ISSN: 3067-2317
Research Article

World Journal of Artificial Intelligence and Robotics Research

AI Competencies for Companies: Definition, Taxonomy and Regulatory Classification

Paul R. Melcher[1]*, Daryoush D. Vaziri[2]

[1]Professor for integrated management systems at University of Applied Science Grantham-Allee 20 D-53757 Sankt Augustin (Germany)

[2]Head of Research Group on Development of human-centered AI-based Systems Head of Digital Sovereignty and AI-Trainer in Mittelstand Digital Fokus Mensch

***Corresponding author:** Prof. Dr. Paul R. Melcher, Professor for integrated management systems at University of Applied Science Grantham-Allee 20 D-53757 Sankt Augustin (Germany).

Submitted: 24 March 2025 **Accepted:** 28 March 2025 **Published:** 08 May 2025

https://doi.org/10.63620/MK.WJAIRR.2025.1012

Citation: *Melcher, P. R., Vaziri, D. D. (2025). AI Competencies for Companies: Definition, Taxonomy and Regulatory Classification. Wor Jour of Arti inte and Rob Res, 2(3), 01-09.*

Abstract

Every authority, organization, and company worldwide is currently facing the challenge of determining which applications of artificial intelligence (AI) are meaningful. This article lists application examples to demonstrate the opportunities. It also explains the difference between GPAI models and GPAI systems. The risk classification follows the risk classes defined in the AI Act in Europe. To ensure trustworthy application and risk limitation, an overview of the most important international standards is provided. Based on the international concept of competence, "AI competencies" are defined and formulated along the competence levels according to BLOOM's taxonomy. These AI competencies are assigned to different functional roles in organizations and companies. Using six typical application examples—from simple users to AI system manufacturers—the required AI competencies are mapped to both international standards and the risk classes from the European AI Act. Finally, eight recommendations for AI implementation are provided that are useful for any organization or company.

Keywords: AI, AI Act, AI Competence, AI International Standards, AI Risk Classes, European AI Regulation, AI Recommendations for Action.

Introduction and Problem Statement

Currently, authorities, organizations, and companies are confronted with questions about possible applications of artificial intelligence, hereinafter referred to as AI. According to a survey of 1,750 companies (approximately 50% worldwide and 50% in Europe) 21% are currently working on implementing AI while 79% are not [1]. The same distribution of figures resulted from a survey by McKinsey & Company of 1,000 German companies: Only 21% of all employees would have basic AI competencies while 79% lack basic AI competence [2].

Thus, every board, management, department head, or executive has been facing the same issues since the breakthrough of Chat GPT in 2022, accompanied by the emergence of worldwide AI standards and the AI Act in Europe through the further implementation stage of the European Regulation on February 2, 2025:

1. Which applications are conceivable and useful with AI as an opportunity?
2. How are risks controlled when applying AI by complying with international standards or the requirements of the AI Act in Europe (EU) 2024/1689?
3. Which AI competencies are required in the organization or company and need to be developed?
4. Which responsibilities need to be defined in the organizational and operational structure?

Worldwide, several internationally valid standards for the trustworthy and secure use of AI for the benefit of people have already been published [3]. The European Union achieved a historic milestone on August 1, 2024, by implementing comprehensive regulation of AI to protect people living in Europe. Following this regulation (EU) 2024/1689 applicable in Europe, the application of prohibitions regulated in the AI Act began on

February 2, 2025. In addition, on August 2, 2025, the application of the requirements regulated in the AI Act for GPAI models and GPAI systems will begin.

A GPAI model means a General-Purpose Artificial Intelligence model and is defined according to (EU) 2024/1689 as "an AI model trained on broad data, oriented toward general output, and adaptable to a wide range of different tasks." A typical example is the model developed in America with the name "Chat GPT" as the world-leading language model from 2022 to 2024.

The competing model "Deep Seek," developed in China since 2023, has taken the top position in January 2025 [4].

The marketing and/or application of AI models takes place via libraries, application programming interfaces (API), through direct download or (rarely) via a physical copy [5].

A GPAI system is defined by [5] as an AI system based on an AI model that can be used for a variety of purposes, both for direct use and for integration into other AI systems." According to Article 3 of (EU) 2024/1689 [3], an "AI system" is defined as: "a machine-based system that is designed to operate with varying degrees of autonomy and that may be adaptable after its deployment and that derives from the inputs received-for explicit or implicit goals and produces-outputs such as predictions, content, recommendations, or decisions influencing physical or virtual environments."

For example, voice control in an automobile could activate the windshield wiper and adjust the wiping frequency according to the rain or moisture on the windshield. The difference between an AI model and an AI system is illustrated in Figure 1.

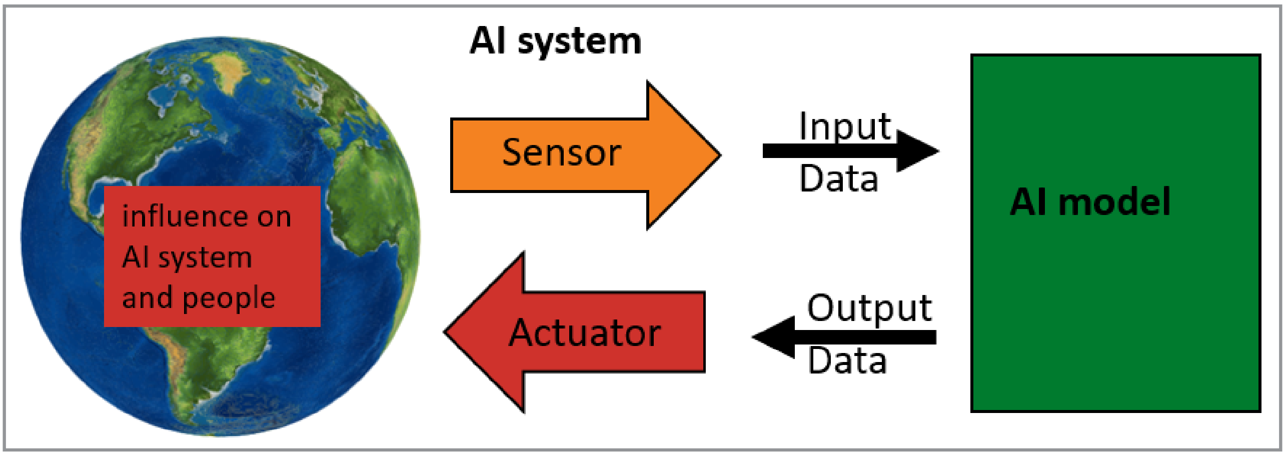

Figure 1: Difference Between AI Model and AI System (Own Illustration)

Competencies for Recognizing Opportunities

For all those working in organizations, companies, or authorities, it is now important to recognize the diverse application possibilities of AI. The goal is to identify which tasks, activities, problems, processes, or business procedures can be meaningfully and resource-efficiently automated with AI. This requires experience and understanding of the existing business model and process management in the organizational structure. Through the consistent continuation of LEAN management and value stream analysis, many improvements can be achieved by analyzing big data. However, completely new areas of application for solving problems or optimizing processes and products as well as systems are also emerging. This requires creativity as a main competency.

A variety of "uses" cases is described in ISO/IEC TR 24030 [6]. An overview of AI application possibilities is listed by the authors in Table 1 alphabetically.

Table 1: AI Application Possibilities in Organizations and Businesses from A to Z

	Application Possibility	Description	Created Outcome
A	Analysis	Detailed data evaluations,	New results
B	Business Image Recognition	Automatic defect detection	Security monitoring
C	Chatbots	24/7 customer support	Integration into various communication channels
D	Document Management	Automatic classification and filing	Intelligent search functions
E	Explanatory AI	Automatic creation of multilingual instructions	Automated user documentation
F	Frequently Asked Questions AI	Automated responses through AI-powered knowledge databases	Faster employee and customer issue resolution
G	Governance & Workflow Optimization	Optimization and automation of workflows	Increased operational efficiency
H	Holographic Training	Virtual product demonstrations	Enhanced interactive learning experiences
I	Intelligent Information Analysis	Real-time data analysis	Improved strategic decision-making
J	Judgment-Based Financial Reports	Automated creation of business and financial reports	Data-driven corporate decision-making
K	Knowledge-Based Engineering	Generative design	Real-time simulation and risk minimization
L	Learning Management System	Learning platform and knowledge management	Personalized employee training
M	Machine Learning Pattern Detection	Anomaly detection, fraud detection in financial transactions	Increased security and fraud prevention
N	Next-Gen Knowledge Systems	Intelligent knowledge management systems	Quick and accurate information retrieval
O	Optimization Strategies	Dynamic optimization of resources	Cost reduction and resource efficiency
P	Predictive Quality Control	Automated quality control	Higher production accuracy and reduced waste
Q	Quality Assurance AI	Real-time monitoring and reporting	Enhanced compliance and production standards
R	Robotics & AI Navigation	Self-learning robots	Autonomous operation
S	Smart Correspondence Processing	Automatic creation and analysis of correspondences	Improved document organization and tracking
T	Text Recognition & Summarization	Automatic transcription	Faster access to critical information
U	User Experience Enhancement	AI-driven personalization	Increased customer satisfaction and engagement
V	Video Analytics & Training AI	Automatic content analysis	More effective training and security monitoring
W	Workflow Automation AI	AI-assisted process automation	Increased productivity and reduced manual workload
X	X-Adaptive AI Solutions	Flexible application possibilities	Custom AI solutions tailored to business needs
Y	Yearly Performance AI	Automated annual performanceanalyses and evaluations	Improved HR and business Performance monitoring
Z	Zero-Defect Manufacturing	AI-powered quality control	Consistently high-quality products and reduced errors

Competencies for Recognizing, Evaluating and Limiting Risks

The following skills are required here as ability and willingness:

- To recognize potential security risks in data protection and confidentiality to ward off the risk of data leaks and unauthorized access.
- To recognize and evaluate the extent of possible hallucinations
- To recognize and evaluate risks of manipulation through training data
- To recognize and evaluate risks due to bias and discrimination.
- To recognize and assess risks due to lack of transparency or clear accountability.
- To recognize and avoid the risks of misuse, e.g. for mass manipulation and profiling.
- To recognize and avoid the risks of non-compliance.

Traditional risk management methods can be used to identify and assess risks. The identification of risks can range from simple brainstorming to a risk portfolio to the internationally widespread Failure Mode and Effects Analysis (FMEA). The risks logically depend very strongly on the intended use: A chatbot that only answers from verified and defined content is harmless. A robot that performs useful tasks in everyday life and cannot harm humans is low risk. The risk of incorrect decisions by an AI system that takes over autonomous driving of aircraft and vehicles must be lower than the risk of human error. Under no circumstances should AI systems harm, disadvantage, or manipulate humans.

To protect people in Europe, Regulation (EU) 2024/1689 [3] follows a risk-based approach, which aims to ensure that AI systems are regulated according to their potential risk. Depending on the risk class, the 7 requirements increase:

1. Risk management system,
2. Transparency and user information,
3. Recording function,
4. Data quality and governance,
5. Accuracy, robustness, and Cybersecurity,
6. Technical documentation,
7. Human oversight.

There are also 12 duties:

1. Obligations of operators,
2. Obligations of the dealers,
3. Obligations of importers,
4. Responsibility along the value chain,
5. Documentation obligation,
6. Cooperation with authorities,
7. Automatic record keeping,
8. Quality management system,
9. Authorized representatives,
10. Fundamental rights impact assessment,
11. General obligations of providers,
12. Remedial measures and information obligation. The classification into the four risk classes of (EU) 2024/1689 is shown in Figure 2.

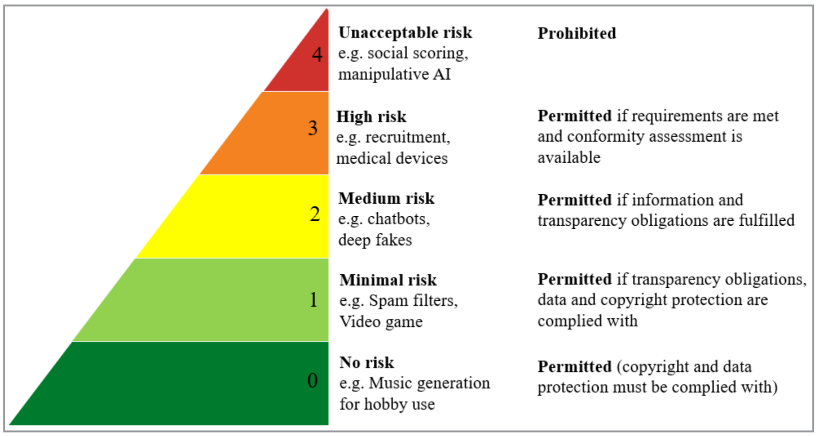
4
Unacceptable risk
e.g. social scoring, manipulative AI
Prohibited
3
High risk
e.g. recruitment, medical devices
Permitted if requirements are met and conformity assessment is available
2
Medium risk
e.g. chatbots, deep fakes
Permitted if information and transparency obligations are fulfilled
1
Minimal risk
e.g. Spam filters, Video game
Permitted if transparency obligations, data and copyright protection are complied with
0
No risk
e.g. Music generation for hobby use
Permitted (copyright and data protection must be complied with)

Figure 2: Classification of Risk Classes for AI Systems According to Risk Class Based on (EU) 2024/1689 [3]

In Europe, the AI Act came into force as law on August 2, 2024. Since February 2, 2025, the ban on operating AI systems with unacceptable risk does apply. An inventory must be made and regulations for dealing with AI must be published. Employees must be trained. From August 2, 2025, the types of AI used and their consequences must be classified. From January 1, 2027, a new Machinery Regulation (EU) 2023/1230 will come into force in Europe, which is important for the cooperation between humans and artificial intelligence and machines as well as robots [7]. From August 2, 2027, the AI Act will apply in full to everyone in Europe.

When developing, offering, trading, and operating AI systems, international standards for the protection of humans should always be observed. Table 2 shows an up-to-date status.

Table 2: Overview of International Standards on Artificial Intelligence

Year	Standard Number	Title
2020	ISO/IEC TR 24028	Overview of trustworthiness in artificial intelligence
2021	ITU-T M.3080	Framework of artificial intelligence enhanced telecom operation and management (AITOM)
2021	ISO/IEC TR 24029	Assessment of the robustness of neural networks (Parts 1–2)
2021	ISO/IEC TR 24030	Artificial intelligence – Use cases (withdrawn version)
2021	IEEE 7010	Recommended Practice for Assessing the Impact of AI Systems on Human well-being
2021	ISO/IEC TR 24027	Bias in AI systems and AI-supported decision-making processes
2022	ISO/IEC 38507	Governance of IT – Governance implications of the use of artificial intelligence by organizations
2022	ISO/IEC 23053	Framework for AI systems using machine learning
2022	ISO/IEC 23053	Framework for AI systems using machine learning
2022	ISO/IEC 22989	Artificial intelligence – Concepts and terminology

2022	ISO/IEC TR 24368	Overview of ethical and societal concerns related to AI
2023	ISO/IEC 23894	Artificial intelligence – Guidance on risk management
2023	ISO/IEC 25059	SQuaRE – Quality model for AI systems
2023	IEC 62243	Cybersecurity requirements for AI-supported industrial automation systems
2023	ISO/IEC 42001	Artificial intelligence – Management system
2023	ISO/IEC 5338	Lifecycle processes for AI systems
2024	ISO/IEC TR 5469	Functional safety and AI systems
2024	ISO/IEC 5469	Functional safety and AI systems
2024	ISO/IEC 5339	Guidelines for AI applications
2024	ISO/IEC 5392	Reference architecture of knowledge engineering
2024	ISO/IEC TR 24030	Artificial intelligence – Use cases
2024	ISO/IEC TS 8200	Controllability of automated AI systems
2024	ISO/IEC TR 17903	Overview of machine learning computing devices
2024	ISO/IEC 5259	Data quality for analytics and machine learning (Parts 1–5)

The most far-reaching and important standard is likely ISO/IEC 42001, as it sets the requirements for a complete management system for certification [8]. The specification for accredited bodies authorized to certify this is currently available as a draft in ISO/IEC FDIS 42006 [9].

AI Competencies

First, the current state is addressed. The definition of "competence" and its requirements in the application of AI is done in line with international standards. Required "AI competencies" are defined along the taxonomy levels from didactics. Subsequently, the required competencies are assigned to groups of people in the company depending on the use case. Finally, the "AI competencies" are assigned to the risk classes of the European AI Act.

Current State

A database search was conducted to identify the state of the art regarding generative AI knowledge [10]. In the current absence of a special AI competence model, the above-mentioned authors defined the following 12 AI competencies:

1. Basic AI literacy
2. Knowledge of generative AI models
3. Knowledge of the capacity and limitations of generative AI tool
4. Skill to use generative AI tools
5. Ability to assess the output of generative AI tools
6. Skill in prompting generative AI tools (prompt engineering)
7. Ability to program and fine-tune generative models
8. Knowledge of the contexts where generative AI is used
9. Knowledge of the ethical implications
10. Knowledge of the legal aspects
11. Ability to continuously learn

Methodological Derivation and Normative Requirements

A competence according to DIN EN ISO 9000 is an "ability and willingness to act". It differs from a qualification, which represents a formally verifiable degree [11]. A competence has three dimensions: theoretical knowledge, practical skills, and goal-oriented behavior.

In didactics, the six competence levels according to the taxonomy of BLOOM (1976) and Anderson & Krathwohl (2001) are often applied [12-14]. The main difference between them is the swapping of the top two competence levels. In contrast to the proposal of Mcnulty, the authors suggest retaining the original version for the AI, as the results created using AI still need to be evaluated. In [15] it was shown which AI competencies should be taught to students in higher education. In organizations and companies, the management and executives must determine and develop the required competencies depending on the use case and role. These are formulated in Figure 3 along the six levels of BLOOM's taxonomy.

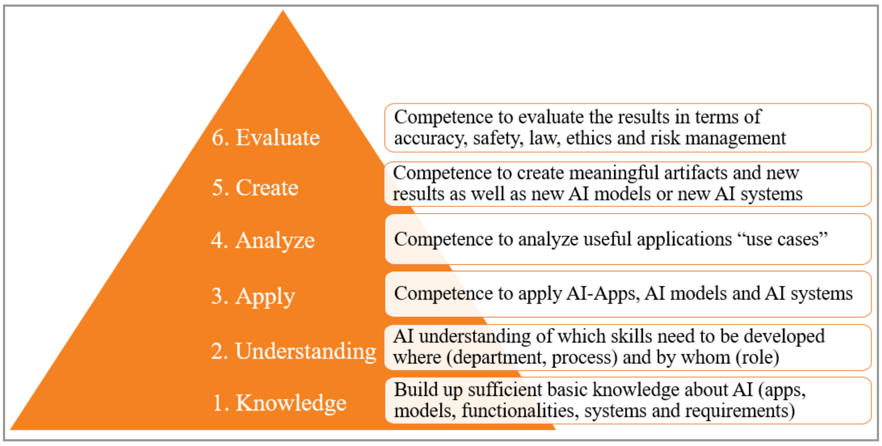
6. Evaluate
Competence to evaluate the results in terms of accuracy, safety, law, ethics and risk management
5. Create
Competence to create meaningful artifacts and new results as well as new AI models or new AI systems
4. Analyze
Competence to analyze useful applications “use cases”
3. Apply
Competence to apply AI-Apps, AI models and AI systems
2. Understanding
AI understanding of which skills need to be developed where (department, process) and by whom (role)
1. Knowledge
Build up sufficient basic knowledge about AI (apps, models, functionalities, systems and requirements)

Figure 3: AI Competences Assigned to the BLOOM Taxonomy (Source: Created by the Authors)

In ISO/ICE 42001 [8], chapter 7 sets out the requirement: "the organizations shall

- determine the necessary competence of person(s) doing work under its control that affect its AI performance;
- ensure that these persons are competent based on appropriate education, training, or experience;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken. Appropriate documented information shall be available as evidence of competence."

According to (EU) 2024/1689 [3] Art. 3 No. 56, an AI competence is conceptually defined as "the skills, knowledge, and understanding that enable providers, operators, and affected parties, taking into account their respective rights and obligations under this regulation, to use AI systems in an informed manner and to be aware of the opportunities and risks of AI and potential harm it may cause."

Definition of AI Competencies and their Assignment to Groups of People (Roles)

In (EU) 2024/1689 [3], Article 4 "AI Competence" consists of the following long sentence: "Providers and operators of AI systems shall take measures to ensure to the best of their ability that their staff and other persons involved in the operation and use of AI systems on their behalf have a sufficient level of AI competence, taking into account their technical knowledge, experience, education and training, and the context in which the AI systems are to be used." Therefore, AI competencies in Table 3 are described more extensively by the authors and assigned to functions in organizations and companies as well as to the roles mentioned in the AI Act.

Table 3: AI Competencies Along the Taxonomy Levels with Assignment of Corporate Roles

Competence Level & AI Competencies	Role according to (EU) 2024/1689
0. None or incompetent behavior: • No knowledge about AI or incorrect understanding • No ability to use AI applications • Misinterpretation of AI results	Private individuals, Majority of the global population
1. Knowledge: • Basics of AI applications (rule-based systems, machine learning, generative AI) • Difference between AI model, AI agent, and AI system • Awareness of AI risk classes according to (EU) 2024/1689 • Basic knowledge of international standards (ISO/IEC 42001, GDPR, AI Act) • Basics of security (access rights, encryption)	Management personnel, Executives, Data protection officers AI providers, importers, distributors, operators, developers
2. Understanding: • Understanding of how AI algorithms function • Understanding of prompt engineering • Recognizing causes of biases and hallucinations • Categorizing data protection and security risks in AI systems • Interpreting regulatory requirements (AI Act, GDPR, ISO/IEC 27001, ISO/IEC 42001)	Management personnel, Executives, Compliance managers, IT security officers AI providers, importers, distributors, operators, developers
3. Applying: • Use and control of AI models, AI agents, and AI systems • Implementation of data protection measures (pseudonymization, anonymization) • Conducting bias tests and model validations • Documentation of AI decisions • Compliance with regulatory requirements	Management personnel, Executives, AI engineer, Data scientist, IT security manager, AI providers, importers, distributors, operators, developers
4. Analyzing: • Capability to analyze which tasks, activities, problems, processes, and business processes can be meaningfully and resource-efficiently automated by AI • Identifying sources of bias and ethical issues • Examining opportunities and risks of AI usage • Analyzing threats and potential attacks (cybersecurity) • Reviewing regulatory violations and compliance risks	Management personnel, Executives, Auditors, Compliance officers, AI risk managers AI providers, importers, distributors, operators, developers
5. Creating: • Using AI to create artifacts (texts, images, videos, audio, holograms) • Designing secure and transparent AI systems • Developing audit trails for traceability • Implementing automated monitoring mechanisms • Developing governance structures for AI	AI architect, IT manager, Ethics expert, AI architect, IT manager, Ethics expert, AI providers, importers, distributors, operators, developers
6. Evaluating: • Evaluation of content generated by AI (accuracy, ethics, data protection, copyright, AI Act) • Verification of AI agents, models, and systems for compliance with AI Act, GDPR • Conducting internal and external audits (ISO/IEC 42001, ISO/IEC 27001) • Optimization of AI processes based on audit results • Evaluation of critical AI systems for ISO/IEC 42001 certification	Regulatory officers, Executives responsible for AI governance, Auditors, AI providers, importers, distributors, operators, developers

Examples of Typical Use Cases and Assignment to Risk Classes and Competencies

For the AI competencies to be developed, a wide variety of cases can arise regarding the introduction, placing on the market, application, operation, trading, and development of AI apps, AI models, and AI systems, which are listed in Table 4.

Table 4: Typical Use Cases with Assignment to the Risk Classes of the AI Act

Use cases	Requirement	Assignment to risk classes & competences
Example 1 No AI application available or in operation.	No operational application, therefore only the rapid development of AI should be observed here.	No risk - no need for AI expertise.
Example 2 Operator as user of AI models in service use.	Internal, mostly standardized use, in which basic data and copyright protection as well as security aspects should be observed.	Low risk class - focus on basic knowledge (e.g. GDPR, data minimization) and initial practical applications (e.g. password protection, encryption).
Example 3 Operators of purchased AI models and AI systems for purposes within the organization or company.	AI solutions used internally, but which may involve more complex processes and data flows.	Medium risk class - Requires a deeper understanding of correlations (e.g. bias sources, secure data processing) and the use of measures (e.g. bias checks, pseudonymization).
Example 4 Operators of AI models or AI systems with which external parties are affected	High external relevance, as decisions or processes can have a direct impact on third parties.	High risk class - Includes advanced skills (e.g. understanding security requirements, carrying out penetration tests, monitoring) and the integration of regulatory requirements (e.g. AI Act, ISO/IEC standards).
Example 5 Suppliers or distributors who sell AI models or AI systems on the market and thus place them on the market	Market launch and distribution require not only technical understanding, but also in-depth knowledge of governance, compliance and security in order to meet external requirements.	High risk class - Also high demands in terms of security, compliance and governance (e.g. implementation of security frameworks, audits, compliance with DIN SPEC and ISO/IEC standards).
Example 6 Developers who develop software for AI models or AI systems and should therefore follow the rules of Amershi et al. [17]	Developers have a responsibility to design systems securely and ethically from the outset. In doing so, they must consider both technical and normative aspects.	High risk class - Developing requires high levels of competence (from analyzing to creating to evaluating), e.g. when implementing security requirements, integrating feedback processes and adhering to best practices.

AI Competencies and their Assignment to the Risk Classes of the AI Act

Article 4 AI competence of (EU) 2024/1689 [3] states: "Providers and operators of AI systems shall take measures to ensure, to the best of their ability, that their personnel and other persons involved in the operation and use of AI systems on their behalf have a sufficient level of AI competence, taking into account their technical knowledge, experience, education and training and the context in which the AI systems are intended to be used and the persons or groups of persons with whom the AI systems are intended to be used."

In Table 5 the AI Competencies are assigned to the Risk Classes of (EU) 2024/1689 [3] according to the Taxonomy of BLOOM [12].

Table 5: AI Competencies for the Risk Classes of the EU AI Act.

Competence level	Competencies for Low risk class	Competencies for medium risk class	Competencies for High risk class
1. Knowledge	DSGVO basics Data minimization Consent procedure Access restrictions	Bias sources unequal data distribution Documentation Security issues	AI Act, DSGVO, ISO/IEC 27001, ISO/IEC 42001 Security requirements
2. Understanding	Possible applications System limits Errors due to incorrect data input	Bias due to incomplete data Secure data processing	Understanding the links between Security, ethics, data protection Understanding High-risk AI threats
3. Apply	Password protection Encryption Transparent Data storage	Bias checks Representative data selection Pseudonymization Data protection	Penetration tests Monitoring Implementation ISO/IEC 42001 requirements DIN SPEC 92001-3

4. Analyze	Missing/incorrect identify data	Bias sources Check safety measures Check safety measures	Decision-making processes Discrimination risks
5. Create	Data validation models Basic documentation	Governance (ISO/IEC 38507) Security Controls	Security framework System optimization Audits Documentations ISO/IEC 42001
6. Evaluate	DSGVO check Data minimization Access control Effectiveness of the basic security	Tests for bias freedom Security checks ISO/IEC 23894:2023	Audits (ISO/IEC 27001, ISO/IEC 42001) Audit (IDW PS 861) Feedback integration

Recommendations for AI Implementation in Companies and Organizations

Even if no AI is currently being used in the organization or company, there should at least be instructions for all employees that no personal or customer-related data, no company-owned or copyrighted data or documents from other sources may be uploaded to large generative language models (LLMs). Finally, the following recommendations are given:

- Analysis of the CURRENT state, which tasks, activities, problems, processes, or business processes can be meaningfully and resource-efficiently automated with AI as an opportunity.
- Use of an open-source model as a host on your own server, because a small model with lower power consumption is already sufficient for most use cases.
- Assignment of the use cases of AI models, AI agents, and AI systems to the risk classes from the AI Act (EU) 2024/1689 [3].
- Definition of the required AI skills depending on the use case and function (role) in the company. Comparison with existing and to-be-developed AI competencies and their verification.
- Clear allocation of responsibilities and delegations for all AI activities in both the organizational and operational structure.
- Planning and implementation of recurring risk and impact analyses, tests, validations, and evaluations as well as audits.
- Compliance with worldwide standards for AI and ethical aspects. Examination of the need for certification according to ISO/IEC 42001 [9].

Summary and Conclusion

Worldwide, protection of people from criminal or ethically incorrect applications of AI would be desirable. Compliance with international standards and regulation according to the European AI Act help to use GPAI models and GPAI systems for the benefit of humanity. This article addresses the current state and methodically derives the concept of competence. As a result, AI competencies are defined using the taxonomy levels of BLOOM [12]. Depending on the business model of the company, these are assigned to roles such as developer, dealer, operator, or just user in six typical examples to the risk classes of the European AI Act. The final recommendations for action can be used as a checklist by any organization or company.

Like any technological leap, there are also the typical three groups with AI: First, the pioneers who already use AI, develop AI software, or apply it enthusiastically. Second, the large majority who now want or need to deal with the application and integration of AI language models or AI systems. Third, the group that continues to only observe the development or does not consider AI application to be useful. Companies that position themselves among the pioneers in AI usage secure more efficient processes, better decisions, and innovative power. Those who hesitate too long risk falling behind and being overtaken by more agile competitors.

Companies worldwide can voluntarily present their AI applications on the EU website [16] and describe how they have built up the necessary AI expertise. 28 companies had already done so by 28 March 2025.

References

1. DNV (2025). Boosting Skills Essential for Successful AI Implementation, DNV Report Reveals, Det Norske Veritas, View Point. https://www.dnv.com/news/successful-artificial-intelligence-implementationresearch/ .
2. Rampelt, F., Klier, J., Kirchherr, J., Ruppert, R. (2025). KI-Kompetenzen in deutschen Unternehmen. Stifterverband in Kooperation mit McKinsey & Company. https://doi.org/10.5281/zenodo.14637137.
3. Regulation (EU) 2024/1689 Of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) https://eur-lex.europa.eu/legal-ontent/EN/TXT/PDF/?uri=OJ:L_202401689 .
4. Rai, S., Purnell, N. (2025). Was Deep Seek – und warum versetzt es die KI-Welt in Angst und Schrecken? In: Wirtschaftswoche 5. https://www.wiwo.de/technologie/digitale-welt/ki-aus-china-was-ist-deepseek-und-warumv-ersetzt-es-die-ki-welt-in-angst-und-schrecken/30185068.
5. Wendt, D. H., & Wendt, J. (2024). Das neue Recht der Künstlichen Intelligenz: Artificial Intelligence Act (AI Act). Beuth Verlag.
6. ISO/IEC TR 24030 (2024). Information technology – Artificial intelligence – Use cases.

7. Regulation (EU) 2023/1230 OF The European Parliament and of the Council of 14 June 2023 on Machinery and Repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1230.
8. ISO/IEC FDIS 42006 (2025). Information technology – Artifical intelligence – Requirements für bodies providing audit and certification of artifical intellingence management systems. https://www.iso.org/standard/44546.html.
9. ISO/IEC 42001 (2023). Information technology – Artifical intelligence – Management system. https://www.iso.org/standard/81230.html.
10. Annapureddy, R., Fornaroli, A., Gatica-Perez, D. (2025). Generative AI Literacy: Twelve Defining Competencies. In: ACM Journals, Digital Governance: Research and Practise., Vol. 6, No. 1, Article 13. 2025. https://doi.org/10.48550/arXiv.2412.12107 .
11. DIN EN ISO 9000 (2015). Quality management systems – Fundamentals and vocabulary. https://www.iso.org/standard/45481.html.
12. Bloom, B. (1956). Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain. New York: David McKay Company. https://www.scirp.org/reference/referencespapers?referenceid=2924447.
13. Anderson, L. W., Krathwohl, D. R. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives: complete edition. Addison Wesley Longman, 83(3), 154-159.
14. McNulty, N. (2021). How the Best teachers use Bloom´s Taxonomy in their Digital Classrooms. https://www.niallmcnulty.com/2017/11/blooms-digital-taxonomy/
15. Melcher, P. R. (2024). KI-Kompetenzen im Curriculum - Handlungsempfehlungen für Hochschulen. In: Die neue Hochschule (DNH), Heft 3/2024, S. 34-37. https://doi.org/10.5281/zenodo.11203053
16. European Commission (2025): Living repository to foster learning and exchange on AI literacy. https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy
17. Amershi et al. (2019). Guidelines for Human-AI Interaction. CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. Paper No.: 3, Pages 1 - 13 https://doi.org/10.1145/3290605.3300233