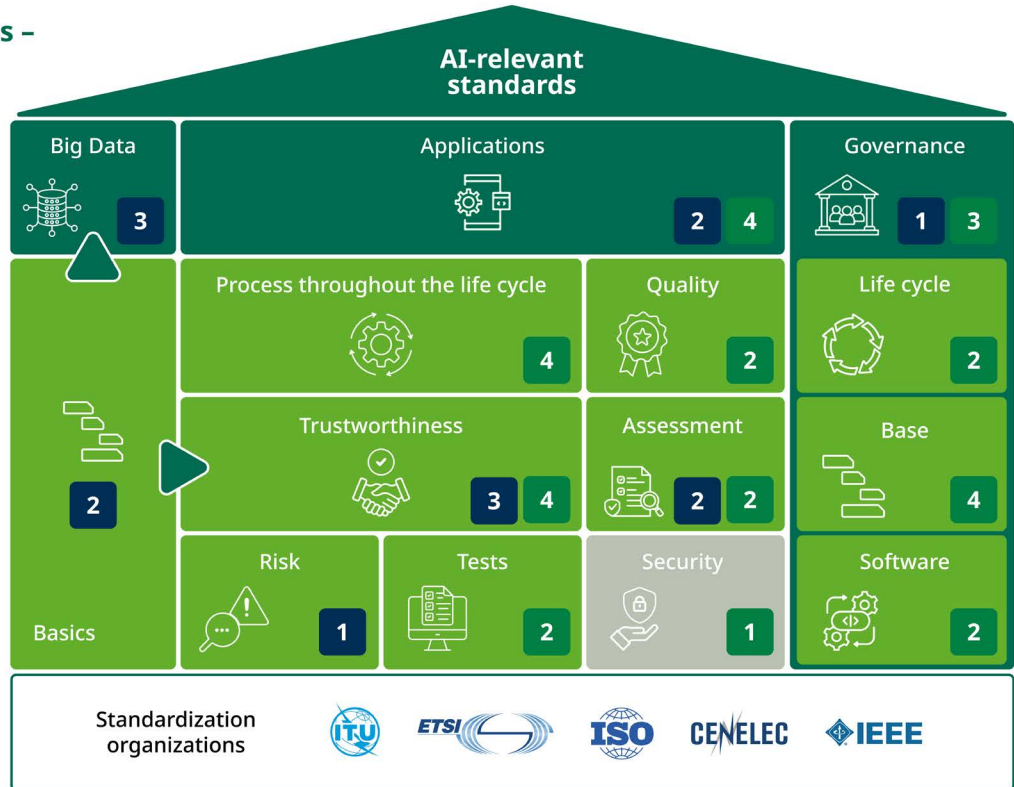
AI-relevant standards – a large “structure”...

AI solutions rely on established basic technologies for which norms and standards already exist.

There are a large number of initiatives for segment-specific use cases that form a broad foundation for various standards.



Compass required for navigation.






4. AI for innovation and to **protect consumers**

Our cross-sector and international services

- DEKRA offers comprehensive AI assessment services that cover the entire lifecycle of AI systems, including the development, validation, and operational phases necessary for successful AI.
- Our expert audits identify risks and weaknesses, and use risk assessment plans to ensure security.
- DEKRA offers professional consulting and training services to get companies “fit for AI”. In this context, we also support companies in implementing AI management systems.
- Our experts provide assistance with the implementation of upcoming AI regulations and assess their impact on the business and product portfolio. We equip companies with the necessary knowledge and experience to effectively and securely manage the use of AI in line with the new regulations.
- The first generation of AI testing and certification covers a wide range of services for assessing the security of AI solutions. The primary aim is to carry out conformity assessments and ensure the highest security standards.

1st Generation AI Testing & Certification Services

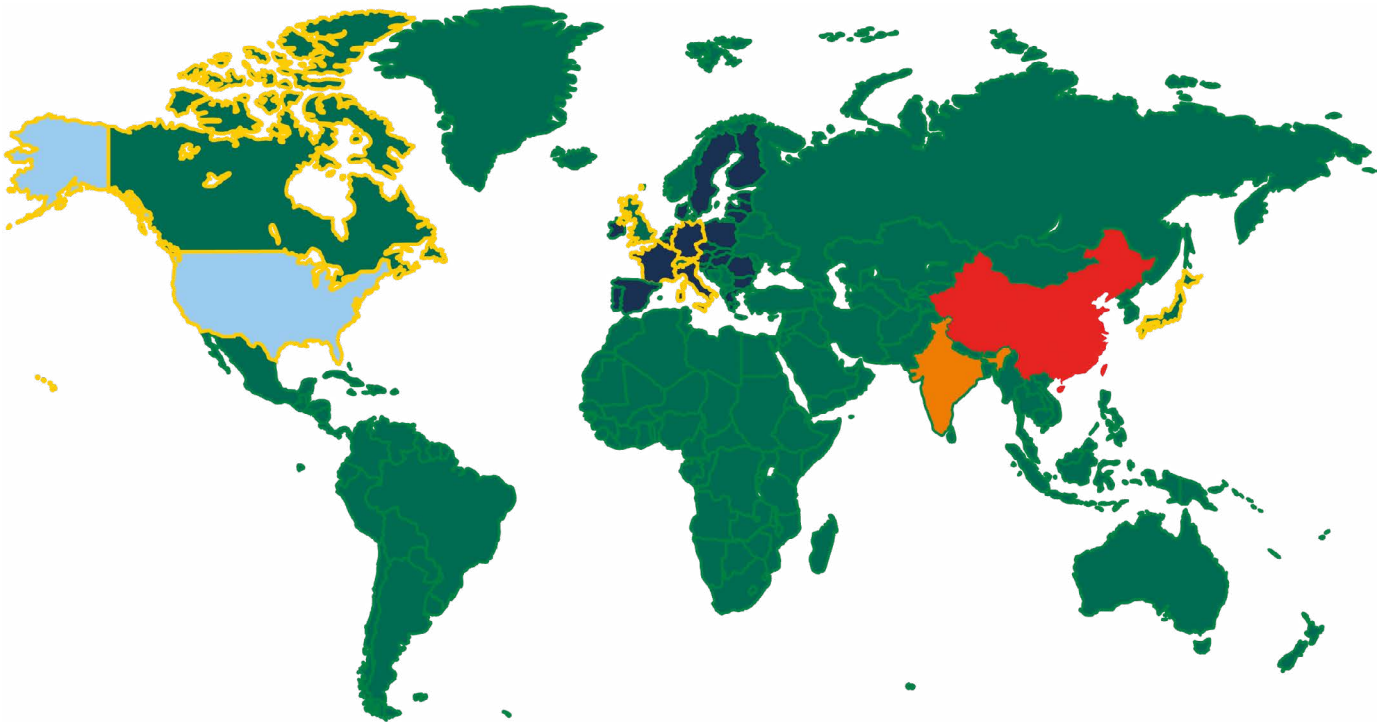
▶ TRAINING & PRE-ASSESSMENTS	▶ ASSESSMENTS	
AI Training & Advisory 	AI Audit & Certification 	AI Testing 
<p>Expert training and pre-assessment services on multiple aspects related to AI technology and regulations</p> <ul style="list-style-type: none"> ▶ AI Risk Awareness ▶ AI Regulations and Standards ▶ Trustworthiness & Ethics ▶ Readiness assessment (DEKRA AI Ready) 	<p>Assessment and conformity with respect to standards and good practices for development and operationalization of AI solutions.</p> <ul style="list-style-type: none"> ▶ Management Systems (ISO 42001) ▶ AI Risk management (ISO 23894) ▶ Data Labelling Assessment (ISO 5259-4) ▶ Road Vehicles Safety&AI (ISO 8800) ▶ A-Spice Machine Learning 	<p>Our expert AI testers conduct thorough assessment leveraged by cutting-edge Software tools.</p> <ul style="list-style-type: none"> ▶ Data Quality (ISO 5259) ▶ Model Robustness (ISO 24029) ▶ AI Bias & Fairness (ISO 24027) ▶ AI Security

Business case

1. In early 2024, DEKRA and LatticeFlow announced the first commercial AI assessment for Migros Bank, a leading Swiss bank, to develop the practical framework for comprehensive AI assessments in compliance with the latest ISO standards for data quality and model robustness. To achieve this, DEKRA is using the AI Readiness Framework to audit the AI system. Our task is to ensure the integrity and quality of the AI system – in other words, to ensure compliance with future regulations at all times and to minimize risks.
2. DEKRA supported the LTS Group, a leading player in the AI and ADAS systems field, in certifying the quality of the data labeling processes of its services, and conducted an assessment according to ISO/IEC 5259-4. This standard provides guidelines and frameworks for the assessment of data quality in the context of machine learning and analytics.



5. With our locations across the world, we contribute **to the secure development of AI**



Source: Own Illustration

“DEKRA offers AI services and cybersecurity solutions worldwide. We use our independent expertise as well as our cross-sector and cross-industry knowledge. We operate globally. In order to address the German market, one of the largest and most important markets, DEKRA decided to join forces with PwC Germany and the City of Hamburg’s Innovation Fund to establish the CertifAI joint venture.”

6. In focus: **Cybersecurity**

Cyberattacks on hardware and software cost the global economy 5.5 trillion euros every year. BITKOM estimates the damage in Germany alone to be 203 billion euros annually. The Federal Office for Information Security's (BSI) Situation Report on IT Security in Germany 2023 revealed the national situation to be 'tense to critical' for the current reporting period. The threat in cyberspace is therefore higher than ever before.

Top 3 threats for each target group

Society



Identity theft

Sextortion
Phishing

Economy



Ransomware

Dependency within the IT supply chain
Vulnerabilities, open or incorrectly configured online servers

State and administration



Ransomware

APT vulnerabilities, open or incorrectly configured online servers



Around **21,000** infected systems were detected and reported to the German providers by the Federal Office for Information Security (BSI) every day during the reporting period.

On average, around **775** emails containing malware were intercepted in German government networks every day during the reporting period.



An average of **370** websites were blocked from being accessed from government networks every day during the reporting period. **The reason:** The pages contained malware.



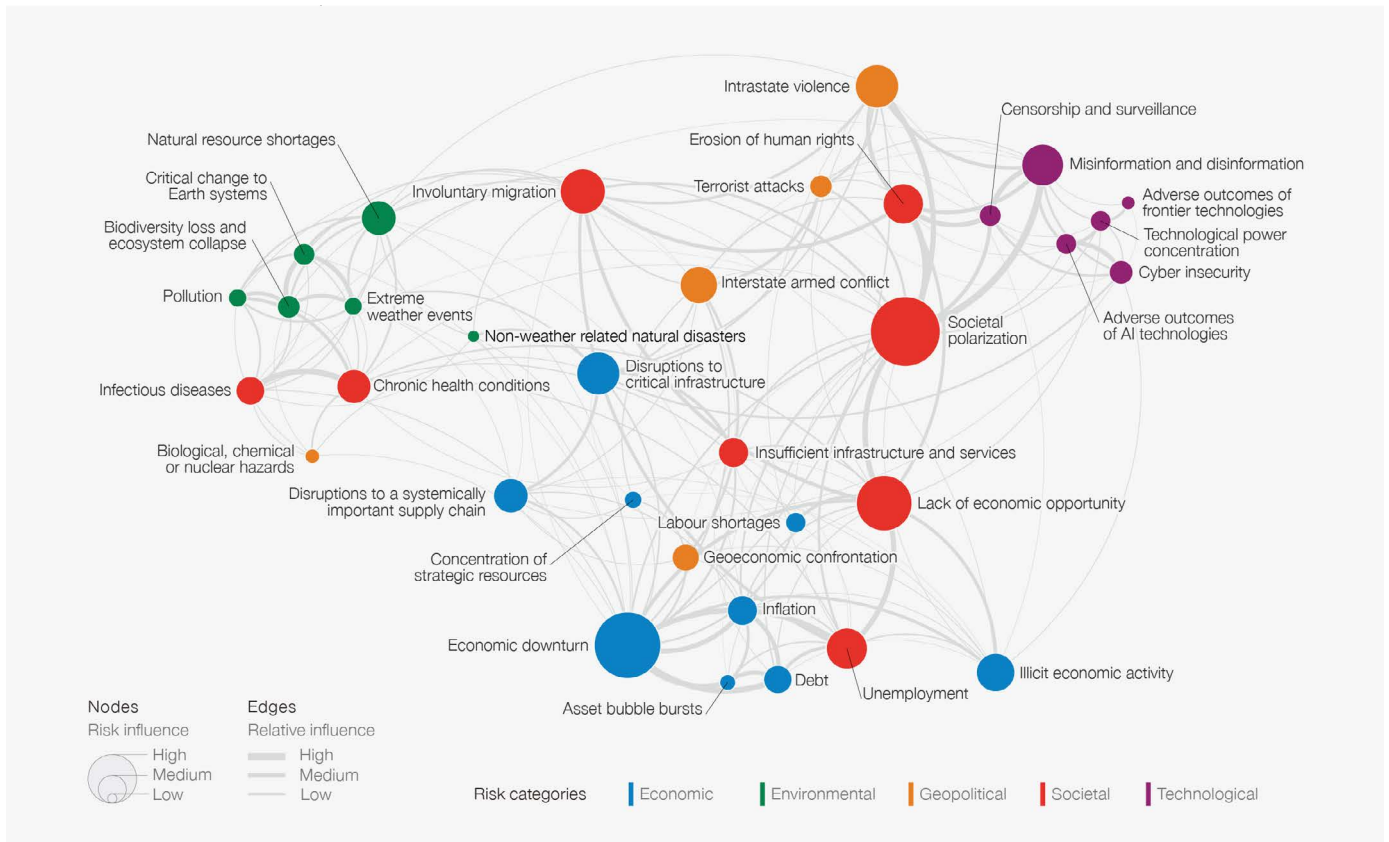
6,220
2022

5,100
2021



7,120
The Alliance for Cyber Security had 7,120 participants in 2023.

Deutschland
Digital•Sicher•BSI



Source: [WEF The Global Risks Report 2024](#)

The 19th edition of the report focuses on the accelerating technological change and economic uncertainty as the world faces two major crises: climate and conflicts.

With its services in the areas of sustainability, cybersecurity, and AI, DEKRA is helping to make our world more secure, cleaner, and more sustainable. The company is thus responding decisively to critical research findings and positioning itself as an important part of the solution to global challenges.

Our expertise in cybersecurity

We support companies in protecting their digital infrastructure as part of the implementation of the Directive on Security of Network and Information Systems and the imminent implementation of the Cyber Resilience Act. A key factor is that the TIC sector is firmly anchored in the legal framework as an independent testing organization. In this way, we contribute to security, maintain our scope as an enabler for companies, and can relieve the burden on supervisory authorities. With more than seven years of experience in cybersecurity services, DEKRA has established a solid global presence in Taiwan, China, Japan, Europe, and the US. Our customers include industry giants such as Amazon, Apple, Google, BYD, BMW, and Continental. Last year, the company doubled its workforce.

- Our experts are committed to the highest possible level of security. In this context, DEKRA cybersecurity services cover the entire product life cycle and include testing, assessment, and certification according to generally recognized cybersecurity standards such as Common Criteria (ISO 15408), FIPS 140-3 (ISO 19790), eIDAS regulation, LINCE, and GSMA - NESAS 3GPP.
- With this in mind, DEKRA's role includes validating the cybersecurity of products and applications for the suppliers of global tech companies. DEKRA was also one of the first accredited certification bodies in Germany to offer cybersecurity services for car manufacturers.
- The legislative framework is an important factor in ensuring that DEKRA, as an independent testing service provider, can contribute to the protection of digital infrastructures in Germany and thus also support downstream authorities.

Locations of the cybersecurity labs





Legal notice

Date Version: 06/2024
Contact Dr. Fabienne Beez
Phone +49 30 986098810
Email fabienne.beez@dekra.com

DEKRA e.V.
Berlin office
Behrenstrasse 29
www.dekra.de/presse





DEKRA

Handwerkstrasse 15

70565 Stuttgart

Tel +49 711 7861-0

Tel +49 711 7861-2240

dekra.de