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.

AI Governance Is Not Optional

Why Every Business Is an AI Business, Whether It Writes Code or Not

AIQA Global, LLC
December 2025

The Question No One Is Asking

There is a question that most corporate leaders are not yet asking, and it is costing them. The question is not whether their company should adopt artificial intelligence. That debate is effectively over. According to McKinsey's 2025 State of AI global survey, eighty-eight percent of organizations now use AI in at least one business function.[1] A separate McKinsey study found that ninety-two percent of companies plan to increase their AI investments over the next three years.[2] The question is not even whether AI introduces risk. Every serious executive acknowledges that it does. The question—the one that separates companies that will govern AI well from those that will govern it badly—is this: ***Do you know where all the AI in your enterprise actually is?***

For most companies, the honest answer is no. And the reason is that the conventional framing of AI governance is dangerously narrow. The public conversation about AI risk focuses overwhelmingly on the companies that build AI—the frontier model developers, the large language model providers, the firms training systems on billions of parameters. That conversation is important. But it has almost nothing to do with the governance challenge facing the vast majority of enterprises, which do not build AI at all. They buy it. They embed it. They inherit it. And increasingly, they are exposed to it through supply chains, vendor relationships, and partner ecosystems that are adopting AI at an extraordinary pace—often without their knowledge and almost always without their oversight.

This article is about that gap. It is about the growing reality that AI governance is not a concern reserved for technology companies or firms with machine learning teams. It is a concern for every enterprise that relies on other organizations to operate—which is to say, every enterprise. The thesis is straightforward: if your suppliers use AI, if your vendors use

AI, if your insurers price AI risk, if your customers expect AI-driven service, then you are an AI business. And if you are an AI business, then AI governance is not optional. It is the cost of operating responsibly in the modern economy.

The Invisible AI Supply Chain

Consider the operating reality of a mid-market manufacturing company. It does not build AI models. It does not employ data scientists. Its leadership team would describe the firm as a traditional industrial business. And yet, consider what its vendors are doing. Its ERP provider has embedded AI-driven demand forecasting into the latest software release. Its logistics partner uses machine learning to optimize routing and delivery schedules. Its primary raw-materials supplier relies on AI-powered quality inspection at the production line. Its bank uses AI credit-scoring models to set the terms of its revolving credit facility. Its insurer is beginning to use AI risk models to price its coverage. Its outside law firm uses AI for document review and contract analysis.

None of these AI systems were built by the manufacturer. None of them appear in the manufacturer's technology budget. None of them are subject to the manufacturer's internal IT policies. And yet every one of them affects the manufacturer's operations, cost structure, risk profile, and competitive position. The manufacturer is, whether it recognizes it or not, a node in a complex AI supply chain—a chain in which decisions made by algorithms it has never seen, trained on data it has never reviewed, govern outcomes that are material to its business.

This is not a hypothetical scenario. It is the operating reality of most enterprises today. Deloitte's 2026 State of AI in the Enterprise survey—covering more than three thousand senior leaders across twenty-four countries—found that organizations are deploying autonomous AI agents across multiple functions, from financial services to manufacturing to customer operations.[3] Gartner projects that forty percent of enterprise applications will feature task-specific AI agents by 2026, up from less than five percent in 2025.[4] The velocity of this shift means that the AI systems affecting your business are proliferating far faster than your ability to catalog them—let alone govern them.

The implications for governance are profound. A company that governs only its own AI—assuming it has any—while ignoring the AI embedded in its supply chain is engaging in a form of risk management theater. The exposure is real even when the technology is invisible. If your logistics provider's routing algorithm fails and your shipments are delayed, the operational consequences are yours. If your bank's credit-scoring model produces discriminatory outcomes and your credit facility is affected, the financial consequences are

yours. If your vendor's AI-powered quality inspection misses a defect, the product liability consequences may well be yours.

Regulation Is Already Here—and It Follows the Supply Chain

If the business case for governing AI across the supply chain were not sufficient, the regulatory case is becoming unavoidable. The EU AI Act—the world's first comprehensive AI regulatory framework—entered into force in August 2024 and is being implemented in phases, with obligations for most high-risk AI systems taking effect by August 2026 and certain high-risk systems embedded in regulated products following by August 2027.[5] Critically, the Act does not limit its obligations to companies that build AI. It imposes responsibilities on every actor in the AI value chain: providers, deployers, importers, and distributors.

Article 25 of the Act is explicit on this point. Any distributor, importer, or deployer that puts its name on a high-risk AI system, makes a substantial modification to one, or changes the intended purpose of an AI system to make it high-risk becomes the provider of that system for regulatory purposes—and inherits the provider's full compliance obligations.[6] The Act further requires that providers and third-party suppliers agree in writing on the sharing of information, technical access, and assistance needed to ensure compliance throughout the supply chain. This is not a suggestion. It is a statutory obligation.

The practical consequence is that a company deploying a third-party AI system for, say, creditworthiness assessment or insurance pricing must conduct fundamental rights impact assessments, retain system logs, monitor performance, and report serious incidents—regardless of whether it built the system or merely licensed it. A bank using a vendor's AI for credit decisions becomes a deployer under the Act, with direct compliance obligations. An insurer using third-party AI risk models faces the same. A manufacturer embedding an AI quality-inspection tool in its production line faces the same.

In the United States, the regulatory trajectory points in the same direction, if by a different route. The NIST AI Risk Management Framework, released in 2023 and updated through 2025, has become the de facto U.S. reference standard for AI governance.[7] Although voluntary, the framework's principles are increasingly referenced by sector regulators. In April 2023, the DOJ, FTC, CFPB, and EEOC issued a joint statement pledging to use their collective enforcement authorities to address AI-related harms, and the SEC has separately probed investment advisers' use of AI.[8] The framework explicitly calls for organizations to map AI systems throughout their lifecycle, including third-party components and

dependencies—effectively requiring supply-chain-level AI governance for any organization that takes it seriously.

Internationally, more than seventy jurisdictions have now published national AI strategies, policies, or regulatory frameworks, according to the OECD AI Policy Observatory.[9] Japan's Cabinet submitted the AI Promotion Act to the Diet in February 2025; the parliament passed it on May 28, 2025, and most provisions entered into force on June 4, 2025—making Japan the second major Asia-Pacific economy to enact comprehensive AI legislation.[10] ISO/IEC 42001 provides an international standard for AI management systems. The direction of travel is unmistakable: AI governance obligations are proliferating, they follow the supply chain, and they apply to deployers and users—not only to developers.

The Insurance Market Is Watching

Regulation creates compliance obligations. The insurance market creates financial ones. And the insurance market is moving faster than many enterprises realize.

For years, AI risk was covered silently—embedded within existing general liability, professional liability, and errors-and-omissions policies without explicit mention, pricing, or exclusion. That era is ending. Major carriers are developing AI-specific products, endorsements, and exclusions. Munich Re's aiSure product provides performance guarantees for AI systems backed by reinsurance. Lloyd's syndicates have introduced AI-specific placements. AXA XL has developed generative-AI endorsements. Beazley has begun pricing AI risk as a distinct underwriting variable.[11]

The common thread across these developments is that insurers are demanding evidence of AI governance quality as a condition of favorable terms. The principle is intuitive and familiar from every other line of coverage: if you can demonstrate that you manage your risks well, you get better pricing. If you cannot, you pay more—or you do not get covered at all. What is new is the extension of this principle to AI. An enterprise that cannot demonstrate measurable AI governance—including governance of the AI in its supply chain—is increasingly likely to face higher premiums, broader exclusions, or reduced coverage limits.

This is not a future concern. It is happening now. And it does not require that your company build or deploy any AI of its own. If your vendors use AI, and their AI fails in a way that causes you loss, the relevant question from your insurer will be: what did you do to assess and manage that risk? If the answer is nothing, the claims conversation will be difficult.

Boards Cannot Govern What They Cannot See

The governance failure at the board level is one of visibility. Most corporate boards today cannot answer basic questions about their company's AI exposure: How many AI systems does the company operate or rely upon? What data do those systems use? Who validated them? What happens when they fail? Who is accountable? These are not esoteric technical questions. They are governance fundamentals—no different in kind from asking how many material contracts the company has, or what its cybersecurity posture looks like, or whether its financial controls are adequate.

The problem is compounded by the fact that much of a company's AI exposure is indirect. A board that asks its CTO for an inventory of internal AI deployments may get a reasonably complete answer. A board that asks for an inventory of AI systems across its vendor and supplier ecosystem will almost certainly discover that no such inventory exists. And yet the fiduciary responsibility for the risks those systems create runs through the board regardless.

Effective AI governance at the board level requires, at minimum, three capabilities that most companies currently lack. First, a comprehensive map of AI exposure—not just internal deployments but third-party AI systems that touch the company's operations, data, customers, or risk profile. Second, a framework for evaluating the governance quality of those systems—not a vague qualitative assessment, but a structured, quantifiable evaluation that can be compared across vendors, tracked over time, and reported to stakeholders. Third, an accountability structure that assigns clear ownership of AI risk at the management level and ensures that the board receives regular, accurate reporting on the company's AI governance posture.

None of this is possible without measurement. You cannot govern what you cannot see, and you cannot manage what you cannot measure. This is, ultimately, why AI governance ratings matter—and why the absence of a standardized, independent AI governance metric has been such a significant gap in the market. Every other class of enterprise risk that matters to boards, investors, and insurers eventually gets a quality metric: credit quality, patent quality, cybersecurity maturity, ESG compliance. AI governance quality is next.

Governance as Competitive Advantage

It is tempting to frame AI governance entirely as a risk-mitigation exercise—a cost center, a compliance burden, an obligation to be minimized. That framing is understandable and incomplete. The companies that govern AI best will not merely avoid losses. They will outperform.

The logic is straightforward. Companies that can demonstrate strong AI governance negotiate better insurance terms. They satisfy regulatory requirements more efficiently. They attract institutional investors who increasingly screen for governance quality. They build more durable relationships with enterprise customers who are themselves under pressure to demonstrate supply-chain governance. They recruit better talent, because the best data scientists and AI engineers prefer to work for organizations with clear ethical frameworks. And they deploy AI faster, because well-governed organizations have the guardrails in place that allow rapid, confident adoption—while organizations without governance stumble through ad hoc risk debates every time a new AI tool is proposed.

This is the insight that transforms AI governance from a defensive posture to a strategic asset. The companies that will lead in the AI economy are not the ones that avoid governance. They are the ones that embrace it early, measure it rigorously, and use it to build trust with every constituency that matters—boards, investors, insurers, regulators, customers, and employees.

What Enterprises Should Do Now

The path from recognizing that AI governance is not optional to actually implementing it requires concrete action. Based on the regulatory landscape, market trends, and governance best practices, we recommend that every enterprise—regardless of whether it builds AI internally—take four immediate steps.

Map your AI exposure. Conduct a comprehensive inventory of AI systems that touch your organization—not only internal deployments but AI embedded in vendor software, supply-chain systems, financial products, and professional services. This mapping exercise is now explicitly recommended by the NIST AI Risk Management Framework and is a precondition for compliance with the EU AI Act's deployer obligations. You cannot govern what you have not identified.

Assess governance quality, not just compliance checkboxes. Compliance frameworks tell you whether a system meets a minimum threshold. Governance quality ratings tell you how well that system is managed relative to best practice and relative to peers. The difference is the same as the difference between knowing that a borrower is not in default and knowing that borrower's credit score. Both are useful. Only one gives you a basis for comparison, benchmarking, and improvement over time.

Extend governance into procurement and vendor management. AI governance cannot stop at your organization's boundary. Every vendor agreement, every supplier

contract, every professional services engagement that involves AI should include governance provisions: disclosure of AI use, evidence of governance practices, incident reporting obligations, and audit rights. The EU AI Act already requires written agreements between providers and third-party suppliers of AI components. Leading enterprises will adopt this discipline voluntarily and universally, not only where regulation compels it.

Bring AI governance into the boardroom. AI risk is an enterprise risk. It belongs on the board's agenda alongside cybersecurity, financial controls, and regulatory compliance. Boards should receive regular reporting on the company's AI governance posture, including metrics that allow tracking over time and benchmarking against peers. This requires measurement—and measurement requires standards.

The Standard Is Coming. The Question Is Whether You'll Be Ready.

The history of intangible-asset measurement is instructive. Before standardized credit ratings, lending decisions were subjective, inconsistent, and opaque. Before patent quality scores, intellectual property portfolios were valued by intuition rather than evidence. Before ESG metrics, responsible investing was an aspiration without a measuring stick. In each case, the introduction of a standardized quality metric did not merely satisfy a regulatory requirement. It created a common language that transformed how capital was allocated, how risk was priced, and how organizations competed.

AI governance is at that inflection point now. The regulatory frameworks are in place. The insurance market is differentiating on governance quality. Boards are recognizing their fiduciary exposure. Institutional investors are beginning to ask the right questions. What has been missing is the metric—the standardized, independent, quantitative measure of AI governance quality that allows comparison, benchmarking, and accountability across organizations.

That metric is the purpose AIQA Global was created to provide. The AIQ™ Score assesses enterprise AI governance across five dimensions and 250 data points, producing a comparable, evidence-based quality rating designed for use by the constituencies that need it most: investors, insurers, corporate boards, and the enterprises themselves. It is built on the same foundational discipline—proprietary quality rating of previously unmeasured intangible assets—that the founders applied at Ocean Tomo to create the first patented patent-quality scoring system and the Ocean Tomo 300® Patent Index.

The organizations that will thrive in the AI economy are not the ones that move fastest. They are the ones that move most intelligently—with governance frameworks that can withstand

regulatory scrutiny, satisfy insurers, attract capital, and earn the trust of every stakeholder in the value chain. AI governance is not optional. And the companies that treat it as a strategic imperative—rather than a compliance afterthought—will be the ones that define the standard for everyone else.

Notes

1. McKinsey & Company, "The State of AI in 2025: Agents, Innovation, and Transformation," McKinsey Global Survey, November 2025. The survey found that eighty-eight percent of organizations use AI in at least one business function.

2. McKinsey & Company, "Superagency in the Workplace: Empowering People to Unlock AI's Full Potential," January 28, 2025. Based on a survey of 3,613 employees and 238 C-suite leaders, the report found that ninety-two percent of companies plan to increase AI investment over the next three years.

3. Deloitte, "State of AI in the Enterprise, 2026," Deloitte Global, 2026. Survey of 3,235 senior leaders across twenty-four countries conducted August–September 2025.

4. Gartner, Inc., "Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up from Less than 5% in 2025," press release, August 26, 2025.

5. European Commission, "Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)," Official Journal of the European Union, August 1, 2024. Obligations apply in phases: prohibited practices from February 2, 2025; high-risk AI system obligations (Annex III) from August 2, 2026; high-risk AI systems in regulated products (Annex I) from August 2, 2027.

6. Artificial Intelligence Act, Article 25: Responsibilities Along the AI Value Chain. See EU AI Act, Regulation 2024/1689, Chapter III, Section 3.

7. National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, January 26, 2023. The framework's four core functions—Govern, Map, Measure, and Manage—include explicit guidance on mapping third-party AI components and dependencies. Updated through the Generative AI Profile (NIST AI 600-1, July 2024) and companion playbooks.

8. 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 "vigorously use [their] collective authorities to protect individuals' rights regardless of whether legal violations occur through traditional means or advanced technologies." See also Richard Vanderford, "SEC Probes Investment Advisers' Use of AI," Wall Street Journal, December 10, 2023.

9. OECD.AI Policy Observatory, "Countries & Initiatives Overview," OECD, accessed March 2026. The observatory's live repository covers AI policy initiatives from more than seventy countries and territories. See https://oecd.ai/en/dashboards.

10. Japan, Act on the Promotion of Research and Development and Utilization of Artificial Intelligence-Related Technologies (AI Promotion Act). Cabinet submission: February 28, 2025. Passed by the National Diet: May 28, 2025. Most provisions entered into force: June 4, 2025. AI Strategy Headquarters chapters effective: September 1, 2025. See Future of Privacy Forum, "Understanding Japan's AI Promotion Act," 2025; International Bar Association, "Japan's Emerging Framework for Responsible AI," 2025.

11. AI insurance product references: Munich Re, "aiSure: De-Risking AI Ventures," Munich Re whitepaper, 2024 (performance guarantees for AI systems backed by reinsurance); Armilla AI and Chaucer (Lloyd's syndicate), "Vanguard AI" placement, 2024; AXA XL, Generative AI Endorsement, 2024;

Beazley, AI risk underwriting practices as reported in industry press. AIQA Global's research on AI adoption in the global insurance market, conducted in Q4 2025 for AXA XL, provides additional context.

© 2025 AIQA Global, LLC. All rights reserved. AIQ™ and AIQ Score™ are trademarks of AIQA Global, LLC. This article is published for informational purposes and does not constitute legal, investment, or regulatory advice.

AIQA Global, LLC | Chicago | North Miami Beach | Greenwich | AIQAglobal.com