European Journal of Risk Regulation (2025), **16**, 1038–1062
doi:10.1017/err.2025.10032

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

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

Robert Kilian[1], Linda Jäck[2] and Dominik Ebel[3]

[1]Faculty of Law, Humboldt University Berlin, German AI Association (KI Bundesverband), Berlin, Germany, [2]General Catalyst, Germany and [3]Faculty of Law, Heidelberg University, Germany
Corresponding author: Robert Kilian; Email: robert.kilian@hu-berlin.de

Abstract

Harmonised 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 harmonised standardisation for organisations providing AI systems. Based on in-depth qualitative interviews with twenty-three 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 start-ups and SMEs, are dealing with the contemplated standardisation under the EU AI Act and sectoral standardisation. Industry sectors covered include mobility, finance, manufacturing, healthcare, as well as defense and legal tech. Key challenges identified comprise an insufficient effective implementation period of likely less than 6 months compared to at least 12 months actually required for around thirty (partially referenced) technical standards, an imbalance of participation and influence in standardisation committees, double regulation and technical implementation hurdles as well as significant annual costs for harmonised 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 start-ups. Hence, the paper offers policy recommendations based on the revealed challenges for AI providers.

Keywords: AI Act; digital regulation; AI regulation; AI standardisation; harmonized standards; technical standards

I. Introduction[1]

The European Union's (EU) effort to regulate artificial intelligence (AI) through the EU AI Act[2] represents the first comprehensive attempt to set harmonised legal rules for safe AI development and deployment. As part of this effort, the European legislator has given technical standardisation a key role,[3] recognising that the deliberately abstract nature of high-risk requirements makes them challenging for stakeholders to implement. Hence, AI

[1] Robert Kilian, Linda Jäck and Dominik Ebel, European AI Standards – Technical Standardization and Implementation Challenges under the EU AI Act. Pre published on SSRN: available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5155591>.

[2] 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."

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

© The Author(s), 2025. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

Act high-risk legal requirements are operationalised by technical standards to make them more prescriptive.[4] 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.[5] 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.[6]

However, as of now, there is limited understanding of how the AI Act's technical specification through standardisation will affect different industries and market participants. Therefore, this paper explores European AI standardisation challenges and opportunities for organisations, based on in-depth qualitative interviews with organisations building and releasing AI applications across different sectors. It specifically examines how organisations, particularly start-ups and small and medium-sized enterprises (SMEs), are dealing with the upcoming technical standardisation following the AI Act. Start-ups and SMEs represent 99% of EU companies but are known to lack resources to participate in standardisation processes.[7] Therefore, the paper uncovers notable differences in how different sectors are preparing for these standards, while also identifying common challenges for organisations. 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 standardisation-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 standardisation under the AI Act and challenges in the said process (2.), the methodology of the research approach is being laid out (3.), before the status quo of the process is being analysed, showing the current (limited) progress on the standardisation deliverables under the AI Act (3.). Based on in-depth interviews with 23 organisations (including start-ups, SMEs, larger corporations and public sector organisations) intending to comply with AI Act high-risk standards across different sectors (e.g., mobility, finance, defense, manufacturing, healthcare), the challenges and opportunities regarding the implementation of these standards are illustrated (4.). Finally, based on the identified challenges, concrete policy recommendations are presented (5.).

[4] For AI Act implementation of technical standards see Robert 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, 15 May 2024) 12ff available at <https://www.bundestag.de/resource/blob/1002540/2c7af0e644c2d1b19d20896994727736/Kilian.pdf> (last accessed 30 May 2025).

[5] cf. Regulation (EC) No 765/2008; Regulation (EU) 2019/1020; Mario Martini and Christiane Wendehorst, Simon Gerdemann, Fabian Wöbbeking, KI-VO Art. 40 (1st edn, 2024), para 2f et seq.; Chiodo, Maurice Chiodo, Henning Grosse Ruse-Khan, Dennis Müller, Lea Ossmann-Magiera and Herbert Zech, Regulating AI: A Matrix for Gauging Impact and its Legal Implementation (March 1, 2024). University of Cambridge Faculty of Law Research Paper No. 12/2024, Available at SSRN: =https://ssrn.com/abstract=4765104 or http://dx.doi.org/10.2139/ssrn.4765104

[6] Philipp Hacker, "The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future" (2023) 51 Computer Law & Security Review 33ff; Robert Kilian, Linda Jäck and Dominik Ebel, Making digital regulation work – The crucial role technical standards play in implementing the EU AI Act, OECD.AI publication, available at https://oecd.ai/en/wonk/making-digital-regulation-work-the-crucial-role-technical-standards-play-in-implementing-the-eu-ai-act (last accessed 30 May 2025); Robert Kilian and Michael Denga, "Das Testen und Zertifizieren von KI-Systemen" (2024) NJW 2945, 2948; DIN, "Standardization Helps Create Innovation-Friendly Framework Conditions for the Technology of the Future" (2019) available at <https://www.din.de/resource/blob/306690/f0eb72ae529d8a352e0b0923c67b6156/position-paper-artificial-intelligence-english–data.pdf> (last accessed 30 May 2025); *German Standardization Roadmap on Artificial Intelligence* (2nd edn, 2022) available at <https://www.dke.de/en/areas-of-work/core-safety/standardization-roadmap-ai> (last accessed 30 May 2025).

[7] Standict.EU, "Support to SMEs – SME Mentorship Programme" (2023) available at <https://standict.eu/supporting-smes> (last accessed 30 May 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

II. Background

1. AI standardisation landscape

There are multiple key stakeholders involved in the global process of AI standardisation, the most important being standardisation bodies, industry players, civil society groups and scientific organisations. With the emergence of AI as a dynamic and global phenomenon, technical standardisation is facing unprecedented challenges.[8] Therefore, these standardisation stakeholders can only partially rely on established standards, but leverage them as foundational references while developing new standards.[9]

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

- ISO/IEC JTC 1/SC 42 (AI), a committee organised by the International Organisation for Standardization (ISO) in collaboration with the International Electrotechnical Commission (IEC), has published 34 standards, with 40 still under development.[10]
- IEEE AI Standards Committee, organised within the Institute of Electrical and Electronics Engineers (IEEE), has produced twelve standards,[11] working on fifty-nine additional standards.[12]
- 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 ten standards,[13] with thirty-three still under development.[14]

On a EU Member state level, the national standardisation bodies installed working committees mainly mirroring the work of ISO/IEC JTC 1/SC 42 (AI) and CEN-CENELEC JTC 21 (AI).[15] 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

[8] For a more in-depth analysis of challenges with AI standardisation from a consumer perspective see Hans-Wolfgang Micklitz, "The Role of Standards in Future EU Digital Policy Legislation: A Consumer Perspective" (2023) available at <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf> (last accessed 30 May 2025).

[9] 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 specialised standards on AI specifics in these realms.

[10] ISO, "ISOIEC JTC 1/SC 42 – Artificial Intelligence" available at <https://www.iso.org/committee/6794475/x/catalogue/p/1/u/1/w/0/d/0> (last accessed 30 May 2025).

[11] IEEE SA, "Artificial Intelligence Standards Committee – Standards" available at <https://sagroups.ieee.org/ai-sc/standards> (last accessed 30 May 2025).

[12] IEEE SA, "Artificial Intelligence Standards Committee – Active PARs" available at <https://sagroups.ieee.org/ai-sc/active-pars/> (last accessed 30 May 2025).

[13] CEN-CENELEC, "Technical Work – CEN Technical Bodies – CEN/CLC/JTC 21 – Artificial Intelligence – Published Standards" available at <https://standards.cencenelec.eu/dyn/www/f?p=205:32:0::::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D> (last accessed 30 May 2025).

[14] CEN-CENELEC, "Technical Work – CEN Technical Bodies – CEN/CLC/JTC 21 – Artificial Intelligence – Work Programme" available at <https://standards.cencenelec.eu/dyn/www/f?p=205:22:0::::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D> (last accessed 30 May 2025).

[15] DIN, "Untergremien von NA 043-01-42 GA" available at <https://www.din.de/de/mitwirken/normenausschuesse/nia/nationale-gremien/wdc-grem:din21:284801493> (last accessed date). 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> (last accessed date), 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> (last accessed 30 May 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

043-01-42 GA. DIN/DKE. Through this, they – like other national standardisation bodies – are actively collaborating with said international bodies.[16] Thereby, national standardisation 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.[17]

2. *Harmonized standards under the AI Act*

Under EU law, a standard is a technical specification adopted by a recognised standardisation body for repeated or continuous application, with which compliance is not compulsory (Art. 2(1) Regulation (EU) 1025/2012. A harmonised standard means a standard developed by an European standardisation organisation (CEN, CENELEC, or ETSI) upon a standardisation request from the European Commission (see Art. 2(1)(c) Regulation (EU) 1025/2012). They are aligned with EU harmonised 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, Article 40(1) lays down the normative foundation for harmonised standards and the presumption of conformity regarding high-risk AI systems.[18] High-risk AI systems are conclusively defined by Article 6 AI Act in conjunction with Annexes I and III, where Annex I focuses 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.).[19] 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.[20] These high-risk systems generally must adhere to the requirements stemming from Chapter III Section 2 AI Act.[21] They will be applicable starting in

[16] DIN, "Nationales Spiegelgremium von CEN/CLC/JTC 21" available at <https://www.din.de/de/mitwirken/normenausschuesse/nia/europaeische-gremien/wdc-grem:din21:339816705> (last accessed 30 May 2025).

[17] S Garrido and Others, "Analysis of the Preliminary AI Standardisation Work Plan in Support of the AI Act" (2023) <doi:10.2760/5847>.

[18] Art. 40 AI Act also provides for the establishment of technical standards regarding GPAI systems, but the EU Commission did not issue a corresponding standardisation 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 December 2024) available at <https://digital-strategy.ec.europa.eu/en/library/second-draft-general-purpose-ai-code-practice-published-written-independent-experts> (last accessed date). For further information on the harmonised standards under the AI Act see Robert Kilian, in Schefzig/Kilian, *BeckOK KI-Recht, Art 40* (2nd edn, June 2025); Simon Gerdemann, "Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI" (2024) MMR 614ff; Robert Kilian and Michael Denga, "Das Testen und Zertifizieren von KI-Systemen" (2024) NJW 2945ff.

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

[20] European Commission, "Commission Staff Working Document: Impact Assessment" SWD (2021) 84 final, 68: 5–15% of European AI providers available at <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence> (last accessed date); appliedAI, "AI Act: Risk Classification of AI Systems from a Practical Perspective" (March 2023): at least 18% out of 106 AI systems <https://aai.frb.io/assets/files/AI-Act-Risk-Classification-Study-appliedAI-March-2023.pdf> (last accessed date); KI Bundesverband and Others, "AI Act Impact Survey" (12 December 2022): 33% out of 113 interviewed AI provider companies <https://aai.frb.io/assets/files/AI-Act-Impact-Survey_Report_Dec12.2022.pdf> (last accessed 30 May 2025).

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

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

August 2026 for Annex III AI systems and August 2027 for Annex I AI systems (Art. 113 AI Act).[22]

To make these requirements actionable, the European Commission has issued a standardisation request to CEN and CENELEC (Art. 40(2) AI Act) in May 2023,[23] which is expected to be amended soon.[24] Once technical standards become harmonised standards through publication in the OJEU, they act as the base for the presumption of conformity according to Article 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 circa thirty-five standardisation activities in fulfillment of the standardisation request.[25] While traditional standardisation 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.[26] 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 standardisation 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).

This EU approach to establishing general legal rules for AI systems and operationalising them through technical standards has not yet been copied on a global scale. For example, in the United States (US) or the United Kingdom (UK), AI is not addressed by centralised, comprehensive regulatory frameworks but rather by soft law.[27] There, mostly non-binding technical standards come into play to specify policy initiatives or sectoral guidelines on AI.[28] In China, technical specifications for AI are often tightly linked with regulations or even developed parallelly.[29] By now, there are mostly recommendatory standards in place, some of which will become de facto mandatory as part of the AI Safety Standard System though.[30] This is similar to the European approach in principle.

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

[23] European Commission, "Commission Implementing Decision of 22.5.2023 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' C(2023) 3215 final available at <https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en> (last accessed 30 May 2025).

[24] cf. ETUC, "Artificial Intelligence Standardisation Inclusiveness Newsletter, Edition 6" (December 2024) p 1.

[25] S Garrido and Others, "Harmonised Standards for the European AI Act" (2024) 4ff.

[26] S Garrido and Others, (n 25) 7.

[27] In general, TechPolicy, "The Need for and Pathways to AI Regulatory and Technical Interoperability" (16 April 2025) available at <https://www.techpolicy.press/the-need-for-and-pathways-to-ai-regulatory-and-technical-interoperability/> (last accessed 1 June 2025). For the UK, Ada Lovelace Institute, "Regulating AI in the UK" (18 July 2023) available at <https://www.adalovelaceinstitute.org/report/regulating-ai-in-the-uk> (last accessed 1 June 2025).

[28] For example, CEIMIA, "A Comparative Framework for AI Regulatory Policy" (2023) 42 available at <https://ceimia.org/wp-content/uploads/2023/05/a-comparative-framework-for-ai-regulatory-policy.pdf> (last accessed 1 June 2025).

[29] Ibid., 42.

[30] See more on the AI Safety Standard System specifying the AI Safety Governance Framework Bird & Bird, "China TMT: Bi-monthly Update – January and February 2025 Issue" (21 March 2025) available at <https://www.twobirds.com/en/insights/2025/china/china-tmt-bimonthly-update-january-and-february-2025-issue> (last accessed 1 June 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

3. Challenges in the AI Act standardization process

However, this legislative approach is challenged by tight implementation timelines, complex stakeholder dynamics, unjustifiable costs for implementation and the additional challenge of operationalisation.[31]

a. Critical timeline

As of now, more than 300 experts from over twenty European Union (EU) Member States are working within CENCENELEC JTC 21 to develop the requested technical standards specifying the AI Act high-risk requirements.[32] Yet, the timeline for developing these standards is highly ambitious and increasingly tight.[33] Initially, the European Commission set an April 2025 deadline for standards development.[34] However, the committee's work is progressing significantly slower than anticipated by the European Commission with first results only expected for late 2025, which the Commission is tolerating this so far without setting a new deadline.[35] The consensus-building process on new work items in JTC 21 has proven challenging, testing the limits of decision-making processes in standardisation committees and leading to delays.[36] The complexity is further compounded by competing interests between global and sector-specific standardisation needs, as well as different requirements across industries, typical for horizontal standards.[37] Also the standardisation deliverables under the AI Act build a complex framework with interactions and dependencies between individual (partly converging, partly diverging) goals.[38] The overall standardisation approach therefore must carefully account for all of these interrelationships to be effective.

However, even after CEN-CENELEC finalises the standards, they must go through an additional review process. The European Commission assesses their compliance with the standardisation request and publishes them in the OJEU, following Article 10, 11 of (EU) No. 1025/2012. This process can take several months before the standards become harmonised under the AI Act and can grant AI providers a presumption of conformity.[39] After the final publication of the standards in the OJEU, currently expected for the beginning of 2026,[40] timing leaves high-risk AI system providers with only about 6–8 months until they need to comply by August 2026 (Art. 113 AI Act).[41] Given that providers will need adequate time to

[31] Hans-Wolfgang Micklitz, (*supra* note 8).

[32] JTC 21, "About the Joint Technical Committee – CEN-CENELEC JTC 21" available at <https://jtc21.eu/about/> (last accessed 30 May 2025).

[33] Robert Kilian, (*supra* note 4) 12ff.

[34] European Commission, "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" C(2023) 3215 final (2023) available at <https://ec.europa.eu/growth/tools-databases/enorm/mandate/593_en> (last accessed 30 May 2025).

[35] A new August deadline, which has now become unrealistic, would roughly match with the median 28.5 months required for technical standards to be finalized after the standardisation request (CEN, "The Default Timeframe for the Development of European Standards" (26 October 2017) available at <https://boss.cen.eu/media/CEN/ref/bt_n_8140.pdf> (last accessed 25 May 2025).

[36] S Garrido and Others, (*supra* n 25) 2.

[37] Castets-Renard and Besse, "Ex Ante Accountability of the AI Act: Between Certification and Standardization, in Pursuit of Fundamental Rights in the Country of Compliance" (2023) 18–20 available at <https://ssrn.com/abstract=4203925> (last accessed 30 May 2025).

[38] 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, optimising an AI system for accuracy might perpetuate bias, if not carefully managed.

[39] Robert Kilian, "Nationale Spielräume bei der Umsetzung des Europäischen AI Acts" (2024) ZRP 130.

[40] 2MLex, "Deadline for AI Standards to be Postponed, EU Standards Chief Says' (1 August 2024) available at <https://mlexmarketinsight.com/news/insight/deadline-for-ai-standards-to-be-postponed-eu-standards-chief-says> (last accessed 30 May 2025).

[41] S Garrido and Others, (*supra* note 25) 1. This is for high-risk AI systems according to Annex III.

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

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 circa thirty-five technical standards that CEN-CENELEC is planning to provide for the AI Act.[42] Especially for start-ups 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.[43] 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 standardisation 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 does not deliver the standards within the deadline set by the European Commission (Art. 41 (1)(a)(ii) AI Act). However, the adoption of common specifications cannot be considered if a harmonised standard is expected to be published within the period of time it would take to adopt an implementing act (Table 1).[44]

b. Complex stakeholder dynamics

Standardisation efforts, involving over 1,000 experts across national mirror committees,[45] are facing a structural challenge regarding stakeholder representation. These standardisation committees are predominantly influenced by large enterprises, with major US technology and consulting companies constituting often the participation majority. This creates a notable disparity in representation, particularly affecting SMEs, start-ups, civil society organisations, 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.[46] 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.[47]

The under-representation of smaller stakeholders in EU AI standardisation stems primarily from the substantial resources required for effective participation in these committees. The resource allocation challenge is particularly acute for smaller organisations, which must prioritise their limited human and financial capital for core operational activities.

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

[43] 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 April 2020) available at <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_589> (last accessed 30 May 2025)).

[44] Mario Martini, Christiane Wendehorst, Simon Gerdemann and Fabian Wübbeking, "KI-VO: Verordnung über Künstliche Intelligenz" (2024) Art. 41, para 17.

[45] DIN/DKE, "Europäische KI-Normung – Endspurt zum AI Act" (17 July 2024) 9 available at <https://www.din.de/resource/blob/1118040/21c9ee1e795105d3d552d8e636ac303f/gesamtpraesentation-ki-webinar-data.pdf> (last accessed 30 May 2025).

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

[47] K Gupta, "The Role of SMEs and Startups in Standards Development" (12 July 2017) 8. See also Dinçkol and Others, "Regulatory Standards and Consequences for Industry Architecture: The Case of UK Open Banking" (27 March 2023) <https://doi.org/10.1016/j.respol.2023.104760> (last accessed 30 May 2025) for how regulatory adjustment can address emerging implementation challenges regarding technical standards.

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

Table 1. Compliance milestones for high-risk AI system providers.

Deadline	Compliance Milestone (AI Act)
April 30, '25	Original deadline for deliverables from SR
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.)

Consequently, industry associations have emerged as crucial intermediaries, bearing the responsibility of aggregating and representing these stakeholders' interests within standardisation 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.[48] Limited participation of smaller entities in standardisation 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 standardisation processes that can effectively incorporate diverse perspectives and expertise.

c. 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 harmonised 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).[49] 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.[50] Specifically, the court argued that such harmonised norms are part of EU law based on their legal effects.[51] However, the situation has further escalated with ISO and IEC issuing a lawsuit against the European Commission before the CJEU on 6 December 2024,[52] aiming to ensure the integrity of their copyright to technical standards that are part of harmonised

[48] Simon Gerdemann, "Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI" (2024) MMR 614, 619ff.

[49] CJEU judgment, 22 February 2022, C-160/20 – Stichting Rookpreventie.

[50] ECJ judgment, 5 March 2024, C-588/21 P – Malamoud.

[51] ECJ judgment, 5 March 2024, C-588/21 P – Malamoud, para 70.

[52] CJEU, International Electrotechnical Commission and ISO v Commission available at <http://data.europa.eu/eli/C/2025/919/oj> (last accessed 1 June 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

standards in the EU and further monetise them. Depending on the outcome of the court proceedings, European standardisation efforts are at risk of losing the contribution of international standardisation organisations.[53]

The current CEN-CENELEC JTC 21 work program encompasses circa thirty-five 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.[54] 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).[55] Failing to meet the compliance deadlines poses significant risks for companies providing high-risk AI systems. 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 start-ups 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.[56]

III. Methodology

This paper is based on a mixed-methods approach with emphasis on qualitative, inductive analysis. The core empirical foundation consists of in-depth interviews with twenty-three AI organisations across the EU, including early-stage start-ups, SMEs, corporates and public sector actors. These organisations span a wide array of sectors such as automotive, transportation, machinery, defense, cybersecurity, healthcare, agriculture, finance, image analysis, legal services, consulting, education, publishing, insurance and manufacturing. Interviewees included companies such as Mistral, Helsing, Merantix, Langdock and Xayn (now Noxtua), with organisational sizes ranging from 5 to over 4,000 employees. All were developing or deploying AI technologies – either as stand-alone systems or integrated into products with safety-relevant implications. Defense companies were deliberately included to explore whether technical standards exert indirect influence through ecosystem effects or dual-use considerations.

In addition to the interviews, a systematic content analysis of publicly available standardisation documents and technical materials from CEN-CENELEC JTC 21 and affiliated working groups was conducted. This included reviews of work item descriptions, committee agendas and draft standards available as of June 2025. To contextualise the European approach, the analysis was supplemented by early comparative insights into regulatory and standardisation practices in other jurisdictions, such as the United States, as well as international standardisation bodies like ISO/IEC and IEEE. Public positioning of stakeholders – for example, through LinkedIn posts or policy briefs – was also examined

[53] Thomas Klindt, "Wie der EuGH am System der europäischen Produktsicherheit sägt" (19 March 2024) available at <https://rsw.beck.de/aktuell/daily/meldung/detail/eugh-malamud-produktsicherheit-europa-normen-klindt> (last accessed 30 May 2025).

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

[55] Simon Gerdemann, "Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI" (2024) MMR 614, 618; Ann-Kristin Mayrhofer, "Produktsicherheit und Produkthaftung – zwei Seiten einer Medaille mit unterschiedlichen Gravuren" (2024) RDi 492, 494ff.

[56] 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, "Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM(2021) 206 final, "Legislative Financial Statement", Sec 1.5.2 available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX> (last accessed 30 May 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

as secondary evidence of regulatory strategy and alignment within the broader AI ecosystem.

This triangulated methodology enabled the identification of both cross-sectoral and sector-specific implementation challenges and informed the policy recommendations outlined in Section V.

IV. Status Quo of the standardisation process

The European Commission's standardisation request for the AI Act outlines ten essential deliverables addressing key regulatory requirements. These deliverables form the foundation for current standardisation 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 standardisation work builds on circa thirty-five standards, most of them addressing individual standardization request (SR) deliverables.[57] Other deliverables as the Artificial Intelligence Trustworthiness Framework and the supporting standards regarding terminology touch upon multiple standardisation deliverables. The standards will form an integrated framework through multiple inter-relationships, such as hierarchical integration or operational dependencies.[58]

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 dashboards presenting the status of work items in European AI standardization as of August 2024[59] and May 2025,[60] as well as (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.[61] 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 standardisation request (April 2025) by more than a year. At the moment, only eight out of circa thirty-five work items have already been published.

In any case, CEN-CENELEC JTC 21 standardisation work is still in progress and this paper can only analyse 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).[62] However, it should be noted that the European Commission in their – not yet published – assessment from February has already expressed criticism regarding the standardisation work of CEN-CENELEC, particularly concerning the scope and the number of referenced standards (Table 2).

[57] Sebastian Hallensleben, "Status Dashboard JTC 21 European AI Standardization" (August 2024).

[58] S Garrido and Others, (*supra* note 25) 3.

[59] Sebastian Hallensleben, (*supra* note 57) available at <https://www.linkedin.com/posts/sebastianhallenslebern_status-dashboard-jtc21-european-ai-standardisation-activity-7235665875112988673-xfEH?> (last accessed 30 May 2025).

[60] Sebastian Hallensleben, "Status Dashboard JTC 21 European AI Standardization" (May 2025) available at <https://www.linkedin.com/posts/sebastianhallensleben_jtc21-status-dashboard-ugcPost-7331425768968716288-vRpt/> (last accessed 1 June 2025).

[61] CEN/CENELEC, 'CEN/CLC/JTC 21 Work programme', available at <https://standards.cencenelec.eu/dyn/www/f?p=205:22:0::::FSP-ORG-ID,FSP-LANG-ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D>.

[62] Nativi, De Nigris and Others, "AI Watch: AI Standardisation Landscape – State of Play and Link to the EC Proposal for an AI Regulatory Framework" (2021) 43–5 <https://doi.org/10.2760/376602> (last accessed 30 May 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

Table 2. Harmonised standards and framework references.[63]

SR	AI Act	Harmonised Standards and Framework References
1	**Art. 9**	*Risk Management for AI Systems:* • ISO/IEC 23894 – IT – AI – Guidance on Risk Management • **AI Risk Management (WI: JT021024)**[82]
2	**Art. 10**	*Governance and Data Quality of Datasets Used to Build AI Systems:* • ISO/IEC/TS 12791 – IT – AI – Treatment of Unwanted Bias in Classification and Regression Machine Learning Tasks • **AI – Concepts, Measures and Requirements for Managing Bias in AI Systems (WI: JT021036)** • ISO/IEC 8183 – IT – AI – Data Life Cycle Framework • ISO/IEC 5259-1 – 5259-4 – Data Quality for Analytics and Machine Learning (ML) • **AI – Quality and Governance of Datasets in AI (WI: JT021037)** • **CEN/CLC/TR 18115 – Data Governance and Quality for AI in the European Context** • **Artificial Intelligence Trustworthiness Framework (WI: JT021007)**
3	**Art. 12**	*Record Keeping Through Built-In Logging Capabilities in AI Systems:* • ISO/IEC 24970 – AI System Logging • **Artificial Intelligence Trustworthiness Framework (WI: JT021008)**
4	**Art. 13**	*Transparency and Information to the Users of AI Systems:* • ISO/IEC 12792 – Transparency Taxonomy of AI Systems • **Artificial Intelligence Trustworthiness Framework (WI: JT021008)**
5	**Art. 14**	*Human Oversight Over AI Systems:* • **Artificial Intelligence Trustworthiness Framework (WI: JT021008)**
6	**Art. 15**	*Accuracy Specifications for AI Systems:* • ISO/IEC 23282 – Evaluation Methods for Accurate Natural Language Processing Systems • ISO/IEC 23281 – AI – Overview of AI Tasks and Functionalities Related to Natural Language Processing • **Evaluation Methods for Accurate Computer Vision Systems (WI: JT021025)** • **Taxonomy of AI Tasks in Computer Vision (WI: JT021044)** • ISO/IEC/TS 12791 – IT – AI – Treatment of Unwanted Bias in Classification and Regression Machine Learning Tasks • **AI – Concepts, Measures and Requirements for Managing Bias in AI Systems (WI: JT021036)** • **Artificial Intelligence Trustworthiness Framework (WI: JT021008)**
7	**Art. 15**	*Robustness Specifications for AI Systems:* • ISO/IEC 24029-3 – AI – Assessment of the Robustness of Neural Networks • ISO/IEC/TR 24029-1 – AI – Assessment of the Robustness of Neural Networks • **AI – Concepts, Measures and Requirements for Managing Bias in AI Systems (WI: JT021036)** • **Artificial Intelligence Trustworthiness Framework (WI: JT021008)**
8	**Art. 15**	*Cybersecurity Specifications for AI Systems:* • ISO/IEC 27090 – Guidance for Addressing Security Threats and Failures in AI Systems • **AI – Cybersecurity Specifications for AI Systems (WI: JT021029)** • Conformity Assessment in Relation to the Technical Solutions to Address AI-Specific Vulnerabilities (n/a) • **Artificial Intelligence Trustworthiness Framework (WI: JT021008)**

(*Continued*)

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

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

Table 2. (*Continued*)

SR	AI Act	Harmonised Standards and Framework References
9	**Art. 17**	*Quality Management for Providers of AI Systems, Including Post Market Monitoring Process:* • ISO/IEC 42001 – IT – AI – Management System • **AI – Quality Management System for Regulatory Purposes (WI: JT021039)**
10	**Art. 43**	*Conformity Assessment for AI Systems:* • ISO/IEC 42006 – Requirements on Bodies Performing Audit and Certification of AI Management Systems • ISO/IEC 29119-11 – Testing of AI Systems • **AI Conformity Assessment Framework (WI: JT021038)** • Conformity Assessment in Relation to the Technical Solutions to Address AI-Specific Vulnerabilities (n/a)
All	**All**	*Supporting Standards (Concepts, Terminology, etc.):* • ISO/IEC 22989:2023 – IT – AI – Artificial Intelligence (AI) Concepts and Terminology • ISO/IEC 22989/prA1 – IT – AI – Artificial Intelligence (AI) Concepts and Terminology (Amendment 1) • ISO/IEC 23053:2023 – Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) • ISO/IEC 23053:2023/prA1 – Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (Amendment 1) • Terminology and Concepts for Domain Engineering of AI Systems (n/a)

1. Risk management

The first standardisation deliverable aims to cover all elements of Article 9 AI Act (Risk Management System) and give specifications for a risk management system regarding AI systems. Following the AI Act, it shall emphasise individual rights protection through a product-centric approach. Most notably, it covers the obligation for testing AI systems (Art. 9(6), (8) AI Act).

While ISO/IEC 23894 provides general guidance on how to manage risks related to AI,[64] its risk definition is not aligned with the AI Act and it is built on a traditional organisation-centric risk management approach.[65] Thus, the upcoming "home-grown" AI Risk Management standard will address these shortcomings. Especially, it will include a risk definition in line with Article 3 AI Act and a product-centric risk management perspective to address specific impacts on health, safety and fundamental rights of individuals.[66] The specifications shall also be integrable with existing risk management systems according to Annex I, Sec. A AI Act.[67]

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 Article 10 AI Act (Data and Data Governance), which focus on statistical validation and bias prevention (esp., Art. 10(2)(f), (g) AI Act).

[64] CEN/CENELEC, "CEN/CLC/JTC 21 Work Programme" available at <https://standards.cencenelec.eu/dyn/www/f?p=205:22:0::::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D> (last accessed 30 May 2025).

[65] S Garrido and Others, (*supra* note 25) 4.

[66] Ibid.

[67] European Commission, C(2023)3215, p 4 ("Annex II, Section A" is "Annex I, Section A" in the final version of the AI Act). For further information on the draft standards see Robert Kilian, in Schefzig/Kilian, BeckOK KI-Recht, Art. 40 (2nd edn, June 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

The standards primarily published, and partly still under drafting/approval will center on quantifiable measures of data quality and statistical properties throughout the AI system lifecycle.[68] Particularly significant is the Article 10 AI Act requirement for empirical validation of bias mitigation techniques and the ability to demonstrate the effectiveness of quality assurance measures.[69] This emphasis on measurable outcomes represents a methodological shift from descriptive to prescriptive standardisation, requiring organisations to implement verifiable controls for data representativeness, correctness and completeness.[70]

3. Record keeping

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

While the Artificial Intelligence Trustworthiness Framework builds an overarching frame, ISO/IEC 24970 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.[71] 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.

4. Transparency and information to users

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

For ISO/IEC 12792, 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.

5. Human oversight

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

The Artificial Intelligence Trustworthiness Framework must establish comprehensive requirements for ensuring effective human control over AI systems.[72] The standards 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, the standard 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,

[68] S Garrido and Others, (*supra* note 25) 4.
[69] Ibid.
[70] S Garrido and Others, (*supra* note 17) 8ff.
[71] S Garrido and Others, (*supra* note 25) 4ff.
[72] Sebastian Hallensleben, (supra note 57).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

and verification procedures to demonstrate the effectiveness of oversight implementations.[73] 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.[74] 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.[75]

6. Accuracy specifications

The Accuracy Specification for AI Systems deliverable addressed the requirements under Article 15(1), (3) AI Act (Accuracy).[76]

The standards establish requirements that go beyond basic performance metrics. Article 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.[77]

7. Robustness specifications

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

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.[78]

8. Cybersecurity specifications

The requirements from Article 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.

The majority of controls from the standards of the ISO/IEC 27090 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

[73] S Garrido and Others, (supra note 25) 5.

[74] Ibid.

[75] Ibid.

[76] The 'accuracy' requirement should be called 'performance' more accurately with accuracy being only one performance metric among many, see Philipp Hacker, "The European AI liability Directives–Critique of a Half-Hearted Approach and Lessons for the Future' (2023) 51 Computer Law & Security Review 34, fn 281; "A Legal Framework for AI Training Data—From First Principles to the Artificial Intelligence Act" (2021) 13 (2) Law, Innovation and Technology 257, 281.

[77] S Garrido and Others, (supra note 25) 5.

[78] S Garrido and Others, (supra note 17) 14 <https://doi.org/10.2760/5847> (last accessed 30 May 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

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.[79]

9. Quality management system

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

The AI – Quality Management System for Regulatory Purposes standard specifically complements ISO/IEC 42001 by focusing on regulatory compliance and builds on multiple ISO/IEC standards.[80] However, additional considerations are required to cover the specificities of AI products, whether embedded in physical products or provided as software services. The new standardisation on quality management systems shall focus on the specific risks addressed by the AI Act from a product-centric view.[81]

10. Conformity assessment

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

The standards currently under consideration and in development will build on existing frameworks, such as the ISO CASCO toolbox, which offers foundational principles and guidance for conformity assessment.[82] 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.[83] 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 standardisation work items is crucial to ensure the resulting standards are complementary and fit for purpose in supporting the implementation of the regulatory framework.[84]

V. Cross-sector and industry-specific implications

1. Cross-sector findings

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

[79] S Garrido and Others, (supra note 25) 6.
[80] Sebastian Hallensleben, (*supra* note 57).
[81] S Garrido and Others, (*supra* note 25) 6.
[82] Ibid.
[83] Ibid.
[84] Ibid.

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

timelines and detailed guidance. This aligns with the observed trend that smaller companies, constrained by limited resources, deprioritise compliance in early stages, often resulting in delayed or insufficient adherence to regulatory demands.

Organisations 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 start-ups 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, start-ups and smaller SMEs face considerable obstacles due to limited operational capacity. These challenges are even more acute for start-ups and SMEs in less regulated industries, which often lack both the experience and resources required to navigate the complexities of harmonised standards effectively and within the designated timeframe.

a. Ambiguity and complexity in compliance

A prominent cross-sector finding is that organisations face 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 start-up 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.

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.

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.

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

These ambiguities particularly affect organisations 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.

b. 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.[85] 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 compliance matters. This represents a significant burden for a start-up with less than twenty 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 minimise regulatory uncertainty and liability risks, even when certification is not strictly mandatory.[86]

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 specialised personnel for the project governance of high-risk systems, representing an ongoing operational cost beyond initial compliance investments.

c. 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 standardisation 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 standardisation activities, citing resource constraints and knowledge gaps as primary barriers. Several interviewees characterise the standardisation process as favouring 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 emphasise the need for structured support mechanisms. Suggestions include working groups specifically designed for start-up participation, consortium models that facilitate SME involvement, and public forums accessible to smaller players.

[85] European Commission, "Leitfaden zur europäischen Normung als Unterstützung für legislative und politische Maßnahmen der Union" SWD(2015) 205 final (27 October 2015) 17ff.

[86] Michael Denga, "Konformitätsbewertung von KI-Systemen" (2023) ZfPC 154, 156, 159; Frauke Rostalski and Erik Weiss, "Der KI-Verordnungsentwurf der Europäischen Kommission" (2021) ZfDR 329, 355ff.

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

d. Fragmentation and inconsistency across jurisdictions

The interview data reveals significant concerns about regulatory fragmentation and inconsistency across jurisdictions high-risk standards might cause.[87] 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 emphasise how varying interpretations of similar requirements across EU member states create implementation challenges. One FinTech start-up explicitly compares this to previous experiences with the Payment Service Directive 2 (PSD2) implementation, where fragmented interpretations led to operational inefficiencies.

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 prioritise other markets with more streamlined regulatory approaches.

e. 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 emphasise that start-ups 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 start-ups, to allow more realistic adaptation periods.

2. Sector-specific findings

a. 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

[87] 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) 27ff available at <https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/The_AI_Act_between_Digital_and_Sectoral_Regulations_2024_en.pdf> (last accessed 30 May 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

emphasises the challenges of balancing privacy, accuracy and care quality, research reveals that organisations are finding practical solutions through their existing regulatory experience.[88] The findings indicate that larger healthcare organisations 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 standardise data processing practices across facilities, manufacturers face challenges in maintaining comprehensive documentation for AI-driven decisions, especially in high-speed production environments.

This aligns with existing literature showing that integrating AI standards with their existing quality management frameworks requires extensive process changes and employee training.[89] 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 start-ups, with interviewees drawing direct parallels to their experiences with PSD2 implementation. While they view standardisation 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 organisations 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 harmonised standards and existing industry standards.

b. 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 harmonised standards.[90] The interview data reveals that AI providers in the mobility sector view these standards as a

[88] DW Bates and Others, "Health Apps and Health Policy: What Is Needed?" (2018) 320 (19) JAMA 1975–1976.

[89] Michael Rüßmann and Others, "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries' (2015) 9 (1) Boston Consulting Group 54–89.

[90] Robert Kilian, (*supra* note 39) ZRP 130, 132; Robert 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, 15 May 2024) 12ff; Philipp Hacker, "The AI Act between Digital and Sectoral Regulations" (2024) 33.

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

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 Article 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.[91] One interviewed company explicitly recognises 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.

VI. Policy recommendations

Based on the analysis of twenty-three organisations operating in manufacturing, finance, mobility and defense, organisations 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 organisations consistently report needing a minimum of 12 months for one standard alone based on prior compliance experience. Second, structural barriers are evident in the standardisation process itself, with CENCENELEC 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 organisations 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, standardisation organisations and the AI community itself.

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

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

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 start-ups and SMEs, as well as larger companies,[92] about how to comply. Additionally, the majority of companies interviewed views 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 circa thirty-five expected AI standards implementation will take even longer, especially for start-ups and SMEs with limited resources for compliance matters.

Consequently, we advise to extend the AI Act implementation timeline to address the critical bottleneck created by delayed harmonised standards development. While high-risk providers under the AI Act can achieve compliance through either harmonised 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 organisations already operating. Until the unsuccessful expiry of deadline for the standardisation request, the European Commission cannot establish common specifications,[93] 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 start-ups 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 circa thirty-five 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. 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. 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 start-ups, to seek clarification and guidance on complex compliance issues.

2. Lower barriers to participation

According to the CJEU Malamud ruling, harmonised standards must be accessible to EU citizens free of charge.[94] While it is important that the ruling is to be adhered to by standardisation bodies, esp. CEN-CENELEC and ISO/IEC, ultimately leading to free access of applicable law for AI providers, the financial impact on standardisation 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

[92] For further information see 4.1.6.
[93] cf. section 2.a.
[94] cf. section 2.d.

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

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.[95]

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. To enable meaningful participation in standardisation for smaller SMEs and start-ups, we recommend establishing substantial funding mechanisms at both EU and federal levels.[96] Specifically, we advocate at the EU level for more dedicated funding programs that subsidise SME participation in standardisation committees (explicitly excluding large industry players who have sufficient resources), and significantly expand existing national funding initiatives.[97] While initiatives like StandICT.eu already provide some support with €2.925 million in funding for European standardisation specialists, this amount is insufficient given the extensive costs of sustained participation in international standardisation.[98] Additionally, we propose implementing mentorship programs similar to StandICT.eu's initiative, which pairs experienced standardisation experts with start-up and SME representatives to provide guidance and support.[99]

We urge to promote standardisation committee participation by emphasising what start-ups can gain by participating in standardisation meetings: direct influence in shaping the regulations governing their technologies. Key to this are visible funding opportunities and simplified committee access. Start-ups 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 standardisation bodies to promote many-faceted collaborative standardisation.

Finally, we propose overhauling the accessibility of standardisation committees, e.g., via a centralized, user-friendly platform, processes, and priorities. This should be realized on an EU and national level, transforming the AI standardisation committees to transparently provide information and simplify entry processes.

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.

[95] Michael Denga, "Technologische Ermessensspielräume der Unternehmensleitung" in DGRI-Jahresband 2021/2022 (2022) 31.

[96] 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 November 2024) available at <https://ec.europa.eu/docsroom/documents/62954> (last accessed 30 May 2025).

[97] Federal Ministry for Economic Affairs and Climate Actions, "R&D Funding Provided by the Federal Ministry for Economic Affairs and Energy" available at <https://www.bmwk.de/Redaktion/EN/Artikel/Industry/electric-mobility-r-d-funding.html> (last accessed 30 May 2025). For existing scholarship programs for SMEs and civil society organisations to participate in standardisation and for preparing for compliance see Hacker, "The AI Act between Digital and Sectoral Regulation" (December 2024) 10, 37.

[98] StandICT, "standICT.eu 2026 – 7th Open Call" (2024) available at <https://standict.eu/index.php/standicteu-2026-7th-open-call> (last accessed 30 May 2025).

[99] StandICT, "Support to SMEs: SME Mentorship Programme" available at <https://standict.eu/supporting-smes> (last accessed 30 May 2025).

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

a. Financial support

The European Commission and EU Member States should establish dedicated financial support programs specifically designed for pre-revenue start-ups pursuing AI Act compliance. These programs should provide direct funding to cover compliance-related costs before start-ups 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 Article 57 AI Act, which allows start-ups and regulators to learn from each other's practical experiences.

b. 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 Article 96(1) AI Act. In particular, small start-ups struggle to even determine if they fall under high-risk AI Act categories according to Article 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.[100]

This guidance should include standardised compliance templates, and providing concrete use cases 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.

Additionally, the implementation of technical standards should be facilitated by standardisation bodies developing them in a manner so that they do not need any further operationalisation. This can be achieved by focusing on threshold-based requirements and allowing for easier digital access, which presupposes deeper technical expertise among standardisation committee members.

c. 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 analyse how organisations 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 Article 57 AI Act, where *vice versa* regulatory learnings are the legislator's explicit purpose.[101] Furthermore, the European Commission should develop guidelines on the practical implementation of the high-risk AI standards (see Art. 96 AI Act).

[100] FDA, "Overview of Device Regulation" (31 January 2024) available at <https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation> (last accessed date); FDA, "Compliance Program: Chapter 56 – Drug Quality Assurance" (17 October 2022) available at <https://www.fda.gov/media/75167/download> (last accessed 30 May 2025).

[101] Robert Kilian, (*supra* note 39) ZRP 130, 131. See also Rec 139 AI Act.

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press

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.** • Drastically reduce the amount of ca. 35 technical standards contributing to the standardisation request's deliverables. • Extend deadline in European Commission standardisation request. • Delay application of AI Act high-risk requirements by min. 12 months.
5.2	**European Commission (DG Connect, DG Grow), Standardisation Bodies**	**Enable and encourage start-up/SME participation in standardisation processes.** • Subsidise costs for smaller organisations to participate in committees. • Increase transparency and accessibility for existing subsidy programs. • 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.** • Ensure free and early access to (draft) harmonised AI standards including referenced technical standards for equitable participation. • Mandate free access to standards in alignment with EU legal principles (transparency/openness) according to the ECJ Malamud ruling. • 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 start-ups and SMEs for their AI Act compliance efforts.** • Allocate direct funding on a European and national level, especially to start-ups and SMEs. • Develop targeted financial programs for start-up/SMEs compliance matters.
5.3.2	**Standardization Bodies/European Commission**	**Reduce the need for further operationalization by developing threshold-based standards.** • Promote target-based instead of rule- or process-based standards. • Strengthen deep technical AI expertise in standardisation committees.
5.3.3, 5.4	**European Commission, European AI Office, National Authorities**	**Provide clear, sector-specific guidance for AI Act compliance.** • Issue implementation tool kits and evaluation frameworks as an orientation. • Build expert networks based on two-way communication channels with high-risk AI industries. • Offer real-time guidance within an institutionalised environment (e.g., regulatory sandboxes).
5.5	**Standardisation Bodies/Committees**	**Align AI Act standards with vertical standards and international standards (esp. ISO/IEC).** • Align industry-specific/sectoral standards with AI Act requirements for high-risk systems. • Align international (esp. ISO/IEC) and European AI standards to streamline compliance. • Collaborate with other standardisation bodies on unified technical definitions and compliance procedures.

4. Structured integration of SMEs in implementation

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

Rapidly establish and staff the advisory forum and scientific panel as outlined by Article 67.

AI Act. These bodies must include start-up and SME representation as well as sectoral industry 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 start-ups/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 start-ups and SMEs, facilitated by industry associations. The findings show significant willingness from start-ups 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. Standards alignment

It is recommended that standardisation bodies (esp., ISO/IEC, CEN-CENELEC and national mirror committees) align industry-specific vertical standards with Article 40 AI Act for high-risk AI systems. As this alignment will likely be required by Article 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.[102] 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.

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 harmonisation 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 (Table 3).

[102] 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 January 2025) available at <https://ec.europa.eu/docsroom/documents/64157> (last accessed 30 May 2025).

Cite this article: R Kilian, L Jäck, and D Ebel (2025). "European AI Standards – Technical Standardisation and Implementation Challenges under the EU AI Act". *European Journal of Risk Regulation* **16**, 1038–1062. https://doi.org/10.1017/err.2025.10032

https://doi.org/10.1017/err.2025.10032 Published online by Cambridge University Press