T H E M E A S U R E D V I E W

AIQA Global's series on the ideas, standards, and market forces shaping enterprise AI governance. In a field defined by speed and speculation, these articles offer something different: informed perspective grounded in the discipline of measurement. Because the organizations that will lead in AI are the ones that can prove it.

Government's Leading, for a Change

How Regulators Got Ahead of Business on AI Standards

AIQA Global, LLC

March 2026

An Unusual Sequence

In the history of technology regulation, governments typically follow. The pattern is familiar: an industry emerges, scales, creates problems, and then—sometimes decades later—legislators and regulators respond. Environmental regulation followed industrial pollution by generations. Financial regulation followed market crises by years. Data privacy regulation, in the form of the GDPR, arrived nearly two decades after the consumer internet had already transformed how personal data was collected and used.

Artificial intelligence is breaking this pattern. For what may be the first time in the modern regulatory era, governments and intergovernmental organizations are establishing AI standards while a substantial share of businesses have yet to adopt formal AI governance frameworks. The EU AI Act was proposed in April 2021[1] and entered into force in August 2024—at a time when, by multiple survey measures, many enterprises still lacked formal governance structures for AI. The OECD AI Principles were adopted in May 2019,[2] years before most organizations had given serious thought to how they would manage AI risk. The NIST AI Risk Management Framework was released in January 2023.[3] Japan enacted its AI Promotion Act in May 2025.[4] South Korea passed its AI Framework Act in December 2024.[5]

Meanwhile, the private sector is still catching up. As noted in earlier articles in this series, the IAPP's 2025 survey found that while seventy-seven percent of organizations say they are working on AI governance, many of these programs are in early stages.[6] IBM's 2025 Cost of a Data Breach Report found that sixty-three percent of organizations lacked AI governance policies entirely.[7] The gap between what governments have established and what businesses have implemented is striking—and historically unusual. Understanding why this happened, and what it means for enterprises, is the subject of this article.

The Speed of Government Action

The scale and velocity of governmental AI activity is remarkable by any historical standard. The Stanford AI Index Report 2025—one of the most comprehensive annual assessments of AI trends—found that across seventy-five major countries, AI mentions in legislative proceedings increased by 21.3 percent in 2024, rising to 1,889 from 1,557 in 2023. Since 2016, the total number of AI mentions in legislative proceedings has grown more than ninefold.[8]

In the United States, federal agencies introduced fifty-nine AI-related regulations in 2024—more than double the twenty-five recorded in 2023—and these regulations came from forty-two unique agencies, twice the twenty-one agencies that had issued AI regulations the prior year.[9] At the state level, the number of AI-related laws passed rose from forty-nine in 2023 to one hundred thirty-one in 2024.[10]

Globally, the picture is one of coordinated acceleration. The OECD AI Policy Navigator now tracks AI policy initiatives from more than eighty jurisdictions and organisations, cataloging over nine hundred discrete policy initiatives.[11] International AI safety institutes, which did not exist before November 2023, have now been pledged or established by the United States, United Kingdom, Japan, France, Germany, Italy, Singapore, South Korea, Australia, Canada, and the European Union.[12] This is not the slow, reactive regulation that characterized earlier technology eras. It is a proactive, globally coordinated effort to establish governance standards in parallel with—and in many cases ahead of—widespread commercial deployment.

Why Governments Moved First

The historical inversion—government standards preceding private-sector governance infrastructure—is not accidental. It reflects a combination of factors that are specific to AI as a technology and to the political moment in which AI is scaling.

Governments learned from the privacy experience. The regulatory failures of the early internet era—particularly the delayed response to data collection and surveillance practices—created a political consensus that waiting for technology harms to materialize before regulating is unacceptable. The EU's experience with the GDPR, which itself was a response to years of unchecked data practices, gave European legislators both the institutional capacity and the political mandate to act preemptively on AI. The EU AI Act follows the GDPR's model of risk-based regulation, applying graduated obligations based on the level of risk a system poses.

AI's societal risks are visible before widespread adoption. Unlike most previous technologies, AI's potential for harm was extensively studied and publicly debated before it reached mass commercial deployment. Academic research on algorithmic bias, deepfakes, surveillance, and autonomous systems created a substantial body of evidence that legislators could point to as justification for preemptive action. The technology's risks were, in a sense, pre-documented—giving regulators the evidentiary basis to act ahead of harm rather than in response to it.

Intergovernmental coordination created momentum. The OECD AI Principles, adopted in 2019 by forty-two countries, established the first intergovernmental standard on AI and provided the conceptual foundation for the G20 AI Principles endorsed the following month.[13] This early multilateral agreement created normative momentum: once the world's major economies had agreed on principles, individual governments faced both political incentive and institutional support to translate those principles into binding frameworks. The EU AI Act, Japan's AI Promotion Act, and South Korea's AI Framework Act all draw, directly or indirectly, on the OECD principles.

Business moved slowly on governance. The private sector's delay in adopting formal AI governance created a vacuum that governments filled. While enterprises were experimenting with AI tools and scaling deployments, few were building the governance infrastructure that would demonstrate self-regulatory capacity. The governance gap was visible—and it undermined the argument that industry could be trusted to regulate itself. The Stanford AI Index's finding that only one percent of organizations consider themselves AI-mature, despite ninety-two percent planning to increase AI investment, illustrates the depth of the execution gap that made governmental intervention politically irresistible.[14]

The Timeline Enterprises Now Face

The consequence of government's first-mover position is that enterprises now face a regulatory timeline they did not create and, in many cases, are not prepared to meet. The obligations are real, they are phased, and they are approaching quickly.

The EU AI Act's prohibited practices took effect in February 2025. General-purpose AI model obligations took effect in August 2025. The core high-risk AI system obligations under Annex III will take effect in August 2026. Additional high-risk requirements for regulated products under Annex I follow in August 2027.[15] For any enterprise that deploys or uses AI systems in the European market—or whose vendors and partners do—these deadlines define the compliance horizon.

In the United States, the regulatory framework is sectoral rather than comprehensive, but the direction is consistent. Regulators including the FTC, EEOC, CFPB, and DOJ have publicly stated that existing enforcement authorities apply to certain AI-related practices, particularly where automated systems create discriminatory or otherwise unlawful outcomes.[16] The NIST AI Risk Management Framework, while voluntary, provides the most widely referenced U.S. governance structure. The net effect is that enterprises operating in any major market now face AI governance expectations from government—whether in the form of binding regulation, voluntary frameworks, or sector-specific enforcement—regardless of how far along their own internal governance programs may be.

What Government's First-Mover Position Means for Business

The fact that governments moved first has four practical implications for enterprises.

The standards already exist. Enterprises do not need to invent AI governance from scratch. The EU AI Act, the NIST AI Risk Management Framework, and the OECD AI Principles collectively provide a substantial governance framework covering risk classification, documentation, transparency, human oversight, monitoring, and accountability. Organizations that align with these existing standards will be well-positioned to meet current and emerging regulatory requirements. The governance playbook has largely been written. The question is whether enterprises will read it.

Compliance timelines are external, not internal. When an enterprise sets its own governance priorities, it can calibrate the pace of implementation to internal readiness. When government sets the timeline, the enterprise must adapt to an external schedule. The August 2026 high-risk deadline under the EU AI Act is not negotiable based on a company's internal governance maturity. Organizations that have not begun building governance infrastructure are already behind.

First-mover advantage now belongs to the governed. In a regulatory environment where government has defined the standards, the organizations that demonstrate governance quality earliest are positioned to gain competitive advantages: potentially better insurance terms, greater investor confidence, smoother regulatory interactions, and stronger relationships with enterprise customers who are themselves under governance pressure. As governance quality becomes a market differentiator, the organizations that invest before enforcement begins are likely to benefit disproportionately.

The cost of inaction is compounding. Every quarter without a governance framework is a quarter of accumulated regulatory risk, unmanaged shadow AI, undocumented systems,

and growing compliance debt. The EU AI Act's penalties for non-compliance can reach up to 35 million euros or seven percent of global annual turnover for violations involving prohibited AI practices.[17] Even for organizations that do not deploy high-risk systems, the transparency and general obligations of the Act create baseline requirements that demand governance infrastructure.

The Opportunity in the Inversion

There is a paradox in government's first-mover position that should encourage rather than alarm enterprise leaders. Precisely because governments have moved first, the path to governance is clearer than it has ever been for any previous technology. Organizations adopting AI today do not face the ambiguity that characterized the early days of data privacy, where standards were evolving and compliance targets were moving. For AI, the standards are substantially defined. The EU AI Act tells you what documentation you need. The NIST AI RMF tells you how to structure your governance. ISO/IEC 42001 provides a management system framework.[18] The OECD principles tell you what values to embed.

This clarity is a gift—even if it does not always feel like one. Enterprises that embrace the existing frameworks rather than waiting for enforcement will build governance as a strategic capability rather than a compliance cost. They will be the organizations that can demonstrate their AI governance quality to boards, investors, insurers, and regulators—not because they were compelled to, but because they recognized that government's early action created a roadmap that smart enterprises would be wise to follow.

For the first time in modern regulatory history, business does not need to guess what government wants. The question is whether business will act on what it already knows.

Notes

1. European Commission, “Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act),” COM(2021) 206 final, April 21, 2021. The proposal was adopted as Regulation (EU) 2024/1689 and entered into force on August 1, 2024. See https://artificialintelligenceact.eu/developments/ for the full legislative timeline.

2. Organisation for Economic Co-operation and Development, “Recommendation of the Council on Artificial Intelligence (OECD AI Principles),” OECD/LEGAL/0449, adopted May 22, 2019, revised November 8, 2023, and updated May 3, 2024. Initially adopted by forty-two countries (OECD member countries plus partner economies). As of 2024, forty-seven countries have adhered to the Principles. See https://oecd.ai/en/ai-principles.

3. National Institute of Standards and Technology, “Artificial Intelligence Risk Management Framework (AI RMF 1.0),” NIST AI 100-1, January 26, 2023. Updated through companion profiles and playbooks including the Generative AI Profile (NIST AI 600-1, July 2024). See https://www.nist.gov/itl/ai-risk-management-framework.

4. Japan, Act on the Promotion of Research and Development and Utilization of Artificial Intelligence-Related Technologies (AI Promotion Act). Cabinet submitted: February 28, 2025. Passed by the National Diet: May 28, 2025. Most provisions entered into force: June 4, 2025. See Future of Privacy Forum, “Understanding Japan’s AI Promotion Act,” 2025; White & Case, “AI Watch: Global Regulatory Tracker — Japan,” 2025.

5. South Korea, Framework Act on Artificial Intelligence Development and Establishment of a Foundation for Trustworthiness (AI Framework Act), passed December 26, 2024, scheduled to take effect January 22, 2026. See Future of Privacy Forum, “South Korea’s New AI Framework Act: A Balancing Act Between Innovation and Regulation,” April 18, 2025. See https://fpf.org/blog/south-koreas-new-ai-framework-act-a-balancing-act-between-innovation-and-regulation/.

6. International Association of Privacy Professionals, “AI Governance Profession Report 2025,” IAPP, April 2025. Survey of more than 670 professionals across forty-five countries. Seventy-seven percent reported working on AI governance; many programs are in early stages. See https://iapp.org/resources/article/ai-governance-profession-report.

7. IBM Security and Ponemon Institute, “Cost of a Data Breach Report 2025,” IBM, 2025. Sixty-three percent of organizations reported having no AI governance policies to manage AI deployment or prevent unauthorized AI usage. See https://www.ibm.com/reports/data-breach.

8. Stanford Institute for Human-Centered Artificial Intelligence, “AI Index Report 2025,” Stanford HAI, April 2025. Chapter 6 (Policy and Governance) reports that AI mentions in legislative proceedings across seventy-five major countries increased by 21.3 percent in 2024, rising to 1,889 from 1,557 in 2023, a ninefold increase since 2016. See https://hai.stanford.edu/ai-index/2025-ai-index-report.

9. Stanford HAI, “AI Index Report 2025,” Chapter 6. In 2024, U.S. federal agencies introduced fifty-nine AI-related regulations from forty-two unique agencies, more than double the twenty-five regulations from twenty-one agencies in 2023.

10. Stanford HAI, “AI Index Report 2025,” Chapter 6. The report notes that U.S. state-level AI-related laws rose from forty-nine in 2023 to one hundred thirty-one in 2024, more than doubling in a single year.

[11.] OECD.AI Policy Navigator, accessed March 2026. The Policy Navigator is a live repository covering more than eighty jurisdictions and organisations and cataloging over nine hundred AI policy initiatives. See https://oecd.ai/en/dashboards.

[12.] Stanford HAI, "AI Index Report 2025," Chapter 6. International AI safety institutes emerged beginning in November 2023 (U.S. and U.K.), with additional institutes pledged at the AI Seoul Summit in May 2024 by Japan, France, Germany, Italy, Singapore, South Korea, Australia, Canada, and the European Union.

[13.] OECD, "Recommendation on AI," adopted May 22, 2019. Initially adopted by forty-two countries; G20 Leaders endorsed the G20 AI Principles drawn from the OECD Recommendation at the Osaka Summit in June 2019. See https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[14.] McKinsey & Company, "Superagency in the Workplace: Empowering People to Unlock AI's Full Potential," January 28, 2025. Ninety-two percent of companies plan to increase AI investment; only one percent of leaders describe their organizations as AI-mature. The Stanford AI Index figure is used for the ninefold increase in legislative mentions; the McKinsey figure is used for the private-sector maturity gap.

[15.] European Commission, "Regulation (EU) 2024/1689 (Artificial Intelligence Act)," Official Journal of the European Union, August 2024. Phased implementation: prohibited practices from February 2, 2025; GPAI model obligations from August 2, 2025; high-risk AI system obligations (Annex III) from August 2, 2026; high-risk AI in regulated products (Annex I) from August 2, 2027.

[16.] U.S. Department of Justice, Federal Trade Commission, Consumer Financial Protection Bureau, and Equal Employment Opportunity Commission, "Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems," April 25, 2023. The agencies pledged to use their collective enforcement authorities to address AI-related harms. See also Gibson Dunn, "Artificial Intelligence Review and Outlook — 2024," which documents SEC, FTC, EEOC, CFPB, and DOJ AI-related enforcement activity.

[17.] Artificial Intelligence Act, Article 99: Fines. Maximum fines of up to €35 million or seven percent of total worldwide annual turnover for violations involving prohibited AI practices; up to €15 million or three percent for other violations. See https://artificialintelligenceact.eu/article/99/.

[18.] International Organization for Standardization, "ISO/IEC 42001:2023 — Information Technology — Artificial Intelligence — Management System," 2023. The standard specifies requirements for establishing, implementing, maintaining, and continually improving an AI management system within organizations. See https://www.iso.org/standard/81230.html.