# European AI Standards – Technical Standardization and Implementation Challenges under the EU AI Act

Robert Kilian, Linda Jäck, Dominik Ebel*

March 24, 2025

**Abstract**

Harmonized standards are the cornerstone of efficient EU AI Act compliance. This paper presents one of the first systematic analyses of European technical and soon to be harmonized standardization for organizations providing AI systems. Based on in-depth qualitative interviews with 23 leading European organisations developing AI applications across different sectors, such as Mistral and Helsing, and providing transparency regarding the status quo of draft standards, it examines how companies, especially startups and SMEs, are dealing with the contemplated standardization under the EU AI Act and sectoral standardization following vertical product safety legislation. Industry sectors covered include mobility, finance, manufacturing, healthcare, enterprise software, as well as defense and legal tech. Key challenges identified comprise an effective implementation period of only approximately 6 months compared to at least 12 months actually required, an imbalance of participation and influence in standardization committees, double regulation and technical implementation hurdles as well as significant annual costs for harmonized standards compliance. Technical standards are currently reshaping global AI competition and will have a massive influence on the AI landscape as market entry barriers, particularly on startups. Hence, the paper offers concrete policy recommendations based on the revealed challenges for AI providers.

*Robert Kilian is a Board Member at KI Bundesverband (German AI Association), CEO of AI testing provider CertifAI, and teaches digital regulation at Humboldt University Berlin. Linda Jäck is a Policy Officer (Europe) at General Catalyst Institute, Berlin. Dominik Ebel is a Doctoral Candidate in digital regulation at Institute for German and European Company and Commercial Law at Heidelberg University and Founder's Associate at CertifAI.

# Contents

# List of Tables



# 1 Introduction

The European Union's (EU) effort to regulate artificial intelligence (AI) through the EU AI Act[1] represents the first comprehensive attempt to set harmonized legal rules for safe AI development and deployment. As part of this effort, the European legislator has given technical standardization a key role,[2] recognizing that the deliberately abstract nature of high-risk requirements makes them challenging for stakeholders to implement. Hence, AI Act high-risk legal requirements are operationalized by technical standards to make them more prescriptive.[3] This approach follows the New Legislative Framework (NLF), under which product safety regulations define only essential legal requirements specified by voluntary technical standards drafted by industry experts. Adherence to these technical standards provides for a presumption of conformity with the legal requirements.[4] The contemplated standards under the AI Act are serving as an accessible option for demonstrating compliance with state-of-the-art regulatory requirements and can assist in reducing legal uncertainties.[5] By that, they aim to strengthen competitiveness and growth in the internal market.[6] Specifically, standards can support the establishment of equal conditions of competition and a level playing field for the technical design and development of AI systems.[7] Finally, if designed appropriately, they help reduce regulatory implementation costs by streamlining processes and avoiding the need for custom R&D-heavy solutions, making product development and operations more efficient.[8]

However, as of now, there is limited understanding of how the AI Act's technical specification through standardization will affect different industries and market participants. Therefore, this paper explores (horizontal and vertical) European AI standardization challenges and opportunities for organizations, based on in-depth qualitative interviews with organizations building and

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. In the following, we refer to the EU AI Act as AI Act.

[2] See Recital 121 AI Act and the corresponding standardization request following Art. 40(2) AI Act, European Commission, C(2023) 3215 final, 'Commission Implementing Decision of 22.5.2023 on a standardisation request'.

[3] For AI Act implementation of technical standards see Kilian, 'Nationale Spielräume bei der Umsetzung des Europäischen Gesetzes über Künstliche Intelligenz' – Written statement for the 63rd meeting of the Committee for Digital Affairs of the German Bundestag on May 15th, 2024, pp. 12 et seq., https://www.bundestag.de/resource/blob/1002540/2c7af0e644c2d1b19d20896994727736/Kilian.pdf.

[4] C.f. Regulation (EC) No 765/2008; Regulation (EU) 2019/1020; Martini/Wendehorst, 'KI-VO: Verordnung über Künstliche Intelligenz', 2024, Art. 40, § 2 et seq. with further references.

[5] Hacker, 'The European AI liability directives – Critique of a half-hearted approach and lessons for the future', Computer Law & Security Review 51 (2023), pp. 33 et seq.; Kilian/Denga, 'Das Testen und Zertifizieren von KI-Systemen', NJW 2024, 2945 (2948); DIN, 'Standardization Helps Create Innovation-Friendly Framework Conditions for the Technology of the Future', 2019, https://www.din.de/resource/blob/306690/f0eb72ae529d8a352e0b0923c67b6156/position-paper-artificial-intelligence-english--data.pdf; 'German Standardization Roadmap on Artificial Intelligence', 2nd ed., 2022, https://www.dke.de/en/areas-of-work/core-safety/standardization-roadmap-ai.

[6] See Recital 121 AI Act.

[7] European Commission, 'C(2023)3215 – Standardisation Request M/593', Recital 3.

[8] OECD, 'Artificial Intelligence in Society', 2019, https://doi.org/10.1787/eedfee77-en.

releasing AI applications across different sectors. It specifically examines how organizations, particularly startups and small and medium-sized enterprises (SMEs), are dealing with the upcoming technical standardization following the AI Act. Startups and SMEs represent 99% of EU companies but are known to lack resources to participate in standardization processes.[9] Therefore, the paper uncovers notable differences in how different sectors are preparing for these standards, while also identifying common challenges for organizations. The analysis provides insights into how technical standards are reshaping competition and offers recommendations for policymakers. The paper contributes to both the academic discussion on standardization-driven AI compliance and a practical understanding of how technical standards influence innovation in the AI economy.

After first laying out the necessary background on AI standardization under the AI Act and challenges in the said process (2.), the status quo of the process is being analyzed, showing the current (limited) progress on the standardization deliverables under the AI Act (3.). Based on in-depth interviews with 23 organizations (including startups, SMEs, larger corporations and public sector organizations) intending to comply with AI Act high-risk standards across different sectors (e.g., mobility, finance, defense, manufacturing, healthcare / medical), the challenges and opportunities regarding the implementation of these standards are illustrated (4.). Finally, based on the identified challenges, policy recommendations are presented (5.).

# 2 Background

## 2.1 AI Standardization Landscape

There are multiple key stakeholders involved in the global process of AI standardization, the most important being standardization bodies, industry players, civil society groups and scientific organizations. With the emergence of AI as a dynamic and global phenomenon, technical standardization is facing unprecedented challenges.[10] Therefore, these standardization stakeholders can only partially rely on established standards, but leverage them as foundational references while developing new standards.[11] The GPAI Code of Conduct following the AI Act can also be seen as a precursor for high-risk AI standards.[12]

As for standardization bodies, there are three notable committees focusing on AI standardization:

- ISO/IEC JTC 1/SC 42 (AI), a committee organized by the International Organisation for Standardization (ISO) in collaboration with the International Electrotechnical Commission (IEC), has published 34 standards, with 40 still under development.[13]
- IEEE AI Standards Committee, organized within the Institute of Electrical and Electronics

[9] Standict.EU, 'Support to SMEs – SME Mentorship Programme', 2023, https://standict.eu/supporting-smes.

[10] For a more in-depth analysis of challenges with AI standardization from a consumer perspective see Micklitz, 'The Role of Standards in Future EU Digital Policy Legislation: A Consumer Perspective', 2023, https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf.

[11] For example, technical standards like ISO/IEC 27001 on information security or ISO/IEC 23894 on risk management are serving as the foundation for highly specialized standards on AI specifics in these realms.

[12] See for more information European Commission, 'General-Purpose AI Code of Practice', https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice.

[13] ISO, 'ISO/IEC JTC 1/SC 42 - Artificial intelligence', accessed 24 Feb, 2025, https://www.iso.org/committee/6794475/x/catalogue/p/1/u/1/w/0/d/0.

Engineers (IEEE), has produced 12 standards,[14] working on 59 additional standards.[15]

- CEN-CENELEC JTC 21 (AI), a joint committee by the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC), has published 10 standards,[16] with 33 still under development.[17]

On a EU Member state level, the national standardization bodies installed working committees mainly mirroring the work of ISO/IEC JTC 1/SC 42 (AI) and CEN-CENELEC JTC 21 (AI).[18] For Germany, the German Institute for Standardization (Deutsches Institut für Normung, DIN) in collaboration with the German Commission for Electrotechnical, Electronic, and Information Technologies (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik, DKE), established the joint working committee NA 043-01-42 GA. DIN/DKE, like other national standardization bodies, are actively collaborating with said international bodies.[19] Thereby, national standardization bodies help to balance national with overarching international (e.g., European) efforts. Finally, national mirror committees help to ensure the coordinated implementation of European standards across EU member states.[20]

In addition to standardization bodies, industry players and scientific organizations contribute to AI standardization through industry standards, particularly via AI audit catalogues and testing frameworks. Notable contributions include:

- AI HLEG ALTAI:[21] In 2020, the High-Level Expert Group on AI, appointed by the European Commission, published their Assessment List for Trustworthy AI, which helps make the AI HLEG Ethics Guidelines for Trustworthy AI from 2019 actionable. It focuses on 7 key requirements: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, environmental and societal well-being and accountability.

- NIST AI RMF:[22] In 2023, the US National Institute of Standards and Technology developed a framework to manage risks associated with AI (AI Risk Management Framework). In

[14] IEEE SA, 'Artificial Intelligence Standards Committee – Standards', accessed 24 Feb., 2025, https://sagroups.ieee.org/ai-sc/standards.

[15] IEEE SA, 'Artificial Intelligence Standards Committee – Active PARs', accessed 24 Feb., 2025, https://sagroups.ieee.org/ai-sc/active-pars/.

[16] CEN-CENELEC, 'Technical Work – CEN Technical Bodies – CEN/CLC/JTC 21 – Artificial Intelligence – Published Standards', accessed 24 Feb., 2025, https://standards.cencenelec.eu/dyn/www/f?p=205:32:0::::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D

[17] CEN-CENELEC, 'Technical Work – CEN Technical Bodies – CEN/CLC/JTC 21 – Artificial Intelligence – Work Programme', accessed on 24 Feb., 2025, https://standards.cencenelec.eu/dyn/www/f?p=205:22:0::::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D

[18] DIN, 'Untergremien von NA 043-01-42 GA', https://www.din.de/de/mitwirken/normenausschuesse/nia/nationale-gremien/wdc-grem:din21:284801493. For example, in France the Association Française de Normalisation (AFNOR) committee AFNOR/CN IA is responsible for this (https://norminfo.afnor.org/structure/afnorcn-ia/intelligence-artificielle/127690#presentation), in Spain the Asociación Española de Normalización (UNE) implements this through the committee CTN 71/SC 42 - Inteligencia artificial y big data (https://www.une.org/encuentra-tu-norma/comites-tecnicos-de-normalizacion/comite?c=CTN+71/SC+42).

[19] DIN, 'Nationales Spiegelgremium von CEN/CLC/JTC 21', https://www.din.de/de/mitwirken/normenausschuesse/nia/europaeische-gremien/wdc-grem:din21:339816705.

[20] Soler Garrido et al., 'Analysis of the Preliminary AI Standardisation Work Plan in Support of the AI Act', 2023, doi:10.2760/5847.

[21] AI High-Level Expert Group on Artificial Intelligence, 'Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment', 2020, https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

[22] NIST, 'Artificial Intelligence Risk Management Framework (AI RMF 1.0)' – NIST AI 100-1, Jan. 2023, https://doi.org/10.6028/NIST.AI.100-1; 'Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile' – NIST AI 600-1, July 2024, https://doi.org/10.6028/NIST.AI.600-1.

2024, they specified the framework with a profile to help identify unique risks posed by generative AI and propose actions for effective risk management aligning with their addressee's priorities.

- Mission KI Standard:[23] Mission KI is an initiative funded by the German Federal Ministry for Digitalization and Transport, and supervised by acatech with a consortium of AI Quality & Testing Hub, CertifAI, Fraunhofer IAIS, PwC Deutschland, TÜV AI Lab and VDE, which is developing a voluntary quality standard that strengthens the reliability and trustworthiness of AI applications beyond the high-risk threshold of the AI Act.

- Fraunhofer IAIS catalog:[24] The AI Assessment Catalog by the Fraunhofer Institute for Intelligent Analysis and Information Systems (IAIS) offers a structured guideline that can be used to define abstract AI quality standards into application-specific assessment criteria covering six dimensions of trustworthiness.

- BSI AIC4:[25] In 2021, the German Federal Office for Information Security published the AI Cloud Service Compliance Catalogue (AIC4). It specifies minimum requirements for the secure use of machine learning methods in cloud services. The aim is to transparently present the information security of an AI cloud service based on a standardised test. The criteria address security and robustness, performance and functionality, reliability, data quality, data management, explainability and bias.

## 2.2 Harmonized Standards under the AI Act

Under EU law, a standard is a technical specification adopted by a recognised standardization body for repeated or continuous application, with which compliance is not compulsory (Art. 2(1) Regulation (EU) 1025/2012. A harmonized standard means a standard developed by an European standardization organisation (CEN, CENELEC, or ETSI) upon a standardization request from the European Commission (see Art. 2(1)(c) Regulation (EU) 1025/2012). They are aligned with EU harmonized legislative objectives and published in the Official Journal of the European Union (OJEU). Products conforming with these standards are presumed to comply with certain covered requirements of the applicable EU legislation. This creates a clear pathway to CE (conformité européenne) marking, ultimately facilitating EU market access.

For the AI Act, Art. 40(1) lays down the normative foundation for harmonized standards and the presumption of conformity regarding high-risk AI systems.[26] High-risk AI systems are conclusively defined by Art. 6 AI Act in conjunction with Annexes I and III, where Annex I focuses

[23] See Mission KI, 'Mission KI Mindeststandards', https://mission-ki.de/de/pruefstandards. The standard has not been published in its final form yet.

[24] Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS, 'AI Assessment Catalog: Guideline for Trustworthy Artificial Intelligence', 2024, https://www.iais.fraunhofer.de/en/research/artificial-intelligence/ai-assessment-catalog.html.

[25] Federal Office for Information Security, 'AI Cloud Service Compliance Criteria Catalogue (AIC4)', 2021, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/AIC4/AI-Cloud-Service-Compliance-Criteria-Catalogue_AIC4.pdf?__blob=publicationFile&v=4.

[26] Art. 40 AI Act also provides for the establishment of technical standards regarding GPAI systems, but the EU Commission did not issue a corresponding standardization request so far. Rather, the European Commission is working on a Code of Practice for GPAI (European Commission, 'Second Draft of the General-Purpose AI Code of Practice published, written by independent experts', 19 Dec. 2024, https://digital-strategy.ec.europa.eu/en/library/second-draft-general-purpose-ai-code-practice-published-written-independent-experts). For further information on the harmonised standards under the AI Act see Gerdemann, 'Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI', MMR 2024, 614 (614 et seq.); Kilian/Denga, 'Das Testen und Zertifizieren von KI-Systemen', NJW 2024, 2945 (2945 et seq.).

on product-specific (e.g., machinery, medical devices, aviation, automotive, etc.) and Annex III on use case-specific risks (e.g., critical infrastructure, education, access to essential services, etc.).[27] However, AI systems under Annex III are only considered high-risk if they pose a significant risk of harm to the health, safety or fundamental rights of natural persons (Art. 6(3) AI Act). It is assumed that between 10 % and 20 % of AI companies in the EU develop and distribute high-risk AI systems.[28] These high-risk systems generally must adhere to the requirements stemming from Chapter III Section 2 AI Act.[29] The requirements are covering risk management, data and data governance, technical documentation, record-keeping, transparency and provision of information to users, human oversight, and accuracy, robustness and cybersecurity measures (Art. 9-15 AI Act). They will be applicable starting in August 2026 for Annex III AI systems and August 2027 for Annex I AI systems (Art. 113 AI Act).[30]

To make these requirements actionable, the European Commission has issued a standardization request to CEN and CENELEC (Art. 40(2) AI Act) in May 2023,[31] which is expected to be amended soon.[32] Once technical standards become harmonized standards through publication in the OJEU, they act as the base for the presumption of conformity according to Art. 40(1) AI Act. As one of the cornerstones of the AI Act, this means that high-risk AI systems meeting these standards are presumed (unless the opposite is proven) to comply with the respective requirements under the AI Act. This aims at simplifying compliance, providing legal certainty and ideally reducing the administrative burden for AI providers.

Currently, CEN-CENELEC JTC 21 is working on ca. 35 standardization activities in fulfillment of the standardization request.[33] While traditional standardization typically builds on existing international work (especially globally distributed ISO/IEC standards), many aspects of the AI Act require new "home-grown" European standards because international standards are not fully aligned with AI Act objectives, particularly regarding fundamental rights protection and societal impacts.[34] Therefore, existing international standards are adopted where they align with EU values and fundamental rights, while remaining gaps are filled by European standards newly developed by CEN-CENELEC JTC 21. Also, the standardization process should involve multiple stakeholders ensuring diverse perspectives shape these technical standards while maintaining consistency with broader EU regulatory objectives (Art. 40(3) AI Act).

[27] This list can be modified through amending acts by the European Commission (Art. 97 AI Act).

[28] European Commission, 'Commission Staff Working Document: Impact Assessment', SWD(2021) 84 final, p. 68: 5–15 % of European AI providers (https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence); appliedAI, 'AI Act: Risk Classification of AI Systems from a Practical Perspective', Mar. 2023: at least 18 % out of 106 AI systems (https://aai.frb.io/assets/files/AI-Act-Risk-Classification-Study-appliedAI-March-2023.pdf); KI Bundesverband et al., 'AI Act Impact Survey', 12 Dec. 2022: 33 % out of 113 interviewed AI provider companies (https://aai.frb.io/assets/files/AI-Act-Impact-Survey_Report_Dec12.2022.pdf).

[29] For the products under Annex I Section B. AI Act, these requirements do not apply directly (Art. 2(2) AI Act), but will eventually be applicable mutatis mutandis via amendments to the respective product safety regulations (see Art. 102 et seq. AI Act).

[30] For AI systems according to Annex I Section B. AI Act, the application will only start depending on the respective delegated acts.

[31] European Commission, C(2023) 3215 final, 'Commission Implementing Decision of 22.5.2023 on a standardisation request on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence', https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en.

[32] See ETUC, 'Artificial Intelligence Standardisation Inclusiveness Newsletter, Edition 6', Dec. 2024, p. 1.

[33] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, pp. 4 et seq.

[34] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 7.

## 2.3 Vertical AI Standards

While the AI Act is an industry-agnostic horizontal regulation, the European Commission was considering in the standardization request additional vertical specifications regarding certain sectors.[35] Therefore, the active involvement of stakeholders from a range of industries is vital for the well-informed development of the harmonized standards. This refers in particular to industries with existing vertical technical requirements and standards, such as machinery, medical devices, aerospace, automotive, infrastructure or the finance sector.

Art. 102 et seq. AI Act ensures that AI Act high-risk requirements are also applied in the respective market access regulations such as the automotive, aviation, and railway industry for example. The changes in the respective homologation regulations will be implemented via delegated acts and thus largely via technical specifications. Hence, it is to be expected that standardization bodies will be requested to incorporate AI Act requirements, if possible, into existing vertical homologation-relevant standards.

For most sectors, there are no established specific vertical standards regarding AI usage up to date. However, in some sectors, non-AI Act-specific but AI-related standards are already established or drafted at the moment.[36] For example, for AI in healthcare BS 30440:2023 by the British Standards Institute (BSI) provides a specific framework for the validation of AI usage.[37] Furthermore, for the automotive sector the standard ISO/PAS 8800 provides technical specifications for safety-critical AI systems in road vehicles.[38] In its next version, ISO/PAS 8800 could be well suited for incorporating the AI Act high-risk requirements via the Type Approval Act (Regulation (EU) No. 168/2013) pursuant to Art. 104 AI Act.[39] For aviation, the standard SAE ARP6983 still to be developed by the Society of Automobile Engineers (SAE) concerns the development and certification / approval of aeronautical safety-related products implementing AI.[40]

Other sectors, such as defense – while mainly excluded from the AI Act's scope (Art. 2(3) AI Act) – identified the need for sector-specific AI standards and are taking steps for evolving them.[41] Additionally, there are other sectors, which are not directly covered by AI Act standards or sector-specific AI standards, but as their customers may be subject to high-risk AI Act requirements in the future, plan to comply voluntarily with the corresponding standards.

[35] European Commission, 'Annex II to the Commission Implementing Decision C(2023)3215 final', pp. 2 et seq.

[36] DIN, 'Artificial Intelligence: Standardization helps create innovation-friendly framework conditions for the technology of the future', Jan. 2019, https://www.din.de/resource/blob/306690/f0eb72ae529d8a352e0b0923c67b6156/position-paper-artificial-intelligence-english--data.pdf.

[37] BSI, 'BS 30440:2023: Validation framework for the use of artificial intelligence (AI) within healthcare. Specification', https://knowledge.bsigroup.com/products/validation-framework-for-the-use-of-artificial-intelligence-ai-within-healthcare-specification?version=standard.

[38] ISO, 'ISO/PAS 8800:2024: Road Vehicles – Safety and Artificial Intelligence', https://www.iso.org/standard/83303.html.

[39] Kilian, ZRP 2024, 130 (131); Burton/Kilian/Schmidt/Zawadzki, 'Impact of AI Regulation on the Automotive Industry: The Connection between Technical Standards and the European Artificial Intelligence Act' [under publication].

[40] SAE International, 'ARP 6983 (WIP): Process Standard for Development and Certification/Approval of Aeronautical Safety-Related Products Implementing AI', 2023, https://www.sae.org/standards/content/arp6983/œARP6983.

[41] See e.g., Delgado-Aguilera Jurado et al., 'An introduction to the current state of standardization and certification on military AI applications', Nov. 2024, https://www.sciencedirect.com/science/article/pii/S0969699724001509.

## 2.4 Challenges in the AI Act Standardization Process

The EU's ambitious goal of becoming a global leader in the development of secure, trustworthy, and ethical AI[42] shall be realized through technical standards as the center of digital product safety legislation. However, this legislative approach is challenged by tight implementation timelines, complex stakeholder dynamics, unjustifiable costs for implementation and the additional challenge of operationalization.[43]

### 2.4.1 Critical Timeline

As of now, more than 300 experts from over 20 EU member states are working within CEN-CENELEC JTC21 to develop the requested technical standards specifying the AI Act high-risk requirements.[44] Yet, the timeline for developing these standards is highly ambitious and increasingly tight.[45] Initially, the European Commission set an April 2025 deadline for standards development.[46] However, in a soon-to-be-published amendment to the standardization request, the deadline is likely to be extended to August 2025 due to the committee's work progressing slower than anticipated by the European Commission.[47] The consensus-building process on new work items in JTC 21 has proven challenging, testing the limits of decision-making processes in standardization committees and leading to delays.[48] The complexity is further compounded by competing interests between global and sector-specific standardization needs, as well as different requirements across industries, typical for horizontal standards.[49] Also the standardization deliverables under the AI Act build a complex framework with interactions and dependencies between individual (partly converging, partly diverging) goals.[50] The overall standardization approach therefore must carefully account for all of these interrelationships to be effective.

However, even after CEN-CENELEC finalizes the standards, they must go through an additional review process. The European Commission assesses their compliance with the standardization request and publishes them in the OJEU, following Art. 10, 11 of (EU) No. 1025/2012. This process can take several months before the standards become harmonized under the AI Act and can grant AI providers a presumption of conformity.[51] After the final publication of the standards in the OJEU, currently expected for the beginning of 2026,[52] timing leaves high-risk AI system

[42] European Commission, COM(2022) 31 final, 'An EU Strategy on Standardisation Setting global standards', 2022,https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0031.

[43] Micklitz, 'The Role of Standards in Future EU Digital Policy Legislation', 2023.

[44] JTC 21, 'About the Joint Technical Committee — CEN-CENELEC JTC 21', https://jtc21.eu/about/.

[45] Kilian, 'Nationale Spielräume bei der Umsetzung des Europäischen Gesetzes über Künstliche Intelligenz. Written statement for the 63rd meeting of the Committee for Digital Affairs of the German Bundestag on May 15th, 2024' p. 12 et seq.

[46] European Commission, C(2023) 3215 final, 'Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence', 2023, https://ec.europa.eu/growth/tools-databases/enorm/mandate/593_en.

[47] This schedule would roughly match with the median 28,5 months required for technical standards to be finalized after the standardization request (CEN, 'The default timeframe for the development of European Standards', 26 Oct. 2017, https://boss.cen.eu/media/CEN/ref/bt_n_8140.pdf).

[48] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 2.

[49] Castets-Renard/Besse, 'Ex Ante Accountability of the AI Act: Between Certification and Standardization, in Pursuit of Fundamental Rights in the Country of Compliance', 2023, pp. 18-20, https://ssrn.com/abstract=4203925.

[50] For example, data governance can support accuracy by ensuring the quality and representativeness of the data used to train and operate the AI system. Then again, optimizing an AI system for accuracy might perpetuate bias, if not carefully managed.

[51] Kilian, 'Nationale Spielräume bei der Umsetzung des Europäischen AI Acts', ZRP 2024, 130.

[52] MLex, 'Deadline for AI standards to be postponed, EU standards chief says', 1 Aug. 2024, https://mlexmarketinsight.com/news/insight/deadline-for-ai-standards-to-be-postponed-eu-standards-chief-says.

providers with only about 6-8 months until they need to comply by August 2026 (Art. 113 AI Act).[53] Given that providers will need adequate time to implement these standards and demonstrate compliance, the current pace of development raises substantial concerns about whether providers will be able to do so in time by mid-2026. This situation is further complicated by the sheer volume of ca. 35 technical standards that CEN-CENELEC is planning to provide for the AI Act.[54] Especially for startups and SMEs, the implementation of such a large number of technical standards will likely take years. However, if the publication of the standards is further delayed and widespread readiness issues among AI providers become apparent, the EU legislator could, as a last resort, postpone the application of the AI Act high-risk requirements.[55] Needless to say, companies cannot rely on such a hypothetical postponement, and any deadline extension would need to undergo the respective legislative procedure.

Another option for the European Commission to address CEN-CENELEC's delay in standardization deliveries is to adopt common specifications for the high-risk requirements (pursuant to Art. 41 (1) AI Act). This requires, inter alia, that CEN-CENELEC is not delivering the standards within the deadline set by the European Commission (Art. 41 (1)(a)(ii) AI Act). Even if the Commission is extending the deadline by an amendment to the standardization request from April to August 2025, it still seems unlikely that CEN-CENELEC is able to deliver in time. However, for the Commission to take this action, based on the legal text wording the deadline must have been missed already, effectively at least it should be inevitable that it is going to be missed. Furthermore, the adoption of common specifications cannot be considered if a harmonized standard is expected to be published within the period of time it would take to adopt an implementing act.[56]

Table 1: Compliance Milestones for High-Risk AI System Providers

| **Deadline** | **Compliance Milestone (AI Act)** |
|---|---|
| April 30, '25 | Original deadline for deliverables from SR |
| August 31, '25 | Postponed deadline for deliverables from SR (upon amendment) |
| End of '25/Early '26 | Contemplated publication of harmonized standards in OJEU following SR |
| August 2, '26 | Application of high-risk requirements to AI systems according to Annex III |
| August 2, '27 | Application of high-risk requirements to AI systems according to Annex I Sec. A |
| Mid-2027 (Est.) | Application of high-risk requirements to AI systems according to Annex I Sec. B (Art. 102 et seq.) |

### 2.4.2 Complex Stakeholder Dynamics

Standardization efforts, involving over 1,000 experts across national mirror committees,[57] are facing a structural challenge regarding stakeholder representation. These standardization commit-

[53] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 1. This is for high-risk AI systems according to Annex III.

[54] For a more detailed overview of the technical standards in question see Table 2 under section 3.

[55] A recent example for the postponement of EU regulations' date of application was the Medical Devices Regulation (MDR), whose application was postponed from May 2020 to May 2021 (European Commission, 'Commission postpones application of the Medical Devices Regulation to prioritise the fight against coronavirus', 3 Apr. 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_589).

[56] Martini/Wendehorst/Gerdemann/Wöbbeking, 'KI-VO: Verordnung über Künstliche Intelligenz', 2024, Art. 41 (17).

[57] DIN/DKE, 'Europäische KI-Normung – Endspurt zum AI Act', 17. July 2024, p. 9, https://www.din.de/resource/blob/1118040/21c9ee1e795105d3d552d8e636ac303f/gesamtpraesentation-ki-webinar-data.pdf.

tees are predominantly influenced by large enterprises, with major US technology and consulting companies constituting oftentimes the participation majority. This creates a notable disparity in representation, particularly affecting SMEs, startups, civil society organizations, independent institutions, and academia.

Participation in standard-setting can provide firms with strategic advantages through knowledge transfer and relationship building beyond lobbying for their interests to facilitate technical compliance.[58] Evidence suggests that well-designed regulatory frameworks can ensure fair participation opportunities while maintaining technical quality. Even smaller stakeholders can successfully contribute to standards development when appropriate institutional structures exist.[59]

The under-representation of smaller stakeholders in EU AI standardization stems primarily from the substantial resources required for effective participation in these committees. The resource allocation challenge is particularly acute for smaller organizations, which must prioritize their limited human and financial capital for core operational activities. Consequently, industry associations have emerged as crucial intermediaries, bearing the responsibility of aggregating and representing these stakeholders' interests within standardization bodies.

This structural imbalance generates competitive advantages for larger enterprises operating in the EU market, as they possess the resources to influence technical standards development according to their interests, resulting in both knowledge and implementation advantages. The substantial influence of US companies raises concerns regarding the adequate representation of EU values and perspectives. The standards necessitate a value-oriented balancing of fundamental rights—decisions that may ultimately be subject to a European Court of Justice review, whereby indirectly shaping EU fundamental rights application.[60] Limited participation of smaller entities in standardization processes potentially excludes crucial knowledge from the standards that will define market access, thereby potentially compromising comprehensive safety development in the field. This situation underscores the need for more inclusive standardization processes that can effectively incorporate diverse perspectives and expertise.

### 2.4.3 Unjustifiable Costs and the Malamud Case

Another challenge is the cost point for identifying applicable technical standards and certification needs and the costs associated with accessing the respective standards. When technical standards become harmonized standards under EU law, the question arises as to whether these standards should be freely accessible, as seen in cases like "Stichting Rookpreventie" before the Court of Justice of the European Union (CJEU).[61] This issue came to a head in March 2024 when the European Court of Justice (ECJ) in the "Malamud" case ruled that harmonised standards to which conformity presumptions in EU product safety law refer to are part of EU law and must therefore be freely accessible and free of charge.[62] Specifically, the court argued that such harmonized norms are part of EU law based on their legal effects.[63] These legal effects are a result

[58] Waguespack/Fleming, 'Scanning the Commons? Evidence on the Benefits to Startups Participating in Open Standards Development', 2009, 210 (214).

[59] Gupta, 'The Role of SMEs and Startups in Standards Development', 12. July, 2017, p. 8. See also Dinçkol et al., 'Regulatory Standards and Consequences for Industry Architecture: The case of UK Open Banking', 27 Mar. 2023, https://doi.org/10.1016/j.respol.2023.104760 for how regulatory adjustment can address emerging implementation challenges regarding technical standards.

[60] Gerdemann, 'Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI', MMR 2024, 614 (619 et seq.) with further references.

[61] CJEU judgement, 22 Feb. 2022, C-160/20 – Stichting Rookpreventie.

[62] ECJ judgement, 5 Mar. 2024, C-588/21 P – Malamoud.

[63] ECJ judgement, 5 Mar. 2024, C-588/21 P – Malamoud, para. 70.

of their connection to the presumption of conformity and the fact that it might prove difficult to fall back on other mechanisms as evidence for legal conformity (e.g., expert opinions) due to administrative challenges and additional costs.[64] Therefore, harmonized standards are covered by the right of access to official documents stemming from Art. 15(3) TFEU, implemented by Regulation (EC) No 1049/2001.[65] The copyright of the standardisation organisations should not prevent this either, as there is in any case an overriding public interest in dissemination (see Art. 4(2) Regulation (EC) No 1049/2001). However, the situation has further escalated with ISO and IEC issuing a lawsuit against the European Commission before the CJEU on December 6, 2024,[66] aiming to ensure the integrity of their copyright to technical standards that are part of harmonized standards in the EU and further monetize them. Depending on the outcome of the court proceedings, European standardization efforts are at risk of losing the contribution of international standardization organizations.[67]

The current CEN-CENELEC JTC 21 work program encompasses ca. 35 standards, which could easily amount to expenses of thousands of € for each AI provider to find out which specifications they need to follow for AI Act compliance.[68] If a company cannot afford to purchase all relevant technical standards, they are at risk of a negative conformity presumption, i.e. not complying with the technical standards for the AI Act can lead to a supervisory authority bias regarding the other available compliance approaches (e.g., legal expert opinions).[69] Failing to meet the compliance deadlines poses significant risks for companies providing high-risk AI sectors. Non-compliance can result in fines of up to €35 million or 7 % of global turnover (Art. 99 AI Act), severely impacting financial stability in particular for smaller companies. Additionally, companies (more likely startups and SMEs) may face restricted access to the EU market, leading to a competitive disadvantage as compliant firms (more likely larger corporations) will capture more market share.[70] Reputational harm is another critical concern for non-compliant companies, as negative media coverage and loss of customer trust can jeopardize long-term business relationships, especially in sensitive and risk-averse industries.

### 2.4.4 Operationalisation and Threshold-Based Standards

One of the most prevalent challenges in standardization, in particular for AI standardization (and the assessment of compliance with these standards), is the need for further operationalization of the technical standards. At the moment, technical standards are mainly digitally represented as PDFs, which means they must be read, interpreted, and executed manually to be applied to the specific use case in question. To streamline compliance adherence and utilization of standards' contents in downstream processes, the German standardization bodies DIN and DKE initiated

[64] ECJ judgement, 5 Mar. 2024, C-588/21 P – Malamoud, paras. 72–77.

[65] ECJ judgement, 5 Mar. 2024, C-588/21 P – Malamoud, para. 84.

[66] CJEU, International Electrotechnical Commission and ISO v Commission.

[67] Klindt, 'Wie der EuGH am System der europäischen Produktsicherheit sägt', 19 Mar. 2024, https://rsw.beck.de/aktuell/daily/meldung/detail/eugh-malamud-produktsicherheit-europa-normen-klindt.

[68] This is based on the average price range of technical standards from 100 to 300 euros.

[69] Gerdemann, 'Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI', MMR 2024, 614 (618); Mayrhofer, 'Produktsicherheit und Produkthaftung – zwei Seiten einer Medaille mit unterschiedlichen Gravuren', RDi 2024, 492 (494 et seq.).

[70] This aspect seems to be overlooked by the legislator who is just referring to a potential boost for the internal market and a competitive edge for the European industry at large, European Commission, COM(2021) 206 final, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonsed rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts', 'Legislative Financial Statement', Sec. 1.5.2., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX.

the SMART Standards project.[71] This project pursues the vision of so-called Smart Standards, which are machine-readable,[72] -interpretable, -executable, and -controllable.[73] Such standards are intended to facilitate scalable testing of whether an AI system satisfies defined technical requirements related to automatically measurable / testable properties of AI models and data.[74] This would also imply a potential for cost reduction associated with the activities for standard applications.[75] In addition, in terms of operationalization, threshold-based or goal-oriented standards focus on desired outcomes or performance levels, allowing stakeholders the freedom to choose the most efficient or innovative ways to meet these requirements. Hence, regarding some requirements for high-risk AI systems this approach is preferable compared to rule-based standards which prescribe highly specific methods or technologies, oftentimes stifling innovation and limiting flexibility.[76] However, the prerequisite for this is a deep technical expertise within AI standardization committees, along with a standardization and policy expertise. Therefore, the number of technical experts actually contributing to the drafting of the standards must be increased.

# 3 Status Quo of the Standardization Process

The European Commission's standardization request for the AI Act outlines ten essential deliverables addressing key regulatory requirements. These deliverables form the foundation for current standardization work at CEN-CENELEC JTC 21, with most ongoing work items directly contributing to fulfilling this mandate. Where possible, the work items in JTC 21 are based on international standards or co-developed with ISO/IEC (approx. 2/3 of work items).

The current AI Act's standardization work builds on ca. 35 standards, most of them addressing individual standardization request deliverables.[77] Other deliverables as the Artificial Intelligence Trustworthiness Framework and the supporting standards regarding terminology touch upon multiple SR deliverables. The standards will form an integrated framework through multiple interrelationships, such as hierarchical integration or operational dependencies.[78]

The following content analysis of the current state of standards activities by CEN-CENELEC JTC 21 in fulfilment of the European Commission's standardisation request for the AI Act is based on two primary sources: 1) the CEN-CENELEC JTC 21 dashboard presenting the status

[71] DIN/DKE, 'German Standardization Roadmap on Artificial Intelligence', 2nd ed., Dec. 2022, pp. 268 et seq., https://www.din.de/resource/blob/916798/ed09ae58b60f0d3a498fa90fa5085b7c/nrm-ki-engl-2023-final-web-250-neu-data.pdf. This is not to be confused with the CEN-CENELEC SMART Project, launched in January 2025, which is providing a tool to streamline the drafting process of standards and their implementation (CEN-CENELEC, 'Transforming European Standards with the SMART Project', 16 Jan. 2025, https://www.cencenelec.eu/news-and-events/news/2025/brief-news/2025-01-16-smart-phase-1-launch/). For more on this, see section 5.3.2.

[72] See for the legal notion of 'machine-readability' Hamburg District Court, 310 O.22723, LAION v Robert Kneschke, [27 September 24] on Art. 4(3) Directive (EU) 2019/790 and the standardization efforts mentioned in the Second Draft General-Purpose AI Code of Practice, pp. 23–24 regarding Art. 53(1)(c) AI Act.

[73] DIN/DKE, 'Workshop Skalierbare KI-Prüfung mit SMART Standards', 29 Nov. 2024, p. 29, https://www.dke.de/resource/blob/2360894/773f3d1b20cc524a565e5d4be6d383a8/ki-pruefung-workshop-data.pdf.

[74] DIN/DKE, 'Workshop Skalierbare KI-Prüfung mit SMART Standards', 29 Nov. 2024, pp. 3, 55 et seq.

[75] DIN/DKE, 'Workshop Skalierbare KI-Prüfung mit SMART Standards', 29 Nov. 2024, p. 24.

[76] Regarding the differentiation and benefits in general, see Department for Business, Energy & Industrial Strategy, 'Goals-Based and Rules-Based Approaches to Regulation', May 2018, https://assets.publishing.service.gov.uk/media/5b17b32eed915d2cb16267d9/regulation-goals-rules-based-approaches.pdf. See regarding the need for reference thresholds Kilian, 'Nationale Spielräume bei der Umsetzung des Europäischen Gesetzes über Künstliche Intelligenz' – Written statement for the 63rd meeting of the Committee for Digital Affairs of the German Bundestag on May 15th, 2024, p. 14.

[77] Hallensleben, 'Status Dashboard JTC21 European AI Standardization', Aug. 2024.

[78] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 3.

of work items in European AI standardization as of August 2024,[79] and 2) the CEN-CENELEC website's current listing of their work program, which is less detailed than the dashboard, yet more up to date on deadlines.[80] It becomes apparent that for a good part of work items the forecasted voting date is only expected for mid-2026, which is exceeding the current deadline from the standardization request (April 2025) by more than a year.

In any case, CEN-CENELEC JTC 21 standardization work is still in progress and this paper can only analyze the current status quo, which might be subject to change in the future. Especially, research publications by the European Commission's Joint Research Center in the past partially identified further technical standards with high operationalisation levels for the AI Act not mentioned by CEN-CENELEC up until now (e.g. ISO/IEC 4213, 5338, 5469, 24027, 38507).[81] However, it should be noted that the European Commission in their–not yet published–assessment from February has already expressed criticism regarding the standardization work of CEN-CENELEC, particularly concerning the scope and the number of referenced standards.

Table 2: Harmonized Standards and Framework References

| SR | AI Act | Harmonized Standards and Framework References |
|---|---|---|
| 1 | **Art. 9** | *Risk Management for AI Systems:*<br>• ISO/IEC 23894 – IT – AI – Guidance on Risk Management<br>• **AI Risk Management (WI: JT021024)**[82] |
| 2 | **Art. 10** | *Governance and Data Quality of Datasets Used to Build AI Systems:*<br>• ISO/IEC/TS 12791 – IT – AI – Treatment of Unwanted Bias in Classification and Regression Machine Learning Tasks<br>• **AI – Concepts, Measures and Requirements for Managing Bias in AI Systems (WI: JT021036)**<br>• ISO/IEC 8183 – IT – AI – Data Life Cycle Framework<br>• ISO/IEC 5259-1 – 5259-4 – Data Quality for Analytics and Machine Learning (ML)<br>• **AI – Quality and Governance of Datasets in AI (WI: JT021037)**<br>• **CEN/CLC/TR 18115 – Data Governance and Quality for AI in the European Context** |
| 3 | **Art. 12** | *Record Keeping Through Built-In Logging Capabilities in AI Systems:*<br>• ISO/IEC 24970 – AI System Logging<br>• **Artificial Intelligence Trustworthiness Framework (WI: JT021008)** |
| 4 | **Art. 13** | *Transparency and Information to the Users of AI Systems:*<br>• ISO/IEC 12792 – Transparency Taxonomy of AI Systems<br>• **Artificial Intelligence Trustworthiness Framework (WI: JT021008)** |
| 5 | **Art. 14** | *Human Oversight Over AI Systems:*<br>• **Artificial Intelligence Trustworthiness Framework (WI: JT021008)** |

*Continued on next page...*

[79] Hallensleben, 'Status Dashboard JTC 21 European AI Standardization', Aug. 2024, https://www.linkedin.com/posts/sebastianhallensleben_status-dashboard-jtc21-european-ai-standardisation-activity-7235665875112988673-xfEH?.

[80] CEN/CENELEC, 'CEN/CLC/JTC 21 Work programme', https://standards.cencenelec.eu/dyn/www/f?p=205:22:0::::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D.

[81] Nativi/De Nigris et al., 'AI Watch: AI Standardisation Landscape – State of Play and Link to the EC Proposal for an AI Regulatory Framework', 2021, pp. 43–45, doi.org/10.2760/376602.

| SR | AI Act | Harmonized Standards and Framework References |
|---|---|---|
| 6 | **Art. 15** | *Accuracy Specifications for AI Systems:*<br>• ISO/IEC 23282 – Evaluation Methods for Accurate Natural Language Processing Systems<br>• ISO/IEC 23281 – AI – Overview of AI Tasks and Functionalities Related to Natural Language Processing<br>• **Evaluation Methods for Accurate Computer Vision Systems (WI: JT021025)**<br>• **Taxonomy of AI Tasks in Computer Vision (WI: JT021044)**<br>• ISO/IEC/TS 12791 – IT – AI – Treatment of Unwanted Bias in Classification and Regression Machine Learning Tasks<br>• **AI – Concepts, Measures and Requirements for Managing Bias in AI Systems (WI: JT021036)**<br>• **Artificial Intelligence Trustworthiness Framework (WI: JT021008)** |
| 7 | **Art. 15** | *Robustness Specifications for AI Systems:*<br>• ISO/IEC 24029-2, -3, -5 – AI – Assessment of the Robustness of Neural Networks<br>• ISO/IEC/TR 24029-1 – AI – Assessment of the Robustness of Neural Networks<br>• **AI – Concepts, Measures and Requirements for Managing Bias in AI Systems (WI: JT021036)**<br>• **Artificial Intelligence Trustworthiness Framework (WI: JT021008)** |
| 8 | **Art. 15** | *Cybersecurity Specifications for AI Systems:*<br>• ISO/IEC 27090 – Guidance for Addressing Security Threats and Failures in AI Systems<br>• **AI – Cybersecurity Specifications for AI Systems (WI: JT021029)**<br>• Conformity Assessment in Relation to the Technical Solutions to Address AI-Specific Vulnerabilities (n/a)<br>• **Artificial Intelligence Trustworthiness Framework (WI: JT021008)** |
| 9 | **Art. 17** | *Quality Management for Providers of AI Systems, Including Post Market Monitoring Process:*<br>• ISO/IEC 42001 – IT – AI – Management System<br>• **AI – Quality Management System for Regulatory Purposes (WI: JT021039)** |
| 10 | **Art. 43** | *Conformity Assessment for AI Systems:*<br>• ISO/IEC 42006 – Requirements on Bodies Performing Audit and Certification of AI Management Systems<br>• ISO/IEC 29119-11 – Testing of AI Systems<br>• **Competence Requirements on AI Systems Auditors and Professionals (WI: JT021019)**<br>• **AI Conformity Assessment Framework (WI: JT021038)**<br>• Conformity Assessment in Relation to the Technical Solutions to Address AI-Specific Vulnerabilities (n/a) |
| All | **All** | *Supporting Standards (Concepts, Terminology, etc.):*<br>• ISO/IEC 22989:2023 – IT – AI – Artificial Intelligence (AI) Concepts and Terminology<br>• ISO/IEC 22989/prAI – IT – AI – Artificial Intelligence (AI) Concepts and Terminology (Amendment 1)<br>• ISO/IEC 23053:2023 – Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)<br>• ISO/IEC 23053:2023 – Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (Amendment 1)<br>• Terminology and Concepts for Domain Engineering of AI Systems (n/a) |

## 3.1 Risk Management

The first standardization deliverable aims to cover all elements of Art. 9 AI Act (Risk Management System) and give specifications for a risk management system regarding AI systems. Following the AI Act, it shall emphasize individual rights protection through a product-centric approach.

[82] Standards written in bold letters are "home-grown" standards by CEN-CENELEC.

Most notably, it covers the obligation for testing AI systems (Art. 9(6), (8) AI Act).

Within CEN-CENELEC JTC 21, there are two work items relating to this deliverable: 1) ISO/IEC 23894 – IT – AI – Guidance on Risk Management (published), and 2) AI Risk Management (WI: JT021024) (under drafting; forcasted voting: September 30, 2026). While ISO/IEC 23894 provides general guidance on how to manage risks related to AI,[83] its risk definition is not aligned with the AI Act and it is built on a traditional organization-centric risk management approach.[84] Thus, the upcoming "home-grown" AI Risk Management standard will address these shortcomings. Especially, it will include a risk definition in line with Art. 3 AI Act and a product-centric risk management perspective to address specific impacts on health, safety and fundamental rights of individuals.[85] The specifications shall also be integrable with existing risk management systems according to Annex I, Sec. A AI Act.[86] Currently, it is under drafting with a forecasted voting date of September 30, 2026.

## 3.2 Governance and Quality of Datasets

The second deliverable on Governance and Quality of Datasets Used to Build AI Systems shall cover the requirements of Art. 10 AI Act (Data and Data Governance), which focus on statistical validation and bias prevention (esp., Art. 10(2)(f), (g) AI Act).

CEN-CENELEC JTC 21 is following six work items to address this deliverable. This includes three work items in collaboration with ISO/IEC, i.e., 1) ISO/IEC/TS 12791 – IT – AI – Treatment of Unwanted Bias in Classification and Regression Machine Learning Tasks (published), 2) ISO/IEC 8183 – IT – AI – Data Life Cycle Framework (published), and 3) ISO/IEC 5259-1 – 5259-4 – Data Quality for Analytics and Machine Learning (ML) (under enquiry; forecasted voting: June 24, 2026 (parts 1-3) respectively December 17, 2025 (part 4). The other three work items are "home-grown" standards, i.e., 1) AI – Concepts, Measures and Requirements for Managing Bias in AI Systems (WI: JT021036) (under drafting; forecasted voting: June 3, 2026), 2) AI – Quality and Governance of Datasets in AI (WI: JT021037) (under drafting; June 18, 2026), and 3) CEN/CLC/TR 18115 – Data Governance and Quality for AI in the European Context. The standards still under drafting / approval will center on quantifiable measures of data quality and statistical properties throughout the AI system lifecycle.[87] Particularly significant is the Art. 10 AI Act requirement for empirical validation of bias mitigation techniques and the ability to demonstrate the effectiveness of quality assurance measures.[88] This emphasis on measurable outcomes represents a methodological shift from descriptive to prescriptive standardization, requiring organizations to implement verifiable controls for data representativeness, correctness and completeness.[89]

[83] ISO, 'ISO/IEC 23894:2023: Information technology — Artificial intelligence — Guidance on risk management', https://www.iso.org/standard/77304.html.

[84] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 4.

[85] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 4.

[86] European Commission, C(2023)3215, p. 4 ("Annex II, Section A" is "Annex I, Section A" in the final version of the AI Act).

[87] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 4.

[88] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 4.

[89] Soler Garrido et al., 'Analysis of the preliminary AI standardisation work plan in support of the AI Act', 2023, p. 8 et seq.

## 3.3 Record Keeping

The deliverable addressing Record Keeping Through Logging Capabilities shall specify the requirements according to Art. 12 AI Act (Record-Keeping), which mandates traceability of AI system operations, capturing events that could lead to risks or affect system performance.

For this, CEN-CENELEC JTC 21 has two work items running: 1) ISO/IEC 24970 – AI System Logging in co-development with ISO/IEC (under drafting; forecasted voting: September 29, 2026), and 2) the Artificial Intelligence Trustworthiness Framework (WI: JT021008) (under drafting; forecasted voting: December 31, 2025). While the Artificial Intelligence Trustworthiness Framework builds an overarching frame, the ISO/IEC standard will provide more detailed specifications, focusing on balancing comprehensive event capture with operational efficiency. It must define requirements for logging plans that account for varying system architectures and performance demands, from high-frequency trading systems requiring millisecond-level transaction logging to less time-sensitive applications.[90] Notably, while the standard aims to establish minimum logging requirements, it must remain flexible enough to accommodate sector-specific needs to ensure consistent verification capabilities across different AI applications.

## 3.4 Transparency and Information to Users

The fourth deliverable on Transparency and Information to the Users shall cover the requirements under Art. 13 AI Act (Transparency and Provision of Information to Deployers).

This is executed through two CEN-CENELEC JTC 21 work items: 1) ISO/IEC 12792 – Transparency Taxonomy of AI Systems, which is being co-developed with ISO/IEC (under approval; forecasted vote: 14 January, 2025), and 2) and the Artificial Intelligence Trustworthiness Framework (WI: JT021008) (under drafting; forecasted voting date 31 December, 2026). For the ISO/IEC standard, there is specific attention given to European regulatory requirements. It must establish requirements for transparency artifacts that ensure information is comprehensive, meaningful, accessible and understandable for intended audiences, thereby addressing the "black box" problem – where AI systems' internal decision-making processes are opaque, despite visible inputs and outputs.

## 3.5 Human Oversight

The deliverable regarding Human Oversight for AI Systems aims to specify the requirements from Art. 14 AI Act (Human Oversight).

This is mapped by CEN-CENELEC JTC 21 to the Artificial Intelligence Trustworthiness Framework (WI: JT021008) alone, which must establish comprehensive requirements for ensuring effective human control over AI systems.[91] The standard must address the complexities of human oversight across diverse operational contexts. In manufacturing environments, requirements must enable human intervention capabilities while maintaining production efficiency. Similarly, in financial services, standards must establish oversight mechanisms for algorithmic systems operating at speeds beyond human reaction times. This includes requirements for technical measures, like monitoring interfaces and control mechanisms, organizational measures such as training protocols, and verification procedures to demonstrate the effectiveness of oversight implementations.[92]

[90] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, pp. 4 et seq.
[91] Hallensleben, 'Status Dashboard JTC21 European AI Standardization', Aug. 2024.
[92] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 5.

It must also establish clear criteria for selecting appropriate oversight measures based on the AI system's intended use and identified risks, along with specific parameters for testing their effectiveness in preventing and minimizing risks while enabling meaningful human control.[93] Of particular importance is the requirement to define verifiable outcomes regarding system oversight, ensuring that natural persons can effectively maintain operational control and intervene when necessary, despite the increasing complexity and speed of AI systems.[94]

## 3.6 Accuracy Specifications

The Accuracy Specification for AI Systems deliverable addressed the requirements under Art. 15(1), (3) AI Act (Accuracy).[95]

In their work programme, CEN-CENELEC JTC 21 is dedicating seven work items to this deliverable, namely three on international standards: 1) ISO/IEC 23282 – Evaluation Methods for Accurate Natural Language Processing Systems (under drafting; forecasted voting: January 2, 2026), 2) ISO/IEC 23281 – AI – Overview of AI Tasks and Functionalities Related to Natural Language Processing (under drafting; forecasted voting: n/a), and 3) ISO/IEC/TS 12791 – IT – AI – Treatment of Unwanted Bias in Classification and Regression Machine Learning Tasks (published), and four on "home-grown" standards: 1) Evaluation Methods for Accurate Computer Vision Systems (WI: JT021025) (preliminary; forecasted voting: n/a), 2) Taxonomy of AI Tasks in Computer Vision (WI: JT021044) (under drafting; forecasted voting: September 2, 2026), 3) AI – Concepts, Measures and Requirements for Managing Bias in AI Systems (WI: JT021036) (under drafting; forecasted voting: June 3, 2026, and 4) Artificial Intelligence Trustworthiness Framework (WI: JT021008).

The standards establish requirements that go beyond basic performance metrics. Art. 15 (1), (3) AI Act mandates that accuracy measurements must be demonstrably appropriate and effective in addressing regulatory objectives. This includes defining clear criteria for selecting accuracy metrics and thresholds, establishing testing protocols, and documenting evidence at appropriate levels of granularity. For general benchmarking approaches, the standards specify processes and assessment frameworks for evaluating AI models against standardized tasks. The standards focus on establishing clear requirements for how providers should select, measure and validate appropriate accuracy metrics based on their system's intended use and identified risks.[96]

## 3.7 Robustness Specifications

The deliverable on Robustness Specifications for AI Systems shall cover the requirements according to Art. 15(1), (4) AI Act (Robustness).

CEN-CENELEC JTC 21 assigned four work items to this, with two each based on international standards and on "home-grown" standards: 1) ISO/IEC 24029-2, -3, -5 – AI – Assessment of the Robustness of Neural Networks (partially preliminary w/o forecasted voting date), 2) ISO/IEC/TR 24029-1 – AI – Assessment of the Robustness of Neural Networks (published),

[93] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 5.
[94] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 5.
[95] The 'accuracy' requirement should be called 'performance' more accurately with accuracy being only one performance metric among many, see Hacker, 'The European AI liability directives–Critique of a half-hearted approach and lessons for the future', Computer Law & Security Review 51 (2023): p. 34, fn. 281; 'A legal framework for AI training data—from first principles to the Artificial Intelligence Act', Law, innovation and technology 13.2 (2021): 257 (281).
[96] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 5.

3) AI – Concepts, Measures and Requirements for Managing Bias in AI Systems (WI: JT021036) (under drafting; forecasted voting: June 3, 2024), and 4) Artificial Intelligence Trustworthiness Framework (WI: JT021008). To fully align with regulatory demands, additional guidance to complement the ISO/IEC 24029 series (and corresponding technical reports) is needed to set practical metrics, thresholds, and methods tailored to specific use cases. Therefore, the additional standards are extending robustness considerations beyond testing and measurement to include design principles, particularly for systems that evolve post-deployment.[97]

## 3.8 Cybersecurity Specifications

The requirements from Art. 15 (1), (5) AI Act (Cybersecurity) are specified by the deliverable on Cybersecurity Specifications for AI System to define both technical and organizational approaches to security.

There are four JTC 21 work items mapping to this deliverable, with (at least) two "home-grown" standards: 1) ISO/IEC 27090 – Guidance for Addressing Security Threats and Failures in AI Systems (preliminary w/o forecasted voting date), 2) AI – Cybersecurity Specifications for AI Systems (WI: JT021029) (under drafting; July 15, 2026), 3) Artificial Intelligence Trustworthiness Framework (WI: JT021008), and 4) Conformity Assessment in Relation to the Technical Solutions to Address AI-Specific Vulnerabilities (WI: n/a).

The majority of controls from the standards of the ISO/IEC 27000 family will be applicable. However, AI-specific vulnerabilities like data poisoning, model poisoning, model evasion and confidentiality attacks pose new challenges requiring dedicated coverage in the standards. Ongoing standardization work is beginning to capture aspects related to AI-specific threats, mostly in the form of guidance. However, as new threats and countermeasures constantly emerge, a main objective of new standardization on AI cybersecurity will be to define essential requirements for implementing a security risk assessment and mitigation plan for high-risk AI systems. Standards shall define specific security objectives to achieve and verify through testing. These objectives are expected to be defined primarily at the system level, especially when mitigation measures for component-level vulnerabilities cannot be expected to be perfectly effective.[98]

## 3.9 Quality Management System

The deliverable on Quality Management for Providers of AI Systems, Including Post Market Monitoring Process refers to the Art. 17 AI Act (Quality Management System) requirements.

It will be met by two JTC 21 work items: 1) ISO/IEC 42001 – IT – AI – Management System (preliminary w/o forecasted voting date), and 2) the "home-grown" AI – Quality Management System for Regulatory Purposes (WI: JT021039) (under drafting; forecasted voting: July 29, 2026). This latter item specifically complements ISO/IEC 42001 by focusing on regulatory compliance and builds on multiple ISO/IEC standards.[99] However, additional considerations are required to cover the specificities of AI products, whether embedded in physical products or provided as software services. The new standardization on quality management systems shall focus on the specific risks addressed by the AI Act from a product-centric view.[100]

[97] Soler Garrido et al., 'Analysis of the Preliminary AI Standardisation Work Plan in Support of the AI Act', 2023, p. 14, https://doi.org/10.2760/5847.

[98] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 6.

[99] Hallensleben, 'Status Dashboard JTC21 European AI Standardization', Aug. 2024.

[100] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 6.

### 3.10 Conformity Assessment

The last deliverable on the Conformity Assessment for AI Providers is mostly related to Art. 43 AI Act (Conformity Assessment).

The following JTC 21 work items are covering this deliverable: 1) ISO/IEC 42006 – Requirements on Bodies Performing Audit and Certification of AI Management Systems (published), 2) ISO/IEC 29119-11 – Testing of AI Systems (published), 3) Competence Requirements on AI Systems Auditors and Professionals (WI: JT021019) (under drafting; forecasted voting: April 1, 2025, 4) AI Conformity Assessment Framework (WI: JT021038) (under drafting; forecasted voting: July 29, 2026), and 5) Conformity Assessment in Relation to the Technical Solutions to Address AI-Specific Vulnerabilities (n/a).

These standards will leverage existing work, such as the ISO CASCO toolbox, which provides a basis for generic principles and guidance on conformity assessment.[101] However, they will also need to define how these conformity assessment frameworks should be adapted and applied specifically to the unique characteristics of high-risk AI systems as defined in the AI Act.[102] Alignment between the standards covering the various technical requirements for high-risk AI systems and the standards for conformity assessment will be essential. Close coordination between the parallel standardization work items is crucial to ensure the resulting standards are complementary and fit for purpose in supporting the implementation of the regulatory framework.[103]

## 4 Cross-Sector and Industry-Specific Implications

The analysis of EU organizations' practical AI standards implementation challenges and opportunities is based on in-depth interviews with 23 organizations across the EU, including companies such as Mistral, Helsing, Merantix, Langdock or Xayn. The sample comprises startups, SMEs, and corporates, with a headcount ranging from 5 to up to 4000 employees, including AI technologies singular or implemented into safety-relevant released or contemplated products. The companies represent a wide array of industries, spanning automotive, transportation, machinery, defense, cybersecurity, healthcare, agriculture, finance, image analysis, legal services, consulting, the public sector, insurance, publishing, manufacturing, medical technology, education, and enterprise AI. Defense companies were included to understand whether technical standards also exert indirect application (e.g., ecosystem impacts, dual-use considerations).

### 4.1 Cross-Sector Findings

The interviews conducted with organizations developing and deploying systems relevant to the AI Act reveal that the challenges associated with technical standardization and compliance exhibit cross-sectoral characteristics. A notable disparity emerges in the levels of preparedness among high-risk providers. Growth-stage startups operating across multiple high-risk industries have proactively begun aligning with anticipated standards since mid-2023. In contrast, early-stage startups report significant difficulties in planning and implementing regulatory requirements, primarily due to the absence of clear timelines and detailed guidance. This aligns with the observed

[101] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 6.
[102] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 6.
[103] Soler Garrido et al., 'Harmonised Standards for the European AI Act', 2024, p. 6.

trend that smaller companies, constrained by limited resources, deprioritize compliance in early stages, often resulting in delayed or insufficient adherence to regulatory demands.

Organizations with prior exposure to regulatory frameworks highlight that implementation timeframes for similar digital regulations frequently exceed 12 months. This extended timeline is attributed to three predominant challenges: (1) uncertainty regarding the content and applicability of unpublished standards, (2) constraints on both financial and human resources, and (3) the necessity to balance compliance efforts with other critical business priorities, particularly in resource-constrained startups and SMEs.

Although the AI Act does not offer explicit exemptions for SMEs concerning technical standards, the findings underscore that achieving compliance within the prescribed timeline is disproportionately burdensome for smaller entities. Even in traditionally regulated sectors such as medical technology and healthcare, where businesses possess established compliance expertise, startups and smaller SMEs face considerable obstacles due to limited operational capacity. These challenges are even more acute for startups and SMEs in less regulated industries, which often lack both the experience and resources required to navigate the complexities of harmonized standards effectively and within the designated timeframe.

### 4.1.1 Ambiguity and Complexity in Compliance

A prominent cross-sector finding is that organizations face the significant interpretative challenges in complying with technical standards for high-risk AI systems. These challenges arise from the complexity of defining compliance boundaries, particularly when systems integrate multiple components or rely on third-party models. For example, a healthcare provider indicated that while their imaging tools clearly fall under existing medical device regulations, the addition of language processing components introduces new layers of regulatory ambiguity.

The divergence in secrecy requirements across EU member states exacerbates these issues, creating operational conflicts for sectors such as legal technology. A legal tech startup highlighted the difficulty of reconciling professional secrecy laws with regulatory logging requirements, which vary significantly between jurisdictions. This regulatory fragmentation further complicates efforts to establish consistent compliance practices across borders.

Another critical concern is classification ambiguity, particularly for companies operating across multiple sectors. For instance, engineering simulation providers face uncertainty when their tools evolve from design support to operational control systems, raising questions about their risk classification under the AI Act. This reflects a broader challenge in interpreting the scope of dual-use technologies, which may serve both regulated and non-regulated purposes. General-purpose AI (GPAI) model providers are facing a certain ambiguity. While not per se classified as high-risk AI systems under the AI Act, GPAI models are also deployed in high-risk settings. In this case, the deployer turned provider (see Art. 25(1)(c) AI Act) must comply with high-risk AI standards, but might pass on the obligations to the GPAI provider.

The integration of AI systems into existing regulatory frameworks adds yet another dimension of complexity. Even experienced healthcare providers, familiar with FDA clearances and CE certification, report difficulties in aligning the AI Act's requirements with existing medical device regulations. This complexity is particularly evident in cases where systems combine multiple AI modalities, such as image processing and language models.

The evolving technical standards for the AI Act compound these challenges. Unlike established

frameworks such as ISO 27001 for cybersecurity, the AI Act's requirements so far lack clear verification protocols – defined processes for confirming, through objective evidence, that specified requirements have been fulfilled.[104]

Companies report substantial uncertainty regarding the specific evidence required to demonstrate compliance, particularly concerning bias testing and model robustness. One manufacturing firm noted that while they could clearly document their development process, they remained uncertain about the acceptable methods for validating their AI systems' performance.

These ambiguities particularly affect organizations working with complex, multi-component AI systems. This includes challenges when their systems incorporate both image processing and natural language processing components, as each component may be subject to different interpretations of the standards. This complexity is further amplified in cross-border operations, where varying national interpretations of the AI Act create additional compliance challenges.

### 4.1.2 Resources Needed for Compliance

Evidence from providers of high-risk AI systems reveals substantial costs specifically related to the AI Act requirements. Although the standards themselves will likely be free of charge, companies worry about indirect costs.[105] AI providers report anticipated annual compliance costs of ca. €100,000 for dedicated compliance personnel and 10-20 % of the founder's/management's time spent on standard matters. This represents a significant burden for a startup with less than 20 employees. Similarly, other companies report substantial compliance efforts, with one medical tech company estimating certification costs exceeding €200,000, while others in legal tech report annual costs between €200,000-300,000. While these costs might seem reasonable for high-risk AI system providers, it could be excessive for non-high-risk providers voluntarily following certification and compliance programs for high-risk AI that will likely become the norm as companies seek to ensure themselves and their customers are on the safe side. This trend toward voluntary compliance reflects companies' desire to minimize regulatory uncertainty and liability risks, even when certification is not strictly mandatory.[106]

Additionally, resource allocation patterns show particular strain in high-risk sectors. A healthcare and a manufacturing AI provider both report dedicating significant personnel resources specifically for AI Act compliance workflows. They highlight the need for specialized personnel for the project governance of high-risk systems, representing an ongoing operational cost beyond initial compliance investments.

### 4.1.3 Impact on Market Reputation

Interview data from AI providers show a complex perspective on how the AI Act affects innovation, particularly highlighting a divide between established and emerging companies. Although established healthcare and legal technology providers see regulation as potentially beneficial for market trust, emerging companies developing AI applications express serious concerns about standard-based innovation barriers

[104] DIN Media, 'DIN EN ISO 9000:2015-11 :Qualitätsmanagementsysteme - Grundlagen und Begriffe (ISO 9000:2015); Deutsche und Englische Fassung EN ISO 9000:2015', https://www.dinmedia.de/de/norm/din-en-iso-9000/235671064.

[105] European Commission, SWD(2015) 205 final, 'Leitfaden zur europäischen Normung als Unterstützung für legislative und politische Maßnahmen der Union', 27 Oct. 2015, pp. 17 et seq.

[106] Denga, 'Konformitätsbewertung von KI-Systemen', ZfPC 2023, 154 (156, 159); Rostalski/Weiss, 'Der KI-Verordnungsentwurf der Europäischen Kommission', ZfDR 2021, 329 (355 et seq.).

The majority of SMEs classified as high-risk under the AI Act argue that compliance requirements disproportionately affect their scaling ability. Some highlight the uncertainty about risk classification when transitioning from design support to operational systems, while others warn about losing ground to more flexible jurisdictions like the US, where lower regulatory burdens enable faster innovation cycles.

The tendency shows that companies in already regulated sectors such as healthcare appear better positioned to adapt due to their experience with existing frameworks such as the Medical Device Regulation (MDR), while companies in previously unregulated sectors face steeper adaptation challenges. For example, companies operating in education report difficulties in interpreting and implementing AI standards without prior regulatory and technical standards experience to build upon. Additionally, early-stage companies are particularly frustrated by intransparent and bureaucratic conditions that limit experimentation.

#### 4.1.4 Asymmetric Participation in Standards-Settings Process

The interview data reveal a pattern of limited participation in the standards development process of JTC 21, its working groups, and mirror committees in member states. Among the interviewed providers, only a small fraction reports active engagement in AI standardization efforts or formal consultations, with participation levels remarkably low among smaller companies.

Most small and medium-sized providers acknowledge being 'rarely' or 'irregularly' involved in standardization activities, citing resource constraints and knowledge gaps as primary barriers. Several interviewees characterize the standardization process as favoring larger corporations, describing discussions as "one-sided". Multiple providers express concern that this imbalance could lead to standards that create disproportionate barriers for smaller market participants.

While some companies indicate interest in future participation, they emphasize the need for structured support mechanisms. Suggestions include working groups specifically designed for startup participation, consortium models that facilitate SME involvement, and public forums accessible to smaller players.

#### 4.1.5 Fragmentation and Inconsistency Across Jurisdictions

The interview data reveals significant concerns about regulatory fragmentation and inconsistency across jurisdictions high-risk standards might cause.[107] Healthcare AI providers report that discrepancies between regulatory frameworks already delay EU market entry, making the US a more attractive first-market option. Legal tech providers particularly highlight the challenges of conflicting national and EU-level laws, especially regarding professional secrecy and data retention requirements that vary significantly between member states.

Further, cross-sector evidence indicates operational conflicts arising from overlapping regulatory frameworks. Several providers operating in multiple jurisdictions emphasize how varying interpretations of similar requirements across EU member states create implementation challenges. One FinTech startup explicitly compares this to previous experiences with the Payment Service Directive 2 (PSD2) implementation, where fragmented interpretations led to operational inefficiencies.

[107] For frictions / inconsistencies of the AI Act (and its standards) with other sectoral European Union law (esp., for financial products, medical devices, and the automotive sector) see Hacker, 'The AI Act Between Digital and Sectoral Regulations', 2024, pp. 27 et seq., https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/The_AI_Act_between_Digital_and_Sectoral_Regulations__2024_en.pdf.

The data shows particular concern about the readiness of EU regulatory bodies to manage certifications consistently. Multiple companies express worry about delays and inconsistencies in the certification process based on their experience with existing frameworks like MDR, indicating that such delays could disrupt market access even for compliant AI systems.

This fragmentation creates particular challenges for smaller companies, who lack resources to navigate multiple interpretations and certification processes. The evidence suggests that without aligning sector-specific and horizontal requirements, companies may delay EU market entry or prioritize other markets with more streamlined regulatory approaches.

#### 4.1.6 Short Implementations Timelines

Findings show significant concerns about implementation timelines for technical standards. The majority of companies interviewed view the August 2026 deadline as impractical, estimating that 12 months are typically needed for compliance with one technical standard alone (e.g., ISO/IEC 27001), even with external support. Despite existing preparations, e.g., SOC 2 and GDPR compliance, providers emphasize that startups and SMEs facing this process for the first time would face significant market access delays.

On the other hand, some established providers, particularly those already operating under strict regulatory frameworks like medical device regulations, express more confidence in meeting the deadlines. One healthcare provider indicates that the transition is less challenging for them compared to previously unregulated firms due to their existing regulatory framework and data governance practices.

Most interviewed companies indicate that the timeline requires significant allocation of resources and could divert resources from core development activities. Several providers recommend a phased implementation approach, particularly for smaller companies and startups, to allow more realistic adaptation periods.

### 4.2 Sector-Specific Findings

#### 4.2.1 Sectoral Impact of Horizontal Standards

In healthcare and MedTech, there was a contrast between theoretical challenges identified in literature and actual implementation approaches observed. While previous literature emphasizes the challenges of balancing privacy, accuracy, and care quality, research reveals that organizations are finding practical solutions through their existing regulatory experience.[108] The findings indicate that larger healthcare organizations are effectively leveraging their MDR compliance experience to address these very tensions. This sector particularly values the standards' potential to enhance interoperability and seamlessly integrate AI tools into existing systems like electronic health records, while maintaining a strong focus on clinical accuracy and public trust.

The manufacturing sector anticipates close alignment between technical standards and established frameworks like ISO 9001, ISO 31000, and Industry 4.0 protocols. While this integration offers opportunities to improve quality control and standardize data processing practices across facilities, manufacturers face challenges in maintaining comprehensive documentation for AI-driven decisions, especially in high-speed production environments.

[108] Bates et al., 'Health apps and health policy: what is needed?' Jama, 320(19), 2018, pp. 1975-1976.

This aligns with existing literature showing that integrating AI standards with their existing quality management frameworks requires extensive process changes and employee training.[109] Further, it was found that the requirements for extensive pre-deployment testing and validation could potentially slow down the adoption of real-time automation solutions, particularly affecting smaller manufacturers who may struggle with compliance costs.

In the legal tech sector, firms are grappling with the resource-intensive nature of maintaining detailed audit trails for AI outputs, especially when handling sensitive client data. The integration of multiple regulatory frameworks, including GDPR, necessitates technical updates and careful consideration of data governance practices. However, companies view compliance with high-risk standards as an opportunity to establish themselves as leaders in ethical AI practices and strengthen client trust in regulated markets.

In FinTech, the interviews reveal particular concern about overly prescriptive requirements potentially favoring established institutions over startups, with interviewees drawing direct parallels to their experiences with PSD2 implementation. While they view standardization as a potential catalyst for establishing trust and clarity in areas like customer authentication, FinTech companies worry that complex compliance requirements could disproportionately burden smaller firms, echoing patterns seen in previous financial sector regulations.

Across all sectors, smaller organizations face particular challenges in implementation. To address this, stakeholders advocate for specific support measures, including a minimum two-year transition period, example-driven guidance, clear cost structures, and SME-specific compliance pathways. These measures could help bridge the gap between the AI Act's harmonized standards and existing industry standards.

#### 4.2.2 Spillover Effects of Technical Standards

While part of both the mobility/automotive and defense sectors fall outside the AI Act's direct scope (see also Art. 103 et seq. AI Act), they will face huge implications from the AI Act and in particular high-risk AI requirements derived from harmonized standards.[110] The interview data reveals that AI providers in the mobility sector view these standards as a double-edged sword – offering opportunities for enhanced transparency and safety while imposing substantial operational burdens, especially for complex systems requiring advanced explainability and cybersecurity measures. One notable challenge emerged when mobility providers discovered that nearly all their dynamic systems would qualify as high-risk AI, including seemingly routine functions like route planning. This broad classification creates operational challenges, particularly for systems incorporating multiple data points such as traffic patterns and demand fluctuations.

The defense sector, explicitly excluded under Art. 2(3) AI Act for national security reasons, experiences indirect pressure through ecosystem impacts and dual-use considerations. While not directly regulated, defense companies closely monitor the AI Act's potential effects on open-source AI model availability and general AI standards. The sector often adheres to strict safety standards comparable to civilian applications.[111] One interviewed company explicitly recognizes

[109] Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). 'Industry 4.0: The future of productivity and growth in manufacturing industries'. Boston Consulting Group, 9(1), pp. 54-89.

[110] Kilian, 'Nationale Spielräume bei der Umsetzung des Europäischen AI Acts', ZRP 2024, 130 (132); Kilian, 'Nationale Spielräume bei der Umsetzung des Europäischen Gesetzes über Künstliche Intelligenz' – Written statement for the 63rd meeting of the Committee for Digital Affairs of the German Bundestag on May 15th, 2024, pp. 12 et seq.; Hacker, 'The AI Act between Digital and Sectoral Regulations', 2024, p. 33.

[111] For example, some companies are following civil aviation standards / guidelines such as DO-178C/ED12C

that integrating high-risk standards – such as explainability, risk management and transparency frameworks – could enhance safety and interoperability in defense AI systems, particularly for autonomous systems operating in high-stakes environments like urban combat zones or disaster response scenarios.

These implications have led to varying responses across both sectors. Some mobility companies are considering alternative markets with lower regulatory burdens due to financial and operational challenges. Meanwhile, defense companies see potential competitive advantages in adopting high-risk standards, as they could facilitate greater civilian-military collaboration and foster trust in AI-human collaboration systems. Both sectors acknowledge that aligning with high-risk technical guidelines for transparency and interoperability could ultimately benefit their operations, despite the initial implementation challenges.

# 5 Policy Recommendations

Based on the analysis of 23 organizations operating in manufacturing, finance, mobility, defense, organizations are facing challenges in three key dimensions: temporal, structural, and operational. First, the timeline gap between standards publication (expected early 2026) and compliance deadlines (August 2026) allows for only 6-8 months of implementation, while organizations consistently report needing a minimum of 12 months for one standard alone based on prior compliance experience. Second, structural barriers are evident in the standardization process itself, with CEN-CENELEC JTC 21's composition showing strong representation from large enterprises but limited participation from European SMEs due to resource constraints. Third, operational challenges arise from significant compliance costs (€100,000-300,000 annually) and regulatory complexity, particularly affecting smaller organizations and previously unregulated sectors. These findings indicate that without targeted interventions, the current approach may create market entry barriers that disadvantage European SMEs and potentially shift innovation activities to less regulated markets. The following recommendations therefore focus on practical measures to address these challenges within the existing AI Act framework.

To not further prolong implementation, the recommendations focus on measures that can be implemented within the existing framework of the AI Act. They avoid proposing amendments to the AI Act itself, with one exception regarding the implementation timeline. The respective recommendations also comprise the respective addresses, including the European legislator, regulatory EU and national authorities, standardization organizations and the AI community itself.

## 5.1 Adjust Implementation Deadlines

The research findings show that the development and implementation of AI standards for high-risk systems is progressing too slowly, creating significant uncertainty among startups and SMEs, as well as larger companies,[112] about how to comply. Additionally, the majority of companies interviewed view the August 2026 deadline as impractical, estimating that at least 12 months are typically needed for compliance with one standard alone, even with external support. Naturally, for the ca. 35 expected AI standards implementation will take even longer, especially for startups and SMEs with limited resources for compliance matters.

(Software Considerations in Airborne Systems and Equipment Certification).

[112] For further information see 4.1.6.

Consequently, we advise to extend the AI Act implementation timeline to address the critical bottleneck created by delayed harmonized standards development. While high-risk providers under the AI Act can achieve compliance through either harmonized standards (Art. 40 AI Act), common specifications (Art. 41 AI Act) or extensive legal memorandums compared with technical expert opinions (Art. 41(5) AI Act), the current timeline very likely eliminates standards-based compliance as a viable option for organizations already operating. Until the unsuccessful expiry of deadline for the standardisation request, the European Commission cannot establish common specifications,[113] which leaves costly expert opinions as the only pathway to compliance in the medium term.

We strongly recommend the EU legislator to postpone implementation deadlines to restore this balance and allow companies to choose their optimal compliance approach. This is particularly crucial for startups and smaller SMEs, which face disproportionate disadvantages due to resource constraints and competing business priorities. Without these timeline adjustments, the EU risks creating an uneven playing field that could significantly hinder innovation in the European AI ecosystem. Additionally, the amount and complexity of ca. 35 technical standards considered or developed as standardization deliverables by CEN-CENELEC must be reduced to make them more practicable.

In addition to the postponement and reduction, we recommend the following measures: First, publishing an early publication of near-to final standards will let businesses adapt to the final standards sooner rather than later. The internal processes for expert input and decision-making should be streamlined and documents should be edited in English only to speed up the pace of standard development while keeping standards robust. Yet, companies should be aware that there is a significant risk that the pre-final version is subject to change. Interviews with SMEs and startups highlight significant resource constraints in preparing for AI Act compliance. Many lack dedicated compliance teams, making early access to standards crucial for timely preparation. Second, create transparent, easy access through a central online portal to current draft standards where companies can monitor development status and upcoming requirements for free and without standardisation body member status. The portal should also include a low-threshold feedback system where companies, esp. those not directly involved in official committee meetings (mostly startups and SMEs), can give their feedback. This recommendation is supported by feedback from interviewed companies, who consistently expressed a need for clearer, more accessible information on evolving standards. Third, the AI Office and national authorities should foster an ongoing dialogue with affected businesses during the implementation period, adopting a service-oriented approach similar to some of the financial supervisory authority practices (e.g., BaFin). This will enable companies, especially SMEs and startups, to seek clarification and guidance on complex compliance issues. Interviewees emphasized the need for direct communication channels with public authorities and regulatory bodies to address sector-specific challenges and ensure practical implementation of AI standards.

## 5.2 Lower Barriers to Participation

According to the CJEU Malamud ruling, harmonized standards must be accessible to EU citizens free of charge.[114] While it is important that the ruling is to be adhered to by standardization

[113] See section 2.4.1.
[114] See section 2.4.4.

bodies, esp. CEN-CENELEC and ISO/IEC, ultimately leading to free access of applicable law for AI providers, the financial impact on standardization organisations needs to be taken into account.

For accelerating AI standards development, more technical expertise must be integrated into standards committees. Therefore, we call industry and in particular companies out of the Safe AI community to actively participate in standards development. It is crucial to note that industry expertise largely determines the duty of care. The duty of care in this context refers to the legal obligation of AI developers and deployers to take reasonable steps to prevent harm and ensure the safe and responsible use of AI systems.[115]

To achieve this, we recommend that the European Commission or CEN-CENELEC is building industry-specific expert networks on a EU level that can provide targeted guidance for sector-specific compliance challenges. This is particularly important as our findings show that growth-stage startups in high-risk industries have begun preparing for AI standards, while early-stage startups struggle with planning and implementing regulatory requirements due to unclear timelines and guidelines. However, since smaller companies lack the necessary resources for such participation, we strongly recommend that access to standardisation committees must be better financially supported for smaller SMEs and startups, enabling specialized support for industry requirements and effectively addressing sector-specific compliance challenges.

To enable meaningful participation, we recommend establishing substantial funding mechanisms at both EU and federal levels.[116] Specifically, we advocate at the EU level for more dedicated funding programs that subsidize SME participation in standardization committees (explicitly excluding large industry players who have sufficient resources), and significantly expand existing national funding initiatives.[117] While initiatives like StandICT.eu provide some support with €2.925 million in funding for European standardisation specialists, this amount – spread across nine calls over two years – is insufficient given the extensive costs of sustained participation in international standardization.[118] Substantially larger funding mechanisms are needed to ensure European representation across the broad spectrum of technical domains. Beyond, the funding is not specifically aimed to support startup and SME engagement. Additionally, we propose implementing mentorship programs similar to StandICT.eu's initiative, which pairs experienced standardization experts with startup and SME representatives to provide guidance and support.[119] The funding should be calculated based on the actual cost of dedicating personnel to these committees to ensure full coverage of a startup's participation expenses. Additionally, we advise the European Commission to increase awareness and accessibility of existing support initiatives through enhanced communication and outreach efforts.

We urge to promote standardisation committee participation by emphasizing what startups can gain by participating in standardization meetings: direct influence in shaping the regulations

[115] Denga, 'Technologische Ermessensspielräume der Unternehmensleitung', in: DGRI-Jahresband 2021/2022, p. 31.

[116] Also arguing along these lines for standardisation in general High-Level Forum on European Standardisation, 'High-Level Forum Recommendations on Increasing Funding for Standardization Activities at International Level', 11 Nov. 2024, https://ec.europa.eu/docsroom/documents/62954.

[117] Federal Ministry for Economic Affairs and Climate Actions, 'R&D funding provided by the Federal Ministry for Economic Affairs and Energy', https://www.bmwk.de/Redaktion/EN/Artikel/Industry/electric-mobility-r-d-funding.html. For existing scholarship programs for SMEs and civil society organisations to participate in standardization and for preparing for compliance see Hacker, 'The AI Act between Digital and Sectoral Regulation', Dec. 2024, pp. 10, 37.

[118] StandICT, 'standICT.eu 2026 – 7th Open Call', 2024, https://standict.eu/index.php/standicteu-2026-7th-open-call.

[119] StandICT, 'Support to SMEs: SME Mentorship Programme', https://standict.eu/supporting-smes.

governing their technologies. Key to this are visible funding opportunities and simplified committee access. Startups must understand they can actively shape their industry's future rules, rather than simply following them. Therefore, active collaboration between large and smaller companies should be fostered by standardization bodies to promote many-faceted collaborative standardisation.

Finally, we propose overhauling the accessibility of standardization committees, e.g. via a centralized, user-friendly platform, processes, and priorities. This should be realized on a EU and national level, transforming the AI standardization committees to transparently provide information and simplify entry processes. Additionally, a 'standardization guide' system should be implemented where experienced members help newcomers navigate the process. Making these changes is essential to ensure startups can effectively participate in developing the standards that will govern their technologies.

## 5.3 Practical Aid for Implementation

The EU AI Office (and subsequently the national supervisory authorities) should establish pragmatic guidance tools for AI Act compliance, with particular focus on SMEs. This should include regular interpretative guidance, concrete implementation tips, and direct support through dedicated contact persons who maintain ongoing relationships with the AI provider community. This aligns with the AI Office's obligation from Art. 62 AI Act, specifically covering standardised templates, a single information platform, and communication campaigns. The interview findings indicate a strong demand for clear, sector-specific guidance to effective implementation.

### 5.3.1 Financial Support

The European Commission and EU member states should establish dedicated financial support programs specifically designed for pre-revenue startups pursuing AI Act compliance. These programs should provide direct funding to cover compliance-related costs before startups have established revenue streams, ensuring that early-stage innovation is not stifled by regulatory requirements. Financial implementation aid could be provided via participation at regulatory sandboxes under Art. 57 AI Act, which allows startups and regulators to learn from each other's practical experiences.

### 5.3.2 Technical Implementation Guidelines

We suggest the European Commission and the EU AI Office create fast practical, industry specific implementation guidance, aligning with the requirements outlined in Art. 96(1) AI Act. In particular, small startups struggle to even determine if they fall under high-risk AI Act categories according to Art. 6 AI Act. Therefore, we recommend providing example-driven, sector-specific documentation following e.g. the U.S. Food and Drug Administration's (FDA) approach. This includes detailed, sector-specific guidance documents, concrete examples and real-world scenarios for use cases, step-by-step implementation guides and regular updates and industry feedback.[120] This guidance should include standardized compliance templates, and providing concrete use cases

[120] FDA, 'Overview of Device Regulation', 31 Jan. 2024, https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation; FDA, 'Compliance Program: Chapter 56 – Drug Quality Assurance', 17 Oct. 2022, https://www.fda.gov/media/75167/download.

that demonstrate compliance requirements in practice. Rather than relying on abstract or high-level concepts, it should offer precise technical definitions that companies can directly apply to their situations. This recommendation is also in line with the European Commission's obligation stemming from Art. 6(5) AI Act to provide guidelines specifying the practical implementation of Art. 6 AI Act with a comprehensive list of practical examples of use cases of AI systems that are considered high-risk and not high-risk.

Additionally, the implementation of technical standards should be facilitated by standardization bodies developing them in a manner so that they do not need any further operationalization. This can be achieved by focusing on threshold-based requirements and allowing for easier digital access, which presupposes deeper technical expertise among standardization committee members. Another way of facilitating the implementation of technical standards could be the tool developed by CEN-CENELEC in their SMART project, which will enable standard users to automatically extract a concise list of requirements that need to be met in order to implement a standard, rather than just a running text PDF.[121]

### 5.3.3 Implementation Quality and Support

Create a two-way communication system between regulators and key industries falling under the high-risk regulation, to enable real-time understanding of challenges and needs and ensure support addresses actual market needs. This refers to the finding that many providers face challenges interpreting how AI Act requirements align with existing regulations, particularly when systems combine multiple AI modalities. Regulators should systematically monitor and analyze how organizations implement technical standards, using this evidence to identify implementation challenges and develop targeted guidance materials. This structured feedback loop will help with continuous improvement of both standards and support documentation. Such communication could be facilitated within the contemplated regulatory sandboxes pursuant to Art. 57 AI Act, where vice versa regulatory learnings are the legislator's explicit purpose.[122] Regulators, including the AI Office and national authorities, should act as service providers, systematically monitoring and analyzing how organizations implement technical standards. Furthermore, the European Commission should develop guidelines on the practical implementation of the high-risk AI standards (see Art. 96 AI Act).

Based on the findings from the interviews, there is significant concern about the implementation timelines for technical standards, which many companies view as impractical without clear frameworks to guide compliance. Establishing clear evaluation frameworks would help measure progress, ensure accountability, and track improvements through quantifiable metrics, thereby addressing these concerns.

## 5.4 Structured Integration of SMEs in Implementation

We advise swift action on stakeholder engagement (esp., SMEs and startups) and structural support for AI standard implementation through two key initiatives:

Rapidly establish and staff the advisory forum and scientific panel as outlined by Art. 67 AI Act. These bodies must include startup and SME representation as well as sectoral industry

[121] See section 2.4.5

[122] Kilian, 'Nationale Spielräume bei der Umsetzung des Europäischen AI Acts', ZRP 2024, 130 (131). See also Rec. 139 AI Act.

knowledge out of the high-risk application scopes under Annex I and Annex III AI Act to ensure their perspectives and challenges are considered in implementation guidance. Early establishment is crucial for timely, informed decision-making and for pragmatic support for the recommended implementation aid. Build direct consultation channels between AI startups / SMEs and regulatory bodies supported by clear EU-level contact points and extending beyond formal advisory structures. Rather than waiting for SMEs to proactively engage, EU bodies should more actively reach out to startups and SMEs, facilitated by industry associations. The findings show significant willingness from startups to participate in consultations, as demonstrated by high engagement in Federal Ministry of Economic Affairs and Climate Action (BMWK) information sessions and our interview findings. Companies consistently express interest in maintaining direct communication lines with the European Commission and being actively involved in the implementation process.

## 5.5 Standards Alignment

It is recommended that standardization bodies (esp., ISO/IEC, CEN-CENELEC and national mirror committees) align industry-specific vertical standards with Art. 40 AI Act for high-risk AI systems. As this alignment will likely be required by Art. 103 et seq. AI Act, early action prepares industries for future requirements. This approach aligns with findings that some sectors, like healthcare and manufacturing, are already leveraging existing regulatory experience to address AI challenges. Also, European and international AI standards should be aligned as closely as possible, to streamline compliance efforts for companies.[123] Therefore, international, European and national standardisation bodies must cooperate closer. However, it is essential that this cooperation takes place with due consideration of European values.

When developing and implementing harmonized standards, it is crucial to avoid a negative conformity presumption. While non-compliance with technical standards does not legally imply a negative presumption, it can significantly increase the burden on the provider in practice.[124] This allows for necessary deviations from standard catalogs, considering diverse AI technologies and specific use cases that may not have been adequately covered, while still ensuring product safety in the European market. However, care should be taken to prevent market surveillance authorities from interpreting non-compliance with standards as an indication of non-conformity, as observed in product safety law practice.[125]

The compliance burden can be reduced by systematically leveraging existing standards for consistency and interoperability and facilitate entry into international markets. As shown in the findings, this harmonization is also crucial for industries operating adjacent to the AI Act's scope, such as defense and automotive sectors. Rather than creating new legislation or standards, existing regulatory frameworks should be adapted at both federal and EU levels to incorporate AI compliance requirements.

[123] For more detailed recommendations on the alignment between European and international standardisation in general see High-Level Forum on European Standardisation, 'Alignment Between European and International Standards – Final Report', 15 Jan. 2025, https://ec.europa.eu/docsroom/documents/64157.

[124] Denga, 'Konformitätsbewertung von KI-Systemen', ZfPC 2023, 154 (157); Gerdemann, 'Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI', MMR 2024, 614 (618); Wilrich, 'Rechtliche Bedeutung von DIN-Normen und technischen Regelwerken', NJW 2023, 1400 (1404).

[125] Wiebe, 'Produktsicherheitsrechtliche Betrachtung des Vorschlags für eine KI-Verordnung', BB 2022, 899 (902).

Table 3: Policy Recommendations

| Ref. | Addressee | Recommendation |
|---|---|---|
| 5.1 | **EU Legislator / European Commission, CEN-CENELEC** | **Reduce amount of referenced standards and adjust implementation deadlines for AI Act requirements.**<br>• Drastically reduce the amount of ca. 35 technical standards contributing to the standardization request's deliverables.<br>• Extend deadline in European Commission standardization request.<br>• Delay application of AI Act high-risk requirements by min. 12 months. |
| 5.2 | **European Commission (DG Connect, DG Grow), Standardization Bodies** | **Enable and encourage startup / SME participation in standardization processes.**<br>• Subsidize costs for smaller organizations to participate in committees.<br>• Increase transparency and accessibility for existing subsidy programs.<br>• Promote collaborative standardization work between large and small players in inclusive working groups / forums. |
| 5.2 | **European Commission, CEN-CENELEC** | **Ensure free, early and convenient access to (draft) AI Act standards.**<br>• Ensure free and early access to (draft) harmonized AI standards including referenced technical standards for equitable participation.<br>• Mandate free access to standards in alignment with EU legal principles (transparency / openness) according to the ECJ Malamud ruling.<br>• Provide free access to AI Act standards via an easy-to-access platform. |
| 5.3.1 | **European Commission (DG Grow, DG Connect), National Governments** | **Provide financial support to startups and SMEs for their AI Act compliance efforts.**<br>• Allocate direct funding on a European and national level, especially to startups and SMEs.<br>• Develop targeted financial programs for startup / SMEs compliance matters. |
| 5.3.2 | **Standardization Bodies / European Commission** | **Reduce the need for further operationalization by developing threshold-based standards.**<br>• Promote target-based instead of rule- or process-based standards.<br>• Strengthen deep technical AI expertise in standardization committees. |
| 5.3.3, 5.4 | **European Commission, European AI Office, National Authorities** | **Provide clear, sector-specific guidance for AI Act compliance.**<br>• Issue implementation tool kits and evaluation frameworks as an orientation.<br>• Build expert networks based on two-way communication channels with high-risk AI industries.<br>• Offer real-time guidance within institutionalized environment (e.g., regulatory sandboxes). |
| 5.5 | **Standardization Bodies / Committees** | **Align AI Act standards with vertical standards and international standards (esp. ISO/IEC).**<br>• Align industry-specific / sectoral standards with AI Act requirements for high-risk systems.<br>• Align international (esp. ISO/IEC) and European AI standards to streamline compliance.<br>• Collaborate with other standardization bodies on unified technical definitions and compliance procedures. |