AI governance and standards

Policy paper

Executive summary

The paper responds to the growing risk of fragmentation in global governance of artificial intelligence (AI). As countries and regions develop their own AI laws, policies and regulations, and even standards, divergent approaches are emerging. The paper highlights the important role of international and market-driven standards in supporting a broad range of government approaches to AI oversight and discusses how standards can help bridge legal differences across jurisdictions.

Standards can provide consistent, practical solutions and guidance to comply with laws, policies and regulation. When governments reference standards as the means to implement non-technical or high-level performance requirements, they avoid writing technical requirements that may introduce unnecessary costs to make products/services available in their jurisdiction. National or regional technical requirements introduced through regulation or standards create complexity for businesses of all sizes, increase compliance costs, limit national productivity gains by impeding AI adoption and risk slowing cross-border collaboration and innovation.

To ensure effective and interoperable AI governance, greater adoption of standards is essential. Businesses and governments can also bring critical expertise and operational insight to the standards development process itself. Promoting the use of market-driven standards can reduce duplication, improve regulatory coherence and support policy objectives.

1. Why we need standards and what they help us achieve

From companies developing algorithms to those deploying AI services or systems for their end-users, each participant in the AI supply chain needs clear, consistent guidelines. International standards are a vital tool for establishing these shared expectations. They serve as a foundation for fostering interoperability, providing the means for regulatory alignment and facilitating the global dissemination of AI innovation.

Standards bodies maintain the standards they produce and regularly determine if each standard should be revised, confirmed or withdrawn. This ability to evolve alongside AI technologies is an important feature of standards (in comparison to other mechanisms) that keep them relevant and effective over time.

What are standards?

Standards are documents specifying requirements, guidelines, or characteristics of a product, service, process, or system.

They are developed in rules-based, voluntary, multistakeholder organisations that can be horizontal or sectoral and can be national, regional or international. Examples of prominent information technology international and market-driven standards bodies include the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC), the International Telecommunications Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF) and the European Telecommunications Standards Institute (ETSI).

Standards development organisations tend to have mature governance systems, particularly due to process requirements[1] that take the time needed to elicit contributions from a broad set of

[1] World Trade Organisation (WTO), Principles for the Development of International Standards, Guides and Recommendations (2024).

stakeholders and establish consensus among them. The process is intended to produce high-quality results that reflect the best available technical solutions or guidance to build public trust and legitimacy especially in sectors like health, justice and education. Regulation can benefit from this deliberative process by citing standards to frame a regulatory approach or set more specific requirements to carry out the regulation.

How are standards and other soft law mechanisms used in relation to AI technologies?

There are a variety of soft law mechanisms available that can be used to govern information technology: standards, open-source software (OSS), high-level expert group findings, requirements mandated through the supply chain (i.e. requirements imposed through procurement), codes of conduct and guidelines.

AI systems and solutions are often built from parts produced by different actors, often in different jurisdictions. Standards contribute to the vital objective of assuring responsible, safe, secure and interoperable AI systems and solutions by fostering technical consistency and regulatory alignment. This harmonisation is essential for maintaining consistency in these practices and compliance across global markets. In the field of AI, some standards are developed with the goal of harmonising foundational concepts or to promote responsible AI management practices. Standards can also provide the means to address broad principles, including principles that are defined in laws and regulation. Other standards are being developed to manage safety and security risks to protect the information managed on those systems as well as the persons and organisations involved. Risk management and AI governance are two areas where standards provide consistency of concepts and approach to risk management and system assurance, as discussed in the case studies below.

Other soft law mechanisms also play valuable roles and are sometimes conflated with standards. In information technology (IT) and operational technology (OT), technical interoperability is often supported by the use of OSS implementation which serves as a methodology for collaborative software development. OSS is widely used to define application programming interfaces (APIs) and protocols.

Technology-specific principles, codes of conduct and guidelines (e.g. secure and safe software engineering) can be developed to outline the norms of behaviour and/or best practice expected from a certain group of actors or experts, including to define how to comply with laws and regulations. For example, the Organization for Economic Cooperation and Development (OECD) adopted groundbreaking AI Principles in 2019[2] which have been formally adhered to by the OECD's 38 member countries, the European Union and nine other countries. Another example is the Hiroshima Code of Conduct for Organizations Developing Advanced AI Systems[3] adopted by the G7 in 2023, on which companies can voluntarily contribute to an OECD reporting framework[4] on their actions to adhere to the code.

Many organisations struggle to adopt AI standards due to a lack of awareness, technical expertise, or regulatory clarity. Regarding the second factor (technical expertise), while there is a growing body of guidelines and frameworks, there is still a need for detailed practical information to guide the comprehensive and coherent implementation of standards which serve also to guide organisations on how to comply with growing regulatory developments. These

---

2 Organisation for Economic Co-operation and Development (OECD), OECD AI Principles (2019, updated 2024).
3 G7, Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems (2023).
4 G7, Hiroshima Process Reporting Framework (2025).

kinds of guides with practical information are best developed through community-driven initiatives that can develop resources (e.g. specific use case guidance, open-source tools) outside of the more formal process used to determine where and how stakeholders can agree to requirements in standards.

International standards can significantly lower barriers to entry for small- and medium-sized enterprises (SMEs) by providing scalable solutions for both customer assurance and regulatory compliance.

2. The current standards landscape

Worldwide, there are hundreds of private organisations developing IT standards. Among those, there are a relatively small number of organisations developing AI standards. These specialised bodies are pivotal in addressing the unique challenges posed by AI technologies, including digital content transparency, security, fairness and accountability. Most of these organisations have many standards projects under development.

The rapid pace of AI development demands agile and adaptable standards that can keep up with evolving technologies. Standards development may be anticipatory or reactionary (or somewhere in between) with respect to products and services entering the marketplace. One of the strengths of the AI standards-setting 'system' has been its ability to act upon global recognition of the need for interoperable standards.

In fact, AI-specific standards started before 2020, and the development of AI standards is progressing rapidly across a range of national, regional, and international bodies. Many initiatives emphasise transparency, fairness, safety and accountability in AI systems, helping to align efforts toward trustworthy AI.

Globally, various organisations, including the ISO, IEC, IEEE, ITU, European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC), ETSI and other smaller industry-led consortia, e.g. Coalition for Content Provenance and Authenticity (C2PA), are actively working on standards to guide the responsible development and deployment of AI.

In Europe, CEN and the CENELEC are playing a crucial role in aligning AI standards with the EU AI Act. In May 2023, the European Commission tasked the CEN and CENELEC to develop standards for the EU AI Act's[5] high-risk provisions. The EU AI Act requires high-risk AI system providers to implement quality and risk management systems even after a product is placed on the market. Harmonised European standards will provide a path to meet these requirements.

Additionally, intergovernmental initiatives such as those led by the OECD, UNESCO or the Council of Europe are contributing to the conversation by establishing terminology and principles that contribute to the development of technical and regulatory standards. Industry-driven standards play a vital role in translating high-level principles and initiatives into practical, interoperable solutions, providing guidance on AI governance, risk management and security considerations.

Government activities in AI standards development

Governments are engaged in developing AI standards to guide the responsible use of AI. In the United States, the National Institute of Standards and Technology (NIST) has been actively

[5] European Union, EU Artificial Intelligence Act (2024).

working also in developing standards in alignment with the Executive Orders (from the White House) as well as the laws and regulations in progress on the matter. Many of those standards are actively used in Canada and Latin America. At the same time, the EU is working on the first Code of Practice[6] for providers of general-purpose AI models, including those considered to pose systemic risks, in anticipation of the EU AI Act coming into effect in August 2025 for these models. The Code of Practice is intended to serve as a bridge ahead of the development and availability of formal standards. Regional or sectoral standards should remain fully compatible with and wherever possible identical to existing international standards such as ISO/IEC standards to prevent market fragmentation.

What are the benefits of standards for AI, what are the challenges and how can we overcome them?

International and market-driven standards can play a key role in fostering globally interoperable AI governance and drive interoperability. This is important for making it easier for organisations and companies to collaborate across borders by providing ways to conform with regulatory and/or customer requirements at a global level, access the best products and tools, and enable the benefits of AI to be spread as broadly as possible. Duplicative and potentially conflicting standards and compliance schemes, however, raise the costs of doing business in an increasingly globalised world, undermining this potential for interoperability.

The growing development of global, regional and national AI policies, laws and regulations risks creating divergent governance approaches and creating a complex regulatory landscape which hinders the potential to spread the technologies across borders. In addition, there can be inconsistencies between policies and technical standards, given that standards often emerge from the needs of technology developers and deployers and not from regulatory needs. However, more often, standards provide a common approach, even where legal and regulatory approaches differ between countries and regions. In addition, they enhance trust among consumers and businesses in AI technologies.

Referencing standards in regulations can explain how to meet the requirements or facilitate the implementation of a regulation, but they cannot extend regulation. Said another way, they are not a substitute for the role of governments. One way to address these issues is therefore for policymakers to consider referring to market-driven standards when designing laws and drafting regulations or allow for conformance with a standard to be considered sufficient for meeting regulatory requirements. Standards can thus support regulation, and policymakers can benefit from taking them into account.

Relatedly, the Global Digital Compact (GDC)[7], adopted in September 2024 by the UN General Assembly, called on standards developing organisations "to collaborate to promote the development and adoption of interoperable AI standards that uphold safety, reliability, sustainability and human rights". Such collaboration and coordination around AI standards is important to promote interoperability and support policymakers' use of standards.

In addition to referencing standards (specifically or generally) in laws and regulations, it is important for standards to be incorporated into procurement processes over government-unique standards or technical requirements. This is a tool for driving interoperability and avoiding fragmentation, as it can help guide smaller companies, often not involved in or aware of the

6 European Commission, General-Purpose AI Code of Practice (effective August 2025).
7 UN, Global Digital Compact, (2024).

standards development process, to use a common approach. As trust mechanisms, governance standards can also facilitate commercial contracting and demonstrate conformity to regulations.

Potential for overlaps, duplications and divergences in AI standards

There are several factors that may result in overlaps, duplications or divergences in AI standards:

1. Overlaps and duplications:

- **Regulatory fragmentation:** While international bodies like ISO and IEC are developing foundational/horizontal AI standards that align with regulation at a high level while remaining country/region agnostic (e.g. ISO/IEC 42001[8], 23894[9] and 42005[10]), the European Commission (EC) has requested that CEN-CENELEC develop standards to carry out requirements of the EU AI Act, potentially fragmenting markets and/or creating overlapping but slightly differing technical requirements. In the case of NIST AI documents, they can also overlap because they can arise from US Executive Orders and/or US laws and regulations.
- **Proliferation of standards:** Standards organisations are compelled to start new projects to address new trends in AI, when limited or no changes to existing standards are sufficient.
- **Policy-driven standard setting:** Some participants attempt to address their specific public policy or trade interests and issues through standards projects. These parties see opportunities in the drafting process to encourage the adoption of policies that reflect their agendas.

2. Divergences:

- **Regulatory vs. voluntary standards:** Harmonised European AI standards, meaning those standards that are officially aligned with the EU AI Act, provide a clear path for the presumption of conformity. Unless ISO, IEEE and other international efforts are recognised through the European standardisation bodies, they remain voluntary in the European context. Some standards focus only on a limited set of use cases, particularly when they are primarily designed to demonstrate compliance of regulation for these use cases (e.g. high-risk EU AI Act use cases).
- **Related standards:** Standards on data sharing or data integrity need to be carefully calibrated so as not to inadvertently accelerate fragmentation of AI standards.
- **Terminology and scope differences:** Various bodies use different terminologies and methodologies to define AI risks, transparency and robustness as well as security and safety, and it is unclear if such inconsistencies might lead to significant differences in implementations across sectors and jurisdictions.

Furthermore, standards-setting efforts are often slow compared to the fast-paced evolution of AI technologies, which could lead to a gap between emerging AI applications and the regulatory or technical guidance needed to ensure their responsible use.

However, it is important to note:

- Groundbreaking or anticipatory standards (in any field) often require more time to develop, but can be more responsive than regulation.

---

8 International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IEC), ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system (2023).

9 International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IEC), ISO/IEC 23894:2023 Information technology—Artificial intelligence—Guidance on risk management (2023).

10 International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IEC), ISO/IEC 42005:2025 Information technology—Artificial intelligence (AI)—AI system impact assessment (2025).

- Standards organisations often start new projects to address new trends, even though existing standards or minor updates to them could address these issues.
- Efforts to create mutual recognition mechanisms, streamline standards where possible and ensure alignment with broader digital governance frameworks will be key to fostering a more coherent and effective AI standards ecosystem.

Case studies: Core international AI standards

Market-driven standards play a crucial role in AI governance by establishing common expectations across the global AI supply chain. The cornerstone of these standards is ISO/IEC 42001, requiring organisations adopting this standard for responsible AI to implement management practices such as demonstrating their ability to evaluate and mitigate risks, maintaining high-quality data documentation practices and ensuring clear communication with partners and customers. Additionally, organisations using or developing high-risk AI systems must implement controls at a system level demonstrating responsible AI design, development and use, such as: Completion of system impact assessments; responsible system lifecycle design and development and data for AI systems. Compliance can be verified through independent audits.

Supporting standards complement ISO/IEC 42001, including frameworks for assessing and managing risks (ISO/IEC 23894), evaluating potential impacts on the organisation and individuals (ISO/IEC 42005) and ensuring data quality throughout the AI development process (ISO/IEC 5259-2)[11] . These standards serve multiple audiences—from technology companies seeking to build trustworthy AI systems to government agencies developing policies and organisations looking to procure AI solutions. As AI systems are fundamentally IT systems, they must be secured with established information security practices, such as ISO/IEC 27001 and 27002, and ISO/IEC 27002, as well as privacy practices, such as ISO/IEC 27701.

However, AI-specific threats also need to be considered. A forthcoming standard (ISO/IEC 27090) will provide AI-specific security guidance. In global trade and supply chain contexts, especially for generative AI and AI agents, structured, semantic data plays a critical role in ensuring accurate, safe and efficient operations. The ICC Digital Standards Initiative (ICC DSI) has advanced this through its Key Trade Documents and Data Elements (KTDDE)[12] modelling work, based on the UN Centre for Trade Facilitation and Electronic Business (UN/CEFACT)'s United Nations Trade Data Elements Directory (UNTDED) ISO 7372[13], which standardises trade documentation and enhances machine interpretability. UN/CEFACT's recent whitepaper further explores how AI can support trade facilitation by leveraging such structured data approaches.[14]

Industry can demonstrate its commitment to responsible AI by adopting international standards, while government entities and purchasers can reference them in legislation,

11 International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IEC), ISO/IEC 5259-2:2024 Artificial Intelligence—Data Quality for Analytics and Machine Learning (ML)—Part 2: Data Quality Measures (2024).

12 International Chamber of Commerce (ICC), Digital Standards Initiative, Key Trade Documents and Data Elements (KTDDE) (2024).

13 International Organisation for Standardisation (ISO), ISO 7372:2005 Trade Data Interchange—Trade Data Elements Directory (June 2005; reviewed 2019).

14 UN, White Paper on the Use of Artificial Intelligence to Facilitate Trade Procedures (2024).

policy development and procurement processes to meet established trust and security requirements benchmarks.

AI risk management forms a cornerstone of AI governance. It refers to frameworks that define policies, procedures, roles and responsibilities across the AI lifecycle that organisations can adopt in order to develop, deploy and maintain AI systems in a way that minimises risks and attains ongoing regulatory compliance. Implementation of such risk management practices has been mandated under several AI regulations. Leveraging existing best practice reference points can help drive interoperability among domestic AI policy and regulation and accelerate the implementation of risk management frameworks. ISO/IEC 23894:2023 AI Risk Management, published in December 2023, provides guidance on how organisations can manage risks specifically related to AI and is applicable for organisations of any size and across sectors. In addition, NIST's AI Risk Management Framework (RMF)[15], version 1.0 of which was published in January 2023, supports responsible development, use and evaluation of AI products and services and is publicly available at no cost. NIST has also published various crosswalks to the RMF, including one to ISO/IEC 42001: NIST Crosswalks[16].

Although approaches to detailed requirements such as risk assessment and management may vary across organisations, adopting voluntary consensus-based standards (for example, the extensive work of ISO/IEC JTC 1 SC42[17], including ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005, ISO/IEC 38507[18]) can serve as a solid foundation for managing AI risks throughout the AI system's lifecycle and ensure an internationally consistent approach to implementation of AI laws.

3. Recommendations

To ensure that AI standards effectively support responsible AI governance globally, policymakers and different stakeholders should consider the following recommendations:

- **Promote strategic alignment in AI standards-development:** Ensure that AI standards are developed in relation to identified market needs, command strong business support and do not conflict or overlap with widely used standards.
- **Ensure domestic/local businesses' and experts' voices are part of AI standards development:** Given the many benefits of international standards, governments should raise awareness of the opportunity to influence market-driven standards and encourage local experts from all domestic sectors to participate in standards development, including businesses that design, develop and deploy AI systems. Industry expertise is crucial for creating practical, implementable standards that align with technological advancements, and local expertise is crucial for shaping standards with local market realities.
- **Prioritise industry-driven and globally recognised standards over strictly national or regional regulatory compliance approaches:** An industry-led, international standard fosters interoperability, accelerates innovation and ensures that standards remain practical, adaptable and rooted in real-world applications.

---

15 National Institute of Standards and Technology (NIST), NIST AI Risk Management Framework (AI RMF) (2023).
16 National Institute of Standards and Technology (NIST), AI RMF Crosswalk Documents (2023-2025).
17 International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), ISO/IEC JTC 1/SC 42: Artificial Intelligence—Subcommittee on Standardization in the Area of Artificial Intelligence.
18 International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), ISO/IEC 38507:2022 Information technology—Governance of IT—Governance implications of the use of artificial intelligence by organizations (2022).

- **Champion multistakeholder collaboration in AI standardisation:** Governments should promote engaging in standards and advocate for their benefits within their countries and in multi- and bi-lateral talks. AI standards should be developed through transparent, inclusive and multistakeholder processes that involve volunteers from all sectors: industry leaders, academia, civil society and policymakers. This ensures that standards are robust, balanced and reflective of diverse perspectives, enhancing their legitimacy and adoption. AI is a global technology, and regulatory fragmentation can hinder innovation and cross-border collaboration. At the same time, fragmentation can also impose complexity at compliance level and costs, especially for SMEs.
- **Leverage existing standards:** AI regulatory or other governance initiatives should reference published standards, such as ISO/IEC 23894 (based on the widely accepted standard ISO 31000[19]), ISO/IEC 42001 on AI risk management (analogous to ISO/IEC 27001[20] for information security) and ISO/IEC 42005 (AI system impact assessment, which covers a complementary angle to risk management, considering harms and benefits of AI systems to individuals, societies and the environment). They should equally encourage voluntary adoption on a wider scale and as a means of demonstrating responsible business practices and providing assurance to consumers and citizens. This approach not only fosters trust but also streamlines compliance processes, enhancing the credibility and effectiveness of AI governance frameworks. In addition, many existing industry-driven standards already provide guidance on AI governance, risk management and security considerations. Policymakers should recognise and incorporate these standards into governance frameworks to avoid duplication of efforts and ensure regulatory coherence.
- **Use standards in public sector procurement:** Governments should incorporate widely supported AI standards into their own policies and public procurement requirements instead of creating government-unique standards or technical requirements. With regards to public procurement outside of the EU, tenders should recognise global standards to avoid distorting competition. Clear and accessible procurement rules are essential for businesses, especially SMEs, looking to enter new markets. By making these regulations easy to understand and comply with, governments can foster greater market participation and drive economic growth. Recognising compliance with established AI governance standards, while also supporting a diverse standardisation ecosystem, public sector entities can lead by example and encourage broader industry uptake.
- **Support the participation of companies in standardisation efforts through funding to participate, tax incentives, training and other resources:** This not only fosters R&D but also facilitates the transition from research to practical application.
- **Enhancing awareness and education:** To overcome the challenges associated with the adoption of AI standards, it is imperative to enhance awareness and educational initiatives. Governments and industry leaders should invest in training programmes and workshops to build technical expertise around AI standards and guidance. By doing so, organisations can better implement these standards, thereby facilitating smoother integration into existing systems and promoting global interoperability.

---

19 International Organisation for Standardisation (ISO), ISO 31000:2018 Risk Management—Guidelines (2018).

20 International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IEC), ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements (2022).

Please cite as:

ICC (2025), ICC Policy paper on AI governance and standards, www.iccwbo.org/news-publications/policies-reports/ai-governance-and-standards/

About the International Chamber of Commerce

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

33-43 avenue du Président Wilson, 75116 Paris, France

T +33 (0)1 49 53 28 28 E icc@iccwbo.org

www.iccwbo.org @iccwbo